



Statewide Contract Summary

Official signed contract documents are on file with OMES Central Purchasing.

Contract title: Software Value Added Reseller

Contract Number: SW1041OR

Date of Contract issuance: 08/02/2024

Contract period: 08/02/2024 through 03/13/2025

Agreement period: 08/02/2024 through 03/14/2028

Type of contract: Mandatory ☐ Non-Mandatory ☒

OMES Central Purchasing contact: Barry

Title: Procurement Specialist

Phone: (405) - 521 - 6721

Email: barry.timberlake@omes.ok.gov

Supplier name: Oracle America

Supplier ID #: 265207

Contract ID #: 7489

Supplier Point of Contact: JP Incorvaja

Supplier address: 500 Oracle Parkway

City: Redwood Shores

State: CA

Zip Code: 94065 -

Phone #: 1 - 651 - 356 - 2531

Email: jp.incorvaja@oracle.com

Contract Overview:

Authorized Users: All state departments, boards, commissions, agencies, and institutions, in Addition to counties, school districts and municipalities which may avail themselves of this contract.

How to order:

Available Brands:

Available Products and Services:

Authorized Dealer/Reseller(s):

Supplier name:

Supplier ID #:

Contract ID #:

Supplier Point of Contact:

Supplier address:

City:

State:

Zip Code:

-

Phone #: 1 - - -

Email:

Supplier name:

Supplier ID #:

Contract ID #:

Supplier Point of Contact:

Supplier address:

City:

State:

Zip Code:

-

Phone #: 1 - - -

Email:

Software Publishers	Description	Maximum Cost + % Markup	% off List Price
The following Oracle Public Price Lists are attached to this submission:			
	Oracle Java SE Universal Subscription Global Price List		
	January 23, 2023		
	ID Edwards Component Global Price List		
	July 11, 2022		
	MySQL Global Price List		
	March 1, 2023		
	Oracle Business Intelligence Applications Global Price List		
	September 1, 2016		
	Oracle Cloud Platform as a Service and Infrastructure as a Service – Public Cloud Global Price List		
	March 9, 2023		
	Oracle E-Business Suite Applications Global Price List		
	March 9, 2023		
	Oracle Engineered Systems Price List		
	December 1, 2022		
	Oracle Fusion Applications Global Price List		
	December 13, 2017		
	Oracle Fusion Cloud Service Global Price List		
	March 21, 2023		
	Oracle Global Price List Siebel CRM Pricing		
	February 1, 2023		
	Oracle Marketing Cloud Global Price List (Including CrowdTwist, Eloqua, Infinity, Maxymiser, and Responsys)		
	February 1, 2023		
	Oracle RightNow (Service Cloud) Global Price List		
	February 1, 2023		
	Oracle Technology Global Price List		
	March 1, 2023		
	Oracle Taleo Cloud Service Global Price List		
	September 8, 2022		
	PeopleSoft Component Global Price List		
	July 11, 2023		
The following Oracle CONFIDENTIAL Price Lists are attached to this submission:			
	Oracle Construction & Engineering Global Price List		
	March 21, 2023		
	Systems Hardware and Software Global Price List		
	March 7, 2023		
Other Value Add Products and Services			
	Description	Maximum Cost + % Markup	% off List Price
Oracle Customer Success Services (CSS) formerly Advanced Customer Services (ACS)			
	Oracle Advanced Management for Hybrid Cloud		15%
	Oracle Managed Analytics Cloud Service		15%
	Oracle Managed Applications Unlimited Non-Production Service on Oracle Technology Cloud		15%
	Oracle Managed Applications Unlimited on Oracle Technology Cloud-Enhanced Recovery Service		15%
	Oracle Managed Applications Unlimited on Oracle Technology Cloud-RAC Support Option for Minimum and Low Complexity Services		15%
	Oracle Managed Cloud Helpdesk for Applications Unlimited		15%
	Oracle Managed Database as a Service		15%
	Oracle Managed Integration Cloud Service		15%
	Oracle Managed Identity and Access Management Services		15%
	Oracle Managed Identity and Access Management-Integrated Applications Unlimited, Custom		15%
	Oracle Managed WebLogic Server		15%
	Oracle Regression Testing Service for OCI, Configurable		15%
	Oracle Managed Security Services-Data Masking, Database Audit, Database Vault, Vulnerability Assessment, Web Application Firewall		15%
	Oracle Managed Security File Integrity Monitoring Service for Oracle Technology Cloud		15%
	Oracle Cloud Service Units		15%
	Oracle Mission Critical Support for SaaS		15%
	Oracle Business Help Desk for SaaS		15%
	Oracle Critical Process Management for SaaS		15%

Oracle Regression Testing Service for SaaS				15%
Oracle Extensions and Integrations Support for SaaS				15%
Oracle Learning Services				
Oracle Cloud Infrastructure and Technology Exam				
Oracle Cloud Applications Exams				15%
Oracle Foundations Exams for Students			\$245/user	15%
Cloud Applications Learning Subscription			\$245/user	0%
Technology Learning Subscription			\$95/user	15%
Event Learning Subscription			\$4,995.00 per user / 12 months	15%
Cloud Applications Senior Consultant User Adoption - Day			\$4,995.00 per user / 12 months	15%
Managed Services Pack for Guided Learning Service			\$5,000/user (10+ user minimum)	15%
Fusion ERP Cloud Guided Learning Service - Hosted Named User			\$2,575.00 per day	15%
Fusion ERP Cloud Guided Learning Service - Hosted Employee			\$30,000.00 per managed service pack	15%
Fusion HCM Cloud Guided Learning Service - Hosted Named User			\$20.00 per Hosted Named User / per month	
Fusion HCM Cloud Guided Learning Service - Hosted Employee			\$5.00 per Hosted Employee / per month	
Fusion HCM Cloud Guided Learning Service - Hosted Named User			\$15.00 per Hosted Named User / per month	
Fusion HCM Cloud Guided Learning Service - Hosted Employee			\$2.00 per Hosted Employee / per month	
Fusion CX Cloud Guided Learning Service - Hosted Named User			\$20.00 per Hosted Named User / per month	
Custom Guided Learning Service - Hosted Employee			\$5.00 per Hosted Employee / per month	
Custom Guided Learning Service - Hosted Named User			\$15.00 per Hosted Named User / per month	
Oracle Communications Cloud Guided Learning Service - Hosted Named User			\$20.00 per Hosted Named User / per month	
Oracle Communications Cloud Guided Learning Service - Hosted Employee			\$5.00 per Hosted Employee / per month	
Oracle Utilities Cloud Guided Learning Service - Hosted Named User			\$20.00 per Hosted Named User / per month	
Oracle Utilities Cloud Guided Learning Service - Hosted Employee			\$5.00 per Hosted Employee / per month	
Oracle Construction and Engineering Cloud Guided Learning Service - Hosted Named User			\$5.00 per Hosted Employee / per month	
Oracle Construction and Engineering Cloud Guided Learning Service - Hosted Employee			\$20.00 per Hosted Named User / per month	
Oracle Retail Cloud Guided Learning Service - Hosted Named User			\$5.00 per Hosted Employee / per month	
Oracle Retail Cloud Guided Learning Service - Hosted Employee			\$20.00 per Hosted Named User / per month	
Oracle Hospitality Cloud Guided Learning Service - Hosted Named User			\$5.00 per Hosted Employee / per month	
Oracle Hospitality Cloud Guided Learning Service - Hosted Employee			\$20.00 per Hosted Named User / per month	
Oracle Health Sciences Cloud Guided Learning Service - Hosted Named User			\$5.00 per Hosted Employee / per month	
Oracle Health Sciences Cloud Guided Learning Service - Hosted Employee			\$20.00 per Hosted Named User / per month	
Oracle Insurance Cloud Guided Learning Service - Hosted Named User			\$5.00 per Hosted Employee / per month	
Oracle Insurance Cloud Guided Learning Service - Hosted Employee			\$20.00 per Hosted Named User / per month	
Oracle Financial Services Cloud Guided Learning Service - Hosted Named User			\$5.00 per Hosted Employee / per month	
Oracle Financial Services Cloud Guided Learning Service - Hosted Employee			\$20.00 per Hosted Named User / per month	
Oracle Financial Services Cloud Guided Learning Service - Hosted Employee			\$5.00 per Hosted Employee / per month	
Professional Services - Hourly Not-to-Exceed Rates				
Description				
Oracle Customer Success Services (CSS) formerly Advanced Customer Services (ACS)				
Senior CSS/ACS Engineer		List Price	\$402.95	Discounted Hourly Rates 1-30 Days \$402.95
CSS/ACS Engineer			\$399.13	31-60 Days \$390.91
Technical Account Manager I			\$399.13	61-90 Days \$382.85
				\$343.09
				\$342.09



STATE OF OKLAHOMA STATEWIDE CONTRACT WITH ORACLE AMERICA, INC.

This State of Oklahoma Statewide Contract No. 1041 (“Contract”) is entered into between the state of Oklahoma by and through the Office of Management and Enterprise Services and Oracle America, Inc. (“Supplier”) and is effective as of the date of last signature to this Contract. The initial Contract term, which begins on the effective date of the Contract, ends on March 13, 2025 and there are three (3) one-year options to renew the Contract.

Purpose

The State is awarding this Contract to Supplier for the provision of the Products and Service Offerings described herein to support State agencies and other eligible Customers (as defined in Attachment B, General Terms) pursuant to orders placed by Customers in accordance with the Contract and as more particularly described in certain Contract Documents. Supplier submitted a proposal which contained exceptions to the Solicitation, which contained additional terms, and with certain information requested to be considered confidential. This Contract memorializes the agreement of the parties with respect to negotiated terms of the Contract that is being awarded to Supplier.

Now, therefore, in consideration of the foregoing and the mutual promises set forth herein, the receipt and sufficiency of which are hereby acknowledged the parties agree as follows:

1. The parties agree that Supplier has not yet begun performance of work under this Contract. Upon full execution of this Contract, Supplier may begin work. Issuance of a purchase order is required prior to payment to a Supplier.
2. The following Contract Documents are attached hereto and incorporated herein:
 - 2.1. Solicitation 0000000199, Attachment A;
 - 2.2. General Terms, Attachment B;
 - 2.3. Oklahoma Statewide Contract Terms, Attachment C;
 - 2.4. Information Technology terms, Attachment D;
 - 2.5. Portions of the Bid as revised, Attachment E

- i. Schedule C, Cloud Services – Public Sector, Attachment E-1;
 - ii. Schedule P, Program, Attachment E-2;
 - iii. Schedule S, Services, Attachment E-3;
 - iv. Schedule OSSS, Oracle Open Source Support Services Schedule, Attachment E-4,
 - v. Pricing, Attachment E-5.
 - 2.6. Negotiated Exceptions to Contract, Attachment F; and
 - 2.7. Template for Contract Modifications for Quotes, Statements of Work, or other Ordering Documents, Attachment F-1.
3. The parties additionally agree:
- 3.1. except for and information deemed confidential by the State pursuant to applicable law, rule, regulation or policy, the parties agree the Contract terms and pricing information are not confidential and are disclosable without further approval of or notice to Supplier; and
 - 3.2. At the end of the then-current Contract term, the Contract will auto-renew for the next option year unless either party gives at least thirty (30) days advance written notice of their intent to not renew (provided that the Contract shall not extend past March 13, 2028 unless agreed to by the parties in an Addendum).
- Attachments referenced in this section are attached hereto and incorporated herein.
4. Any reference to a Contract Document refers to such Contract Document as it may have been amended. If and to the extent any provision is in multiple documents and addresses the same or substantially the same subject matter but does not create an actual conflict, the more recent provision is deemed to supersede earlier versions.

[Remainder of Page Intentionally Blank]

STATE OF OKLAHOMA
by and through the
OFFICE OF MANAGEMENT AND
ENTERPRISE SERVICES

ORACLE AMERICA, INC.

By: 
Joe McIntosh (Aug 2, 2024 13:14 CDT)

Name: Joe McIntosh

Title: CIO

Date: 08/02/2024

By: 
3C26488AB41E4BB...

Name: Jake Camarillo

Title: Manager, Deal Management

Date: 01-Aug-2024 | 1:07 PM CDT

Oracle Agreement Number: **US-GMA-80421183**

ATTACHMENT A
EVENT NO. 0000000199

This Solicitation is a Contract Document and is a request for proposal in connection with the Contract awarded by the Office of Management and Enterprise Services as more particularly described below. Any defined term used herein but not defined herein shall have the meaning ascribed in the General Terms or other Contract Document.

PURPOSE

The Contract is awarded as a statewide contract on behalf of the Office of Management and Enterprise Services for software and services to support State agencies and other eligible Oklahoma Interlocal Entities. This Supplier will provide software, training, pre-sales assistance, documentation, installation, maintenance, support, configuration, customization, and license agreement administration. This bid supports both SaaS Cloud Based Solutions and On-Prem Software Solutions.

1. Contract Term and Renewal Options

The initial Contract term, which begins on the effective date of the Contract, will run concurrently with award dated 03/14/2023. There will be four (4) annual renewals remaining.

This RFP is a supplemental solicitation to Solicitation 0900000556 to add additional suppliers within scope.

ATTACHMENT B

STATE OF OKLAHOMA GENERAL TERMS

This State of Oklahoma General Terms (“General Terms”) is a Contract Document in connection with a Contract awarded by the Office of Management and Enterprise Services on behalf of the State of Oklahoma.

In addition to other terms contained in an applicable Contract Document, Supplier and State agree to the following General Terms:

1 Scope and Contract Renewal

- 1.1** Supplier may not add products or services to its offerings under the Contract without the State’s prior written approval. Such request may require a competitive bid of the additional products or services. If the need arises for goods or services outside the scope of the Contract, Supplier shall contact the State.
- 1.2** At no time during the performance of the Contract shall the Supplier have the authority to obligate any Customer for payment for any products or services (a) when a corresponding encumbering document is not signed or (b) over and above an awarded Contract amount. Likewise, Supplier is not entitled to compensation for a product or service provided by or on behalf of Supplier that is neither requested nor accepted as satisfactory.
- 1.3** If applicable, prior to any Contract renewal, the State shall subjectively consider the value of the Contract to the State, the Supplier’s performance under the Contract, and shall review certain other factors, including but not limited to the: a) terms and conditions of Contract Documents to determine validity with current State and other applicable statutes and rules; b) current pricing and discounts offered by Supplier; and c) current products, services and support offered by Supplier. If the State determines changes to the Contract are required as a condition precedent to renewal, the State and Supplier will cooperate in good faith to evidence such required changes in an Addendum. Further, any request for a price increase in connection with a renewal or otherwise will be conditioned on the Supplier providing appropriate documentation supporting the request.
- 1.4** The State may extend the Contract for ninety (90) days beyond a final renewal term at the Contract compensation rate for the extended period. If the State

exercises such option to extend ninety (90) days, the State shall notify the Supplier in writing prior to Contract end date. The State, at its sole option and to the extent allowable by law, may choose to exercise subsequent ninety (90) day extensions at the Contract pricing rate, to facilitate the finalization of related terms and conditions of a new award or as needed for transition to a new Supplier.

- 1.5** Supplier understands that supplier registration expires annually and, pursuant to OAC 260:115-3-3, Supplier shall maintain its supplier registration with the State as a precondition to a renewal of the Contract.

2 Contract Effectiveness and Order of Priority

- 2.1** Unless specifically agreed in writing otherwise, the Contract is effective upon the date last signed by the parties. Supplier shall not commence work, commit funds, incur costs, or in any way act to obligate the State until the Contract is effective.
- 2.2** Contract Documents shall be read to be consistent and complementary. Any conflict among the Contract Documents shall be resolved by giving priority to Contract Documents in the following order of precedence:
- A.** any Addendum;
 - B.** any applicable Solicitation;
 - C.** any Contract-specific State terms contained in a Contract Document including, without limitation, information technology terms and terms specific to a statewide Contract or a State agency Contract;
 - D.** the terms contained in this Contract Document;
 - E.** any successful Bid as may be amended through negotiation and to the extent the Bid does not otherwise conflict with the Solicitation or applicable law;
 - F.** any statement of work, work order, or other similar ordering document as applicable; and
 - G.** other mutually agreed Contract Documents.
- 2.3** If there is a conflict between the terms contained in this Contract Document or in Contract-specific terms and an agreement provided by or on behalf of Supplier including but not limited to linked or supplemental documents which alter or diminish the rights of Customer or the State, the conflicting terms

provided by Supplier shall not take priority over this Contract Document or Acquisition-specific terms. In no event will any linked document alter or override such referenced terms except as specifically agreed in an Addendum.

- 2.4 Any Contract Document shall be legibly written in ink or typed. All Contract transactions, and any Contract Document related thereto, may be conducted by electronic means pursuant to the Oklahoma Uniform Electronic Transactions Act.

3 **Modification of Contract Terms and Contract Documents**

- 3.1 The Contract may only be modified, amended, or expanded by an Addendum. Any change to the Contract, including the addition of work or materials, the revision of payment terms, or the substitution of work or materials made unilaterally by the Supplier, is a material breach of the Contract. Unless otherwise specified by applicable law or rules, such changes, including without limitation, any unauthorized written Contract modification, shall be void and without effect and the Supplier shall not be entitled to any claim under the Contract based on those changes. No oral statement of any person shall modify or otherwise affect the terms, conditions, or specifications stated in the Contract.
- 3.2 Any additional terms on an ordering document provided by Supplier are of no effect and are void unless mutually executed. OMES bears no liability for performance, payment or failure thereof by the Supplier or by a Customer other than OMES in connection with an Acquisition.

4 **Definitions**

In addition to any defined terms set forth elsewhere in the Contract, the Oklahoma Central Purchasing Act and the Oklahoma Administrative Code, Title 260, the parties agree that, when used in the Contract, the following terms are defined as set forth below and may be used in the singular or plural form:

- 4.1 **Acquisition** means items, products, materials, supplies, services and equipment acquired by purchase, lease purchase, lease with option to purchase, value provided or rental under the Contract.
- 4.2 **Addendum** means a mutually executed, written modification to a Contract Document.
- 4.3 **Amendment** means a written change, addition, correction or revision to the Solicitation.
- 4.4 **Bid** means an offer a Bidder submits in response to the Solicitation.

- 4.5 **Bidder** means an individual or business entity that submits a Bid in response to the Solicitation.
- 4.6 **Contract** means the written, mutually agreed and binding legal relationship resulting from the Contract Documents and an appropriate encumbering document as may be amended from time to time, which evidences the final agreement between the parties with respect to the subject matter of the Contract.
- 4.7 **Contract Document** means this document; any master or enterprise agreement terms entered into between the parties that are mutually agreed to be applicable to the Contract; any Solicitation; any Contract-specific terms; any Supplier's Bid as may be negotiated; any statement of work, work order, or other similar mutually executed ordering document; other mutually executed documents and any Addendum.
- 4.8 **Customer** means the entity receiving goods or services contemplated by the Contract.
- 4.9 **Debarment** means action taken by a debarring official under federal or state law or regulations to exclude any business entity from inclusion on the Supplier list; bidding; offering to bid; providing a quote; receiving an award of contract with the State and may also result in cancellation of existing contracts with the State.
- 4.10 **Destination** means delivered to the receiving dock or other point specified in the applicable Contract Document.
- 4.11 **Indemnified Parties** means the State and Customer and/or its officers, directors, agents, employees, representatives, contractors, assignees and designees thereof.
- 4.12 **Inspection** means examining and testing an Acquisition (including, when appropriate, raw materials, components, and intermediate assemblies) to determine whether the Acquisition meets Contract requirements.
- 4.13 **Moral Rights** means any and all rights of paternity or integrity of the Work Product and the right to object to any modification, translation or use of the Work Product and any similar rights existing under the judicial or statutory law of any country in the world or under any treaty, regardless of whether or not such right is denominated or referred to as a moral right.
- 4.14 **OAC** means the Oklahoma Administrative Code.
- 4.15 **OMES** means the Office of Management and Enterprise Services.

- 4.16 Solicitation** means the document inviting Bids for the Acquisition referenced in the Contract and any amendments thereto.
- 4.17 State** means the government of the state of Oklahoma, its employees and authorized representatives, including without limitation any department, agency, or other unit of the government of the state of Oklahoma.
- 4.18 Supplier** means the Bidder with whom the State enters into the Contract awarded pursuant to the Solicitation or the business entity or individual that is a party to the Contract with the State.
- 4.19 Suspension** means action taken by a suspending official under federal or state law or regulations to suspend a Supplier from inclusion on the Supplier list; be eligible to submit Bids to State agencies and be awarded a contract by a State agency subject to the Central Purchasing Act.
- 4.20 Supplier Confidential Information** means certain confidential and proprietary information of Supplier that is clearly marked as confidential and agreed by the State Purchasing Director or Customer, as applicable, but does not include information excluded from confidentiality in provisions of the Contract or the Oklahoma Open Records Act.
- 4.21 Work Product** means any and all deliverables produced by Supplier under a statement of work or similar Contract Document issued pursuant to this Contract, including any and all tangible or intangible items or things that have been or will be prepared, created, developed, invented or conceived at any time following the Contract effective date including but not limited to any (i) works of authorship (such as manuals, instructions, printed material, graphics, artwork, images, illustrations, photographs, computer programs, computer software, scripts, object code, source code or other programming code, HTML code, flow charts, notes, outlines, lists, compilations, manuscripts, writings, pictorial materials, schematics, formulae, processes, algorithms, data, information, multimedia files, text web pages or web sites, other written or machine readable expression of such works fixed in any tangible media, and all other copyrightable works), (ii) trademarks, service marks, trade dress, trade names, logos, or other indicia of source or origin, (iii) ideas, designs, concepts, personality rights, methods, processes, techniques, apparatuses, inventions, formulas, discoveries, or improvements, including any patents, trade secrets and know-how, (iv) domain names, (v) any copies, and similar or derivative works to any of the foregoing, (vi) all documentation and materials related to any of the foregoing, (vii) all other goods, services or deliverables to be provided by or on behalf of Supplier under the Contract and (viii) all Intellectual Property Rights in any of the foregoing, and which are or were created,

prepared, developed, invented or conceived for the use of benefit of Customer in connection with this Contract or with funds appropriated by or for Customer or Customer's benefit (a) by any Supplier personnel or Customer personnel or (b) any Customer personnel who then became personnel to Supplier or any of its affiliates or subcontractors, where, although creation or reduction-to-practice is completed while the person is affiliated with Supplier or its personnel, any portion of same was created, invented or conceived by such person while affiliated with Customer.

5 Pricing

- 5.1** Pursuant to 68 O.S. §§ 1352, 1356, and 1404, State agencies are exempt from the assessment of State sales, use, and excise taxes. Further, State agencies and political subdivisions of the State are exempt from Federal Excise Taxes pursuant to Title 26 of the United States Code. Any taxes of any nature whatsoever payable by the Supplier shall not be reimbursed.
- 5.2** Pursuant to 74 O.S. §85.40, all travel expenses of Supplier must be included in the total Acquisition price.
- 5.3** The price of a product offered under the Contract shall include and Supplier shall prepay all shipping, packaging, delivery and handling fees. All product deliveries will be free on board Customer's Destination. No additional fees shall be charged by Supplier for standard shipping and handling. If Customer requests expedited or special delivery, Customer may be responsible for any charges for expedited or special delivery.

6 Ordering, Inspection, and Acceptance

- 6.1** Any product or service furnished under the Contract shall be ordered by issuance of a valid purchase order or other appropriate payment mechanism, including a pre-encumbrance, or by use of a valid Purchase Card. All orders and transactions are governed by the terms and conditions of the Contract. Any purchase order or other applicable payment mechanism dated prior to termination or expiration of the Contract shall be performed unless mutually agreed in writing otherwise.
- 6.2** Services will be performed in accordance with industry best practices and are subject to acceptance by the Customer. Notwithstanding any other provision in the Contract, deemed acceptance of a service or associated deliverable shall not apply automatically upon receipt of a deliverable or upon provision of a service.

Supplier warrants and represents that a product or deliverable furnished by or through the Supplier shall individually, and where specified by Supplier to perform as a system, be substantially uninterrupted and error-free in operation and guaranteed against faulty material and workmanship for a warranty period of the greater of ninety (90) days from the date of acceptance or the maximum allowed by the manufacturer. A defect in a product or deliverable furnished by or through the Supplier shall be repaired or replaced by Supplier at no additional cost or expense to the Customer if such defect occurs during the warranty period.

Any product to be delivered pursuant to the Contract shall be subject to final inspection and acceptance by the Customer at Destination. The Customer assumes no responsibility for a product until accepted by the Customer. Title and risk of loss or damage to a product shall be the responsibility of the Supplier until accepted. The Supplier shall be responsible for filing, processing, and collecting any and all damage claims accruing prior to acceptance.

Pursuant to OAC 260:115-9-5, payment for an Acquisition does not constitute final acceptance of the Acquisition. If subsequent inspection affirms that the Acquisition does not meet or exceed the specifications of the order or that the Acquisition has a latent defect, the Supplier shall be notified as soon as is reasonably practicable. The Supplier shall retrieve and replace the Acquisition at Supplier's expense or, if unable to replace, shall issue a refund to Customer. Refund under this section shall not be an exclusive remedy.

- 6.3 Supplier shall deliver products and services on or before the required date specified in a Contract Document. Failure to deliver timely may result in liquidated damages as set forth in the applicable Contract Document. Deviations, substitutions, or changes in a product or service, including changes of personnel directly providing services, shall not be made unless expressly authorized in writing by the Customer. Any substitution of personnel directly providing services shall be a person of comparable or greater skills, education and experience for performing the services as the person being replaced. Additionally, Supplier shall provide staff sufficiently experienced and able to perform with respect to any transitional services provided by Supplier in connection with termination or expiration of the Contract.
- 6.4 Product warranty and return policies and terms provided under any Contract Document will not be more restrictive or more costly than warranty and return policies and terms for other similarly situated customers for a like product.

7 Invoices and Payment

- 7.1** Supplier shall be paid upon submission of a proper invoice(s) at the prices stipulated in the Contract in accordance with 74 O.S. §85.44B which requires that payment be made only after products have been provided and accepted or services rendered and accepted.

The following terms additionally apply:

- A.** An invoice shall contain the purchase order number, description of products or services provided and the dates of such provision.
- B.** Failure to provide a timely and proper invoice may result in delay of processing the invoice for payment. Proper invoice is defined at OAC 260:10-1-2.
- C.** Payment of all fees under the Contract shall be due NET 45 days. Payment and interest on late payments are governed by 62 O.S. §34.72. Such interest is the sole and exclusive remedy for late payments by a State agency and no other late fees are authorized to be assessed pursuant to Oklahoma law.
- D.** The date from which an applicable early payment discount time is calculated shall be from the receipt date of a proper invoice. There is no obligation, however, to utilize an early payment discount.
- E.** If an overpayment or underpayment has been made to Supplier any subsequent payments to Supplier under the Contract may be adjusted to correct the account. A written explanation of the adjustment will be issued to Supplier.
- F.** Supplier shall have no right of setoff.
- G.** Because funds are typically dedicated to a particular fiscal year, an invoice will be paid only when timely submitted, which shall in no instance be later than six (6) months after the end of the fiscal year in which the goods are provided or services performed.
- H.** The Supplier shall accept payment by Purchase Card as allowed by Oklahoma law.

8 Maintenance of Insurance, Payment of Taxes, and Workers' Compensation

- 8.1** As a condition of this Contract, Supplier shall procure at its own expense, and provide proof of, insurance coverage with the applicable liability limits set

forth below and any approved subcontractor of Supplier shall procure and provide proof of the same coverage. The required insurance shall be underwritten by an insurance carrier with an A.M. Best rating of A- or better.

Such proof of coverage shall additionally be provided to the Customer if services will be provided by any of Supplier's employees, agents or subcontractors at any Customer premises and/or employer vehicles will be used in connection with performance of Supplier's obligations under the Contract. Supplier may not commence performance hereunder until such proof has been provided. Additionally, Supplier shall ensure each insurance policy includes a thirty (30) day notice of cancellation and name the State and its agencies as certificate holder and shall promptly provide proof to the State of any renewals, additions, or changes to such insurance coverage. Supplier's obligation to maintain insurance coverage under the Contract is a continuing obligation until Supplier has no further obligation under the Contract. Any combination of primary and excess or umbrella insurance may be used to satisfy the limits of coverage for Commercial General Liability, Auto Liability and Employers' Liability. Unless agreed between the parties and approved by the State Purchasing Director, the minimum acceptable insurance limits of liability are as follows:

- A.** Workers' Compensation and Employer's Liability Insurance in accordance with and to the extent required by applicable law;
- B.** Commercial General Liability Insurance covering the risks of personal injury, bodily injury (including death) and property damage, including coverage for contractual liability, with a limit of liability of not less than \$5,000,000 per occurrence;
- C.** Automobile Liability Insurance with limits of liability of not less than \$5,000,000 combined single limit each accident;
- D.** Directors and Officers Insurance which shall include Employment Practices Liability as well as Consultant's Computer Errors and Omissions Coverage, if information technology services are provided under the Contract, with limits not less than \$5,000,000 per occurrence;
- E.** Security and Privacy Liability insurance, including coverage for failure to protect confidential information and failure of the security of Supplier's computer systems that results in unauthorized access to Customer data with limits \$5,000,000 per occurrence; and
- F.** Additional coverage required in writing in connection with a particular Acquisition.

- 8.2** Supplier shall be entirely responsible during the existence of the Contract for the liability and payment of taxes payable by or assessed to Supplier or its employees, agents and subcontractors of whatever kind, in connection with the Contract. Supplier further agrees to comply with all state and federal laws applicable to any such persons, including laws regarding wages, taxes, insurance, and Workers' Compensation. Neither Customer nor the State shall be liable to the Supplier, its employees, agents, or others for the payment of taxes or the provision of unemployment insurance and/or Workers' Compensation or any benefit available to a State or Customer employee.
- 8.3** Supplier agrees to indemnify Customer, the State, and its employees, agents, representatives, contractors, and assignees for any and all liability, actions, claims, demands, or suits, and all related costs and expenses (including without limitation reasonable attorneys' fees and costs required to establish the right to indemnification) relating to tax liability, unemployment insurance and/or Workers' Compensation in connection with its performance under the Contract.

9 Compliance with Applicable Laws

- 9.1** As long as Supplier has an obligation under the terms of the Contract and in connection with performance of its obligations, the Supplier represents its present compliance, and shall have an ongoing obligation to comply, with all applicable federal, State, and local laws, rules, regulations, ordinances, and orders, as amended, including but not limited to the following:
- A.** Drug-Free Workplace Act of 1988 set forth at 41 U.S.C. §81.
 - B.** Section 306 of the Clean Air Act, Section 508 of the Clean Water Act, Executive Order 11738, and Environmental Protection Agency Regulations which prohibit the use of facilities included on the EPA List of Violating Facilities under nonexempt federal contracts, grants or loans;
 - C.** Prospective participant requirements set at 45 C.F.R. part 76 in connection with Debarment, Suspension and other responsibility matters;
 - D.** 1964 Civil Rights Act, Title IX of the Education Amendment of 1972, Section 504 of the Rehabilitation Act of 1973, Americans with Disabilities Act of 1990, and Executive Orders 11246 and 11375;
 - E.** Anti-Lobbying Law set forth at 31 U.S.C. §1325 and as implemented at 45 C.F.R. part 93;

- F.** Requirements of Internal Revenue Service Publication 1075 regarding use, access and disclosure of Federal Tax Information (as defined therein);
 - G.** Obtaining certified independent audits conducted in accordance with Government Auditing Standards and Office of Management and Budget Uniform Guidance, 2 CFR 200 Subpart F §200.500 et seq. with approval and work paper examination rights of the applicable procuring entity;
 - H.** Requirements of the Oklahoma Taxpayer and Citizen Protection Act of 2007, 25 O.S. §1312 and applicable federal immigration laws and regulations and be registered and participate in the Status Verification System. The Status Verification System is defined at 25 O.S. §1312, includes but is not limited to the free Employment Verification Program (E-Verify) through the Department of Homeland Security, and is available at www.dhs.gov/E-Verify;
 - I.** Requirements of the Health Insurance Portability and Accountability Act of 1996; Health Information Technology for Economic and Clinical Health Act; Payment Card Industry Security Standards; Criminal Justice Information System Security Policy and Security Addendum; and Family Educational Rights and Privacy Act; and
 - J.** Be registered as a business entity licensed to do business in the State, have obtained a sales tax permit, and be current on franchise tax payments to the State, as applicable.
- 9.2** The Supplier's employees, agents and subcontractors shall adhere to applicable Customer policies including, but not limited to acceptable use of Internet and electronic mail, facility and data security, press releases, and public relations. As applicable, the Supplier shall adhere to the State Information Security Policy, Procedures, Guidelines set forth at [Information Security Policy, Procedures, Guidelines \(oklahoma.gov\)](http://Information Security Policy, Procedures, Guidelines (oklahoma.gov)). Supplier is responsible for reviewing and relaying such policies covering the above to the Supplier's employees, agents and subcontractors.
- 9.3** At no additional cost to Customer, the Supplier shall maintain all applicable licenses and permits required in association with its obligations under the Contract.
- 9.4** In addition to compliance under subsection 9.1 above, Supplier shall have a continuing obligation to comply with applicable Customer-specific mandatory

contract provisions required in connection with the receipt of federal funds or other funding source.

- 9.5** The Supplier is responsible to review and inform its employees, agents, and subcontractors who provide a product or perform a service under the Contract of the Supplier's obligations under the Contract and Supplier certifies that its employees and each such subcontractor shall comply with minimum requirements and applicable provisions of the Contract. At the request of the State, Supplier shall promptly provide adequate evidence that such persons are its employees, agents or approved subcontractors and have been informed of their obligations under the Contract.
- 9.6** As applicable, Supplier agrees to comply with the Governor's Executive Orders related to the use of any tobacco product, electronic cigarette or vaping device on any and all properties owned, leased, or contracted for use by the State, including but not limited to all buildings, land and vehicles owned, leased, or contracted for use by agencies or instrumentalities of the State.
- 9.7** The execution, delivery and performance of the Contract and any ancillary documents by Supplier will not, to the best of Supplier's knowledge, violate, conflict with, or result in a breach of any provision of, or constitute a default (or an event which, with notice or lapse of time or both, would constitute a default) under, or result in the termination of, any written contract or other instrument between Supplier and any third party.
- 9.8** Supplier represents that it has the ability to pay its debts when due and it does not anticipate the filing of a voluntary or involuntary bankruptcy petition or appointment of a receiver, liquidator or trustee.
- 9.9** Supplier represents that, to the best of its knowledge, any litigation or claim or any threat thereof involving Supplier has been disclosed in writing to the State and Supplier is not aware of any other litigation, claim or threat thereof.
- 9.10** If services provided by Supplier include delivery of an electronic communication, Supplier shall ensure such communication and any associated support documents are compliant with Section 508 of the Federal Rehabilitation Act and with State standards regarding accessibility. Should any communication or associated support documents be non-compliant, Supplier shall correct and re-deliver such communication immediately upon discovery or notice, at no additional cost to the State. Additionally, as part of compliance with accessibility requirements where documents are only provided in non-electronic format, Supplier shall promptly provide such communication and any associated support documents in an alternate format

usable by individuals with disabilities upon request and at no additional cost, which may originate from an intended recipient or from the State.

10 Audits and Records Clause

- 10.1** As used in this clause and pursuant to 67 O.S. §203, “record” includes a document, book, paper, photograph, microfilm, computer tape, disk, record, sound recording, film recording, video record, accounting procedures and practices, and other data, regardless of type and regardless of whether such items are in written form, in the form of computer data, or in any other form. Supplier agrees any pertinent federal or State agency or governing entity of a Customer shall have the right to examine and audit, at no additional cost to a Customer, all records relevant to the execution and performance of the Contract except, unless otherwise agreed, costs of Supplier that comprise pricing under the Contract.
- 10.2** The Supplier is required to retain records relative to the Contract for the duration of the Contract and for a period of seven (7) years following completion or termination of an Acquisition unless otherwise indicated in the Contract terms. If a claim, audit, litigation or other action involving such records is started before the end of the seven-year period, the records are required to be maintained for two (2) years from the date that all issues arising out of the action are resolved, or until the end of the seven (7) year retention period, whichever is later.
- 10.3** Pursuant to 74 O.S. §85.41, if professional services are provided hereunder, all items of the Supplier that relate to the professional services are subject to examination by the State agency, State Auditor and Inspector and the State Purchasing Director.

11 Confidentiality

- 11.1** The Supplier shall maintain strict security of all State and citizen data and records entrusted to it or to which the Supplier gains access, in accordance with and subject to applicable federal and State laws, rules, regulations, and policies and shall use any such data and records only as necessary for Supplier to perform its obligations under the Contract. The Supplier further agrees to evidence such confidentiality obligation in a separate writing if required under such applicable federal or State laws, rules and regulations. The Supplier warrants and represents that such information shall not be sold, assigned, conveyed, provided, released, disseminated or otherwise disclosed by Supplier, its employees, officers, directors, subsidiaries, affiliates, agents, representatives, assigns, subcontractors, independent contractors, successor or any other persons or entities without Customer’s prior express written

permission. Supplier shall instruct all such persons and entities that the confidential information shall not be disclosed or used without the Customer's prior express written approval except as necessary for Supplier to render services under the Contract. The Supplier further warrants that it has a tested and proven system in effect designed to protect all confidential information.

- 11.2** Supplier shall establish, maintain and enforce agreements with all such persons and entities that have access to State and citizen data and records to fulfill Supplier's duties and obligations under the Contract and to specifically prohibit any sale, assignment, conveyance, provision, release, dissemination or other disclosure of any State or citizen data or records except as required by law or allowed by written prior approval of the Customer.
- 11.3** Supplier shall immediately report to the Customer any and all unauthorized use, appropriation, sale, assignment, conveyance, provision, release, access, acquisition, disclosure or other dissemination of any State or citizen data or records of which it or its parent company, subsidiaries, affiliates, employees, officers, directors, assignees, agents, representatives, independent contractors, and subcontractors is aware or have knowledge or reasonable should have knowledge. The Supplier shall also promptly furnish to Customer full details of the unauthorized use, appropriation, sale, assignment, conveyance, provision, release, access, acquisition, disclosure or other dissemination, or attempt thereof, and use its best efforts to assist the Customer in investigating or preventing the reoccurrence of such event in the future. The Supplier shall cooperate with the Customer in connection with any litigation and investigation deemed necessary by the Customer to protect any State or citizen data and records and shall bear all costs associated with the investigation, response and recovery in connection with any breach of State or citizen data or records including but not limited to credit monitoring services with a term of at least three (3) years, all notice-related costs and toll free telephone call center services.
- 11.4** Supplier further agrees to promptly prevent a reoccurrence of any unauthorized use, appropriation, sale, assignment, conveyance, provision, release, access, acquisition, disclosure or other dissemination of State or citizen data and records.
- 11.5** Supplier acknowledges that any improper use, appropriation, sale, assignment, conveyance, provision, release, access, acquisition, disclosure or other dissemination of any State data or records to others may cause immediate and irreparable harm to the Customer and certain beneficiaries and may violate state or federal laws and regulations. If the Supplier or its affiliates, parent company, subsidiaries, employees, officers, directors, assignees, agents,

representatives, independent contractors, and subcontractors improperly use, appropriate, sell, assign, convey, provide, release, access, acquire, disclose or otherwise disseminate such confidential information to any person or entity in violation of the Contract, the Customer will immediately be entitled to injunctive relief and/or any other rights or remedies available under this Contract, at equity or pursuant to applicable statutory, regulatory, and common law without a cure period.

11.6 The Supplier shall immediately forward to the State Purchasing Director, and any other applicable person listed in the Notices section(s) of the Contract, any request by a third party for data or records in the possession of the Supplier or any subcontractor or to which the Supplier or subcontractor has access and Supplier shall fully cooperate with all efforts to protect the security and confidentiality of such data or records in response to a third party request.

11.7 Customer may be provided access to Supplier Confidential Information. State agencies are subject to the Oklahoma Open Records Act and Supplier acknowledges information marked confidential information will be disclosed to the extent permitted under the Open Records Act and in accordance with this section. Nothing herein is intended to waive the State Purchasing Director's authority under OAC 260:115-3-9 in connection with Bid information requested to be held confidential by a Bidder. Notwithstanding the foregoing, Supplier Confidential Information shall not include information that: (i) is or becomes generally known or available by public disclosure, commercial use or otherwise and is not in contravention of this Contract; (ii) is known and has been reduced to tangible form by the receiving party before the time of disclosure for the first time under this Contract and without other obligations of confidentiality; (iii) is independently developed without the use of any of Supplier Confidential Information; (iv) is lawfully obtained from a third party (without any confidentiality obligation) who has the right to make such disclosure or (v) résumé, pricing or marketing materials provided to the State. In addition, the obligations in this section shall not apply to the extent that the applicable law or regulation requires disclosure of Supplier Confidential Information, provided that the Customer provides reasonable written notice, pursuant to Contract notice provisions, to the Supplier so that the Supplier may promptly seek a protective order or other appropriate remedy.

12 Conflict of Interest

In addition to any requirement of law or of a professional code of ethics or conduct, the Supplier, its employees, agents and subcontractors are required to disclose any outside activity or interest that conflicts or may conflict with the best interest of the State. Prompt disclosure is required under this section if the activity or interest is

related, directly or indirectly, to any person or entity currently under contract with or seeking to do business with the State, its employees or any other third-party individual or entity awarded a contract with the State. Further, as long as the Supplier has an obligation under the Contract, any plan, preparation or engagement in any such activity or interest shall not occur without prior written approval of the State. Any conflict of interest shall, at the sole discretion of the State, be grounds for partial or whole termination of the Contract.

13 Assignment and Permitted Subcontractors

- 13.1** Supplier's obligations under the Contract may not be assigned or transferred to any other person or entity without the prior written consent of the State which may be withheld at the State's sole discretion. Should Supplier assign its rights to payment, in whole or in part, under the Contract, Supplier shall provide the State and all affected Customers with written notice of the assignment. Such written notice shall be delivered timely and contain details sufficient for affected Customers to perform payment obligations without any delay caused by the assignment.
- 13.2** Notwithstanding the foregoing, the Contract may be assigned by Supplier to any corporation or other entity in connection with a merger, consolidation, sale of all equity interests of the Supplier, or a sale of all or substantially all of the assets of the Supplier to which the Contract relates. In any such case, said corporation or other entity shall by operation of law or expressly in writing assume all obligations of the Supplier as fully as if it had been originally made a party to the Contract. Supplier shall give the State and all affected Customers prior written notice of said assignment. Any assignment or delegation in violation of this subsection shall be void.
- 13.3** If the Supplier is permitted to utilize subcontractors in support of the Contract, the Supplier shall remain solely responsible for its obligations under the terms of the Contract, for its actions and omissions and those of its agents, employees and subcontractors and for payments to such persons or entities. Prior to a subcontractor being utilized by the Supplier, the Supplier shall obtain written approval of the State of such subcontractor and each employee, as applicable to a particular Acquisition, of such subcontractor proposed for use by the Supplier. Such approval is within the sole discretion of the State. Any proposed subcontractor shall be identified by entity name, and by employee name, if required by the particular Acquisition, in the applicable proposal and shall include the nature of the services to be performed. As part of the approval request, the Supplier shall provide a copy of a written agreement executed by the Supplier and subcontractor setting forth that such subcontractor is bound by and agrees, as applicable, to perform the same covenants and be subject to

the same conditions and make identical certifications to the same facts and criteria, as the Supplier under the terms of all applicable Contract Documents. Supplier agrees that maintaining such agreement with any subcontractor and obtaining prior written approval by the State of any subcontractor and associated employees shall be a continuing obligation. The State further reserves the right to revoke approval of a subcontractor or an employee thereof in instances of poor performance, misconduct or for other similar reasons.

13.4 All payments under the Contract shall be made directly to the Supplier, except as provided in subsection A above regarding the Supplier's assignment of payment. No payment shall be made to the Supplier for performance by unapproved or disapproved employees of the Supplier or a subcontractor.

13.5 Rights and obligations of the State or a Customer under the terms of this Contract may be assigned or transferred, at no additional cost, to other Customer entities.

14 Background Checks and Criminal History Investigations

Prior to the commencement of any services, background checks and criminal history investigations of the Supplier's employees and subcontractors who will be providing services may be required and, if so, the required information shall be provided to the State in a timely manner. Supplier's access to facilities, data and information may be withheld prior to completion of background verification acceptable to the State. The costs of additional background checks beyond Supplier's normal hiring practices shall be the responsibility of the Customer unless such additional background checks are required solely because Supplier will not provide results of its otherwise acceptable normal background checks; in such an instance, Supplier shall pay for the additional background checks. Supplier will coordinate with the State and its employees to complete the necessary background checks and criminal history investigations. Should any employee or subcontractor of the Supplier who will be providing services under the Contract not be acceptable as a result of the background check or criminal history investigation, the Customer may require replacement of the employee or subcontractor in question and, if no suitable replacement is made within a reasonable time, terminate the purchase order or other payment mechanism associated with the project or services.

15 Patents and Copyrights

Without exception, a product or deliverable price shall include all royalties or costs owed by the Supplier to any third party arising from the use of a patent, intellectual property, copyright or other property right held by such third party. Should any third party threaten or make a claim that any portion of a product or service provided by Supplier under the Contract infringes that party's patent, intellectual property,

copyright or other property right, Supplier shall enable each affected Customer to legally continue to use, or modify for use, the portion of the product or service at issue or replace such potentially infringing product, or re-perform or redeliver in the case of a service, with at least a functional non-infringing equivalent. Supplier's duty under this section shall extend to include any other product or service rendered materially unusable as intended due to replacement or modification of the product or service at issue. If the Supplier determines that none of these alternatives are reasonably available, the State shall return such portion of the product or deliverable at issue to the Supplier, upon written request, in exchange for a refund of the price paid for such returned goods as well as a refund or reimbursement, if applicable, of the cost of any other product or deliverable rendered materially unusable as intended due to removal of the portion of product or deliverable at issue. Any remedy provided under this section is not an exclusive remedy and is not intended to operate as a waiver of legal or equitable remedies because of acceptance of relief provided by Supplier.

16 Indemnification

16.1 Acts or Omissions

- A.** Supplier shall defend and indemnify the Indemnified Parties, as applicable, for any and all liability, claims, damages, losses, costs, expenses, demands, suits and actions of third parties (including without limitation reasonable attorneys' fees and costs required to establish the right to indemnification) arising out of, or resulting from any action or claim for bodily injury, death, or property damage brought against any of the Indemnified parties to the extent arising from any negligent act or omission or willful misconduct of the Supplier or its agents, employees, or subcontractors in the execution or performance of the Contract.
- B.** To the extent Supplier is found liable for loss, damage, or destruction of any property of Customer due to negligence, misconduct, wrongful act, or omission on the part of the Supplier, its employees, agents, representatives, or subcontractors, the Supplier and Customer shall use best efforts to mutually negotiate an equitable settlement amount to repair or replace the property unless such loss, damage or destruction is of such a magnitude that repair or replacement is not a reasonable option. Such amount shall be invoiced to, and is payable by, Supplier sixty (60) calendar days after the date of Supplier's receipt of an invoice for the negotiated settlement amount.

16.2 Infringement

Supplier shall indemnify the Indemnified Parties, as applicable, for all liability, claims, damages, losses, costs, expenses, demands, suits and actions of third parties (including without limitation reasonable attorneys' fees and costs required to establish the right to indemnification) arising from or in connection with Supplier's breach of its representations and warranties in the Contract or alleged infringement of any patent, intellectual property, copyright or other property right in connection with a product or service provided under the Contract. Supplier's duty under this section is reduced to the extent a claimed infringement results from: (a) a Customer's or user's content; (b) modifications by Customer or third party to a product delivered under the Contract or combinations of the product with any non-Supplier-provided services or products unless Supplier recommended or participated in such modification or combination; (c) use of a product or service by Customer in violation of the Contract unless done so at the direction of Supplier, or (d) a non-Supplier product that has not been provided to the State by, through or on behalf of Supplier as opposed to its combination with products Supplier provides to or develops for the State or a Customer as a system.

16.3 Notice and Cooperation

In connection with indemnification obligations under the Contract, the parties agree to furnish prompt written notice to each other of any third-party claim. Any Customer affected by the claim will reasonably cooperate with Supplier and defense of the claim to the extent its interests are aligned with Supplier. Supplier shall use counsel reasonably experienced in the subject matter at issue and will not settle a claim without the written consent of the party being defended, which consent will not be unreasonably withheld or delayed, except that no consent will be required to settle a claim against Indemnified Parties that are not a State agency, where relief against the Indemnified Parties is limited to monetary damages that are paid by the defending party under indemnification provisions of the Contract.

16.4 Coordination of Defense

In connection with indemnification obligations under the Contract, when a State agency is a named defendant in any filed or threatened lawsuit, the defense of the State agency shall be coordinated by the Attorney General of Oklahoma, or the Attorney General may authorize the Supplier to control the defense and any related settlement negotiations; provided, however, Supplier shall not agree to any settlement of claims against the State without obtaining advance written concurrence from the Attorney General. If the Attorney General does not authorize sole control of the defense and settlement negotiations to Supplier, Supplier shall have authorization to equally

participate in any proceeding related to the indemnity obligation under the Contract and shall remain responsible to indemnify the applicable Indemnified Parties.

16.5 Limitation of Liability

- A.** With respect to any claim or cause of action arising under or related to the Contract, neither the State nor any Customer shall be liable to Supplier for lost profits, lost sales or business expenditures, investments, or commitments in connection with any business, loss of any goodwill, or for any other indirect, incidental, punitive, special or consequential damages, even if advised of the possibility of such damages.
- B.** Notwithstanding anything to the contrary in the Contract, no provision shall limit damages, expenses, costs, actions, claims, and liabilities arising from or related to property damage, bodily injury or death caused by Supplier or its employees, agents or subcontractors; indemnity, security or confidentiality obligations under the Contract; the bad faith, negligence, intentional misconduct or other acts for which applicable law does not allow exemption from liability of Supplier or its employees, agents or subcontractors.
- C.** The limitation of liability and disclaimers set forth in the Contract will apply regardless of whether Customer has accepted a product or service. The parties agree that Supplier has set its fees and entered into the Contract in reliance on the disclaimers and limitations set forth herein, that the same reflect an allocation of risk between the parties and form an essential basis of the bargain between the parties. These limitations shall apply notwithstanding any failure of essential purpose of any limited remedy.

17 Termination for Funding Insufficiency

- 17.1** Notwithstanding anything to the contrary in any Contract Document, the State may terminate the Contract in whole or in part if funds sufficient to pay obligations under the Contract are not appropriated or received from an intended third-party funding source. In the event of such insufficiency, Supplier will be provided at least fifteen (15) calendar days' written notice of termination. Any partial termination of the Contract under this section shall not be construed as a waiver of, and shall not affect, the rights and obligations of any party regarding portions of the Contract that are not terminated. The determination by the State of insufficient funding shall be accepted by, and shall be final and binding on, the Supplier.

- 17.2** Upon receipt of notice of a termination, Supplier shall immediately comply with the notice terms and take all necessary steps to minimize the incurrence of costs allocable to the work affected by the notice. If a purchase order or other payment mechanism has been issued and a product or service has been accepted as satisfactory prior to the effective date of termination, the termination does not relieve an obligation to pay for the product or service but there shall not be any liability for further payments ordinarily due under the Contract or for any damages or other amounts caused by or associated with such termination. Any amount paid to Supplier in the form of prepaid fees that are unused when the Contractor certain obligations are terminated shall be refunded.
- 17.3** The State's exercise of its right to terminate the Contract under this section shall not be considered a default or breach under the Contract or relieve the Supplier of any liability for claims arising under the Contract.

18 Termination for Cause

- 18.1** Supplier may terminate the Contract if (i) it has provided the State with written notice of material breach and (ii) the State fails to cure such material breach within thirty (30) days of receipt of written notice. If there is more than one Customer, material breach by a Customer does not give rise to a claim of material breach as grounds for termination by Supplier of the Contract as a whole. The State may terminate the Contract in whole or in part if (i) it has provided Supplier with written notice of material breach, and (ii) Supplier fails to cure such material breach within thirty (30) days of receipt of written notice. Any partial termination of the Contract under this section shall not be construed as a waiver of, and shall not affect, the rights and obligations of any party regarding portions of the Contract that are not terminated.
- 18.2** The State may terminate the Contract in whole or in part immediately without a thirty (30) day written notice to Supplier if (i) Supplier fails to comply with confidentiality, privacy, security, environmental or safety requirements applicable to Supplier's performance or obligations under the Contract; (ii) Supplier's material breach is reasonably determined to be an impediment to the function of the State and detrimental to the State or to cause a condition precluding the thirty (30) day notice or (iii) when the State determines that an administrative error in connection with award of the Contract occurred prior to Contract performance.
- 18.3** Upon receipt of notice of a termination, Supplier shall immediately comply with the notice terms and take all necessary steps to minimize the incurrence

of costs allocable to the work affected by the notice. If a purchase order or other payment mechanism has been issued and a product or service has been accepted as satisfactory prior to the effective date of termination, the termination does not relieve an obligation to pay for the product or service but there shall not be any liability for further payments ordinarily due under the Contract or for any damages or other amounts caused by or associated with such termination. Such termination is not an exclusive remedy but is in addition to any other rights and remedies provided for by law. Any amount paid to Supplier in the form of prepaid fees that are unused when the Contract or certain obligations are terminated shall be refunded. Termination of the Contract under this section, in whole or in part, shall not relieve the Supplier of liability for claims arising under the Contract.

- 18.4** The Supplier's repeated failure to provide an acceptable product or service; Supplier's unilateral revision of linked or supplemental terms that have a materially adverse impact on a Customer's rights or obligations under the Contract (except as required by a governmental authority); actual or anticipated failure of Supplier to perform its obligations under the Contract; Supplier's inability to pay its debts when due; assignment for the benefit of Supplier's creditors; or voluntary or involuntary appointment of a receiver or filing of bankruptcy of Supplier shall constitute a material breach of the Supplier's obligations, which may result in partial or whole termination of the Contract. This subsection is not intended as an exhaustive list of material breach conditions. Termination may also result from other instances of failure to adhere to the Contract provisions and for other reasons provided for by applicable law, rules or regulations; without limitation, OAC 260:115-9-9 is an example.

19 Termination for Convenience

- 19.1** The State may terminate the Contract, in whole or in part, for convenience if it is determined that termination is in the State's best interest. In the event of a termination for convenience, Supplier will be provided at least thirty (30) days' written notice of termination. Any partial termination of the Contract shall not be construed as a waiver of, and shall not affect, the rights and obligations of any party regarding portions of the Contract that remain in effect.
- 19.2** Upon receipt of notice of such termination, Supplier shall immediately comply with the notice terms and take all necessary steps to minimize the incurrence of costs allocable to the work affected by the notice. If a purchase order or other payment mechanism has been issued and a product or service has been accepted as satisfactory prior to the effective date of termination, the termination does not relieve an obligation to pay for the product or service but

there shall not be any liability for further payments ordinarily due under the Contract or for any damages or other amounts caused by or associated with such termination. Such termination shall not be an exclusive remedy but shall be in addition to any other rights and remedies provided for by law. Any amount paid to Supplier in the form of prepaid fees that are unused when the Contract or certain obligations are terminated shall be refunded. Termination of the Contract under this section, in whole or in part, shall not relieve the Supplier of liability for claims arising under the Contract.

20 Suspension of Supplier

- 20.1** Supplier may be subject to Suspension without advance notice and may additionally be suspended from activities under the Contract if Supplier fails to comply with confidentiality, privacy, security, environmental or safety requirements applicable to Supplier's performance or obligations under the Contract.
- 20.2** Upon receipt of a notice pursuant to this section, Supplier shall immediately comply with the notice terms and take all necessary steps to minimize the incurrence of costs allocable to the work affected by the notice. If a purchase order or other payment mechanism has been issued and a product or service has been accepted as satisfactory prior to receipt of notice by Supplier, the Suspension does not relieve an obligation to pay for the product or service but there shall not be any liability for further payments ordinarily due under the Contract during a period of Suspension or suspended activity or for any damages or other amounts caused by or associated with such Suspension or suspended activity. A right exercised under this section shall not be an exclusive remedy but shall be in addition to any other rights and remedies provided for by law. Any amount paid to Supplier in the form of prepaid fees attributable to a period of Suspension or suspended activity shall be refunded.
- 20.3** Such Suspension may be removed, or suspended activity may resume, at the earlier of such time as a formal notice is issued that authorizes the resumption of performance under the Contract or at such time as a purchase order or other appropriate encumbrance document is issued. This subsection is not intended to operate as an affirmative statement that such resumption will occur.

21 Certification Regarding Debarment, Suspension, and Other Responsibility Matters

The certification made by Supplier with respect to Debarment, Suspension, certain indictments, convictions, civil judgments and terminated public contracts is a material representation of fact upon which reliance was placed when entering into the Contract.

A determination that Supplier knowingly rendered an erroneous certification, in addition to other available remedies, may result in whole or partial termination of the Contract for Supplier's default. Additionally, Supplier shall promptly provide written notice to the State Purchasing Director if the certification becomes erroneous due to changed circumstances.

22 Certification Regarding State Employees Prohibition From Fulfilling Services

Pursuant to 74 O.S. § 85.42, the Supplier certifies that no person involved in any manner in development of the Contract employed by the State shall be employed to fulfill any services provided under the Contract.

23 Force Majeure

23.1 Either party shall be temporarily excused from performance to the extent delayed as a result of unforeseen causes beyond its reasonable control including fire or other similar casualty, act of God, strike or labor dispute, war or other violence, or any law, order or requirement of any governmental agency or authority provided the party experiencing the force majeure event has prudently and promptly acted to take any and all steps within the party's control to ensure continued performance and to shorten duration of the event. If a party's performance of its obligations is materially hindered as a result of a force majeure event, such party shall promptly notify the other party of its best reasonable assessment of the nature and duration of the force majeure event and steps it is taking, and plans to take, to mitigate the effects of the force majeure event. The party shall use commercially reasonable best efforts to continue performance to the extent possible during such event and resume full performance as soon as reasonably practicable.

23.2 Subject to the conditions set forth above, non-performance as a result of a force majeure event shall not be deemed a default. However, a purchase order or other payment mechanism may be terminated if Supplier cannot cause delivery of a product or service in a timely manner to meet the business needs of Customer. Supplier is not entitled to payment for products or services not received and, therefore, amounts payable to Supplier during the force majeure event shall be equitably adjusted downward.

23.3 Notwithstanding the foregoing or any other provision in the Contract, (i) the following are not a force majeure event under the Contract: (a) shutdowns, disruptions or malfunctions in Supplier's system or any of Supplier's telecommunication or internet services other than as a result of general and widespread internet or telecommunications failures that are not limited to Supplier's systems or (b) the delay or failure of Supplier or subcontractor personnel to perform any obligation of Supplier hereunder unless such delay

or failure to perform is itself by reason of a force majeure event and (ii) no force majeure event modifies or excuses Supplier's obligations related to confidentiality, indemnification, data security or breach notification obligations set forth herein.

24 Security of Property and Personnel

In connection with Supplier's performance under the Contract, Supplier may have access to Customer personnel, premises, data, records, equipment and other property. Supplier shall use commercially reasonable best efforts to preserve the safety and security of such personnel, premises, data, records, equipment, and other property of Customer. Supplier shall be responsible for damage to such property to the extent such damage is caused by its employees or subcontractors and shall be responsible for loss of Customer property in its possession, regardless of cause. If Supplier fails to comply with Customer's security requirements, Supplier is subject to immediate suspension of work as well as termination of the associated purchase order or other payment mechanism.

25 Notices

All notices, approvals or requests allowed or required by the terms of any Contract Document shall be in writing, reference the Contract with specificity and deemed delivered upon receipt or upon refusal of the intended party to accept receipt of the notice. In addition to other notice requirements in the Contract and the designated Supplier contact provided in a successful Bid, notices shall be sent to the State at the physical address set forth below. Notice information may be updated in writing to the other party as necessary. Notwithstanding any other provision of the Contract, confidentiality, breach and termination-related notices shall not be delivered solely via e-mail.

If sent to the State:

State Purchasing Director
2401 North Lincoln Boulevard, Suite 116
Oklahoma City, Oklahoma 73105

With a copy, which shall not constitute notice, to:

Purchasing Division Deputy General Counsel
2401 North Lincoln Boulevard, Suite 116
Oklahoma City, Oklahoma 73105

26 Miscellaneous

26.1 Choice of Law and Venue

Any claim, dispute, or litigation relating to the Contract Documents, in the singular or in the aggregate, shall be governed by the laws of the State without regard to application of choice of law principles. Pursuant to 74 O.S. §85.14, where federal granted funds are involved, applicable federal laws, rules and regulations shall govern to the extent necessary to insure benefit of such federal funds to the State. Venue for any action, claim, dispute, or litigation relating in any way to the Contract Documents, shall be in Oklahoma County, Oklahoma.

26.2 No Guarantee of Products or Services Required

The State shall not guarantee any minimum or maximum amount of Supplier products or services required under the Contract.

26.3 Employment Relationship

The Contract does not create an employment relationship. Individuals providing products or performing services pursuant to the Contract are not employees of the State or Customer and, accordingly are not eligible for any rights or benefits whatsoever accruing to such employees.

26.4 Transition Services

If transition services are needed at the time of Contract expiration or termination, Supplier shall provide such services on a month-to-month basis, at the contract rate or other mutually agreed rate. Supplier shall provide a proposed transition plan, upon request, and cooperate with any successor supplier and with establishing a mutually agreeable transition plan. Failure to cooperate may be documented as poor performance of Supplier.

26.5 Publicity

The existence of the Contract or any Acquisition is in no way an endorsement of Supplier, the products or services and shall not be so construed by Supplier in any advertising or publicity materials. Supplier agrees to submit to the State all advertising, sales, promotion, and other publicity matters relating to the Contract wherein the name of the State or any Customer is mentioned or language used from which, in the State's judgment, an endorsement may be inferred or implied. Supplier further agrees not to publish or use such advertising, sales promotion, or publicity matter or release any informational pamphlets, notices, press releases, research reports, or similar public notices concerning the Contract or any Acquisition hereunder without obtaining the prior written approval of the State.

26.6 Open Records Act

Supplier acknowledges that all State agencies and certain other Customers are subject to the Oklahoma Open Records Act set forth at 51 O.S. §24A-1 *et seq.* Supplier also acknowledges that compliance with the Oklahoma Open Records Act and all opinions of the Oklahoma Attorney General concerning the Act is required.

26.7 Failure to Enforce

Failure by the State or a Customer at any time to enforce a provision of, or exercise a right under, the Contract shall not be construed as a waiver of any such provision. Such failure to enforce or exercise shall not affect the validity of any Contract Document, or any part thereof, or the right of the State or a Customer to enforce any provision of, or exercise any right under, the Contract at any time in accordance with its terms. Likewise, a waiver of a breach of any provision of a Contract Document shall not affect or waive a subsequent breach of the same provision or a breach of any other provision in the Contract.

26.8 Mutual Responsibilities

- A.** No party to the Contract grants the other the right to use any trademarks, trade names, other designations in any promotion or publication without the express written consent by the other party.
- B.** The Contract is a non-exclusive contract and each party is free to enter into similar agreements with others.
- C.** The Customer and Supplier each grant the other only the licenses and rights specified in the Contract and all other rights and interests are expressly reserved.
- D.** The Customer and Supplier shall reasonably cooperate with each other and any Supplier to which the provision of a product and/or service under the Contract may be transitioned after termination or expiration of the Contract.
- E.** Except as otherwise set forth herein, where approval, acceptance, consent, or similar action by a party is required under the Contract, such action shall not be unreasonably delayed or withheld.

26.9 Invalid Term or Condition

To the extent any term or condition in the Contract conflicts with a compulsory applicable State or United States law or regulation, such Contract term or

condition is void and unenforceable. By executing any Contract Document which contains a conflicting term or condition, no representation or warranty is made regarding the enforceability of such term or condition. Likewise, any applicable State or federal law or regulation which conflicts with the Contract or any non-conflicting applicable State or federal law or regulation is not waived.

26.10 Severability

If any provision of a Contract Document, or the application of any term or condition to any party or circumstances, is held invalid or unenforceable for any reason, the remaining provisions shall continue to be valid and enforceable and the application of such provision to other parties or circumstances shall remain valid and in full force and effect. If a court finds that any provision of this contract is invalid or unenforceable, but that by limiting such provision it would become valid and enforceable, then such provision shall be deemed to be written, construed, and enforced as so limited.

26.11 Section Headings

The headings used in any Contract Document are for convenience only and do not constitute terms of the Contract.

26.12 Sovereign Immunity

Notwithstanding any provision in the Contract, the Contract is entered into subject to the State's Constitution, statutes, common law, regulations, and the doctrine of sovereign immunity, none of which are waived by the State nor any other right or defense available to the State.

26.13 Survival

As applicable, performance under all license, subscription, service agreements, statements of work, transition plans and other similar Contract Documents entered into between the parties under the terms of the Contract shall survive Contract expiration. Additionally, rights and obligations under the Contract which by their nature should survive including, without limitation, certain payment obligations invoiced prior to expiration or termination; confidentiality obligations; security incident and data breach obligations and indemnification obligations, remain in effect after expiration or termination of the Contract.

26.14 Entire Agreement

The Contract Documents taken together as a whole constitute the entire agreement between the parties. No statement, promise, condition,

understanding, inducement or representation, oral or written, expressed or implied, which is not contained in a Contract Document shall be binding or valid. The Supplier's representations and certifications, including any completed electronically, are incorporated by reference into the Contract.

26.15 Gratuities

The Contract may be immediately terminated, in whole or in part, by written notice if it is determined that the Supplier, its employee, agent, or another representative violated any federal, State or local law, rule or ordinance by offering or giving a gratuity to any State employee directly involved in the Contract. In addition, Suspension or Debarment of the Supplier may result from such a violation.

26.16 Import/Export Controls

Neither party will use, distribute, transfer or transmit any equipment, services, software or technical information provided under the Contract (even if incorporated into other products) except in compliance with all applicable import and export laws, conventions and regulations.

ATTACHMENT C

OKLAHOMA STATEWIDE CONTRACT TERMS

1. Statewide Contract Type

- 1.1** The Contract is a non-mandatory statewide contract for use by State agencies. Additionally, the Contract may be used by any governmental entity specified as a political subdivision of the State pursuant to the Governmental Tort Claims Act including any associated institution, instrumentality, board, commission, committee, department or other entity designated to act on behalf of the political subdivision; a state, county or local governmental entity in its state of origin; and entities authorized to utilize contracts by the State via a multistate or multigovernmental contract.
- 1.2** The Contract is a firm, fixed price contract for indefinite delivery and quantity for the Acquisitions available under the Contract.

2. Orders and Addendums

- 2.1** Unless mutually agreed in writing otherwise, orders shall be placed directly with the Supplier by issuance of written purchase orders or by Purchase Card by state agencies and other authorized entities. All orders are subject to the Contract terms and any order dated prior to Contract expiration shall be performed. Delivery to multiple destinations may be required.
- 2.2** Any ordering document shall be effective between Supplier and the Customer only and shall not be an Addendum to the Contract in its entirety or apply to any Acquisition by another Customer.
- 2.3** Additional terms added to a Contract Document by a Customer shall be effective if the additional terms do not conflict with the General Terms and are acceptable to Supplier. However, an Addendum to the Contract shall be signed by the State Purchasing Director or designee. Regarding information technology and telecommunications contracts, pursuant to 62 O.S., §34.11.1, the Chief Information Officer acts as the Information Technology and Telecommunications Purchasing Director.

3. Termination for Funding Insufficiency

In addition to Contract terms relating to termination due to insufficient funding, a Customer may terminate any purchase order or other payment mechanism if funds sufficient to pay obligations under the Contract are not appropriated or received from an intended third-party funding source. The determination by the Customer of insufficient funding shall be accepted by, and shall be final and binding on, the Supplier.

4. Termination for Cause

In addition to Contract terms relating to termination for cause, a customer may terminate its obligations, in whole or in part, to Supplier if it has provided Supplier with written notice of material breach and Supplier fails to cure such material breach within thirty (30) days of receipt of written notice. The Customer may also terminate a purchase order or other payment mechanism or Supplier's activities under the Contract immediately without a thirty (30) day written notice to Supplier, if Supplier fails to comply with confidentiality, privacy, security, environmental or safety requirements if such non-compliance relates or may relate to Supplier provision of products or services to the Customer or if Supplier's material breach is reasonably determined (i) to be an impediment to the function of the Customer and detrimental to the Customer, or (ii) when conditions preclude the thirty (30) day notice.

5. Termination for Convenience

In addition to any termination for convenience provisions in the Contract, a Customer may terminate a purchase order or other payment mechanism for convenience if it is determined that termination is in the Customer's best interest. Supplier will be provided at least thirty (30) days' written notice of termination.

6. Contract Management Fee and Usage Report

6.1 Pursuant to 74 O.S. § 85.33A, the State assesses a contract management fee on all transactions under a statewide contract. The payment of such fee will be calculated for all transactions, net of returns and the Supplier has no right of setoff against such fee regardless of the payment status of any Customer or any aggregate accounts receivable percentage. Supplier acknowledges and agrees that all prices quoted under any statewide contract shall include the contract management fee and the contract management fee shall not be reflected as a separate line item in Supplier's billing. The State reserves the

right to change this fee upward or downward upon sixty (60) calendar days' written notice to Supplier without further requirement for an Addendum.

6.2 While Supplier is the awardee of a statewide contract, transactions that occur under the terms of the statewide contract are subject to a one percent (1%) contract management fee to be paid by Supplier. Supplier shall submit a Contract Usage Report on a quarterly basis for each contract using a form provided by the State and such report shall include applicable information for each transaction. Reports shall include usage of the statewide contract by every Customer during the applicable quarter. A singular report provided late will not be considered a breach of the statewide contract; provided, however, repeated failure to submit accurate quarterly usage reports and submit timely payments may result in suspension or termination, in whole or in part, of the Contract.

6.3 All Contract Usage Reports shall meet the following criteria:

- i. Electronic submission in Microsoft Excel format to strategic.sourcing@omes.ok.gov;
- ii. Quarterly submission regardless of whether there were transactions under the Contract during the applicable quarterly reporting period;
- iii. Submission no later than forty-five (45) days following the end of each calendar quarter;
- iv. Contract quarterly reporting periods shall be as follows:
 - a. January 01 through March 31;
 - b. April 01 through June 30;
 - c. July 01 through September 30; and
 - d. October 01 through December 31.
- v. Reports must include the following information:
 - a. Procuring entity;
 - b. Order date;

- c. Purchase Order number or note that the transaction was paid by Purchase Card;
- d. City in which products or services were received or specific office or subdivision title;
- e. Product manufacturer or type of service;
- f. Manufacturer item number, if applicable;
- g. Product description;
- h. General product category, if applicable;
- i. Quantity;
- j. Unit list price or MSRP, as applicable;
- k. Unit price charged to the purchasing entity; and
- l. Other Contract usage information requested by the State.

6.4 Payment of the contract management fee shall be delivered to the following address within forty-five (45) calendar days after the end of each quarterly reporting period:

State of Oklahoma
Office of Management and Enterprise Services, Central Purchasing
2401 North Lincoln Boulevard, Suite 116
Oklahoma City, Oklahoma 73105

To ensure payment is properly accounted for, Supplier shall provide the following information with payment: (i) reference to the applicable Contract Usage Report and quarterly reporting period and (ii) the applicable statewide contract number(s) and the amount of the contract management fee being paid for each contract number.

ATTACHMENT D

STATE OF OKLAHOMA INFORMATION TECHNOLOGY TERMS

The parties further agree to the following terms (“Information Technology Terms”), as applicable, for any Acquisition of products or services with an information technology or telecommunication component. Pursuant to the Oklahoma Information Technology Consolidation and Coordination Act, OMES-Information Services (“OMES-IS”) is designated to purchase information technology and telecommunication products and services on behalf of the State. The Act directs OMES-IS to acquire necessary hardware, software and services and to authorize the use by other State agencies. OMES, as the owner of information technology and telecommunication assets and contracts on behalf of the State, allows other State agencies to use the assets while retaining ownership and the right to reassign the assets, at no additional cost, upon written notification to Supplier. OMES-IS is the data custodian for State agency data; however, such data is owned by the respective State agency.

1 Definitions

- 1.1 **COTS** means software that is commercial off the shelf.
- 1.2 **Customer Data** means all data supplied by or on behalf of a Customer in connection with the Contract, excluding any confidential information of Supplier.
- 1.3 **Data Breach** means the unauthorized access by an unauthorized person that results in the use, disclosure or theft of Customer Data.
- 1.4 **Host** includes the terms **Hosted** or **Hosting** and means the accessing, processing or storing of Customer Data.
- 1.5 **Intellectual Property Rights** means the worldwide legal rights or interests evidenced by or embodied in any idea, design, concept, personality right, method, process, technique, apparatus, invention, discovery or improvement including any patents, trade secrets and know-how; any work of authorship including any copyrights, Moral Rights or neighboring rights; any trademark, service mark, trade dress, trade name or other indicia of source or origin; domain name registrations; and any other proprietary or similar rights. Intellectual Property Rights of a party also includes all worldwide legal rights or interests that the party may have acquired by assignment or license with the right to grant sublicenses.
- 1.6 **Moral Rights** means any and all rights of paternity or integrity of the Work Product and the right to object to any modification, translation or use of the Work Product and any similar rights existing under the judicial or statutory law of any country in the world or under any treaty, regardless of whether or not such right is denominated or referred to as a moral right.
- 1.7 **Non-Public Data** means Customer Data, other than Personal Data, that is not subject to distribution to the public as public information. It is deemed to be sensitive and confidential

by Customer because it contains information that is exempt by statute, ordinance or administrative rule from access by the general public as public information. Non-Public Data includes any data deemed confidential pursuant to the Contract, otherwise identified by Customer as Non-Public Data, or that a reasonable person would deem confidential.

- 1.8 Personal Data** means Customer Data that contains 1) any combination of an individual's name, social security numbers, driver's license, state/federal identification number, account number, credit or debit card number and/or 2) data subject to protection under a federal, state or local law, rule, regulation or ordinance.
- 1.9 Security Incident** means the attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with the Hosted environment used to perform the services.
- 1.10 State CIO** means the State Chief Information Officer or authorized designee.
- 1.11 Supplier Intellectual Property** means all tangible or intangible items or things, including the Intellectual Property Rights therein, created or developed by Supplier and identified in writing as such (a) prior to providing any services or Work Product to Customer and prior to receiving any documents, materials, information or funding from or on behalf of a Customer relating to the services or Work Product, or (b) after the effective date of the Contract if such tangible or intangible items or things were independently developed by Supplier outside Supplier's provision of services or Work Product for Customer under the Contract and were not created, prepared, developed, invented or conceived by any Customer personnel who then became personnel to Supplier or any of its affiliates or subcontractors, where, although creation or reduction-to-practice is completed while the person is affiliated with Supplier or its personnel, any portion of same was created, invented or conceived by such person while affiliated with Customer.
- 1.12 Third Party Intellectual Property** means the Intellectual Property Rights of any third party that is not a party to the Contract, and that is not directly or indirectly providing any goods or services to a Customer under the Contract.
- 1.13 Work Product** means any and all deliverables produced by Supplier for Customer under a statement of work issued pursuant to the Contract, including any and all tangible or intangible items or things that have been or will be prepared, created, developed, invented or conceived at any time following the effective date of the Contract, including but not limited to any (i) works of authorship (such as manuals, instructions, printed material, graphics, artwork, images, illustrations, photographs, computer programs, computer software, scripts, object code, source code or other programming code, HTML code, flow charts, notes, outlines, lists, compilations, manuscripts, writings, pictorial materials, schematics, formulae, processes, algorithms, data, information, multimedia files, text web pages or web sites, other written or machine readable expression of such works fixed in any tangible media, and all other copyrightable works), (i) trademarks, service marks, trade dress, trade names, logos, or other indicia of source or origin, (iii) ideas, designs, concepts,

personality rights, methods, processes, techniques, apparatuses, inventions, formulas, discoveries, or improvements, including any patents, trade secrets and know-how, (iv) domain names, (v) any copies, and similar or derivative works to any of the foregoing, (vi) all documentation and materials related to any of the foregoing, (vii) all other goods, services or deliverables to be provided to Customer under the Contract or statement of work, and (viii) all Intellectual Property Rights in any of the foregoing, and which are or were created, prepared, developed, invented or conceived for the use or benefit of Customer in connection with this Contract or a statement of work, or with funds appropriated by or for Customer or Customer's benefit: (a) by any Supplier personnel or Customer personnel, or (b) any Customer personnel who then became personnel to Supplier or any of its affiliates or subcontractors, where, although creation or reduction-to-practice is completed while the person is affiliated with Supplier or its personnel, any portion of same was created, invented or conceived by such person while affiliated with Customer.

2 Termination of Maintenance and Support Services

Customer may terminate maintenance or support services without an adjustment charge, provided any of the following circumstances occur:

- 2.1** Customer removes the product for which the services are provided, from productive use or;
- 2.2** The location at which the services are provided is no longer controlled by Customer (for example, because of statutory or regulatory changes or the sale or closing of a facility).

If Customer chooses to renew maintenance or support after maintenance has lapsed, Customer may choose to pay the additional fee, if any, associated with renewing a license after such maintenance or support has lapsed, or to purchase a new license. Any amount paid to Supplier in the form of prepaid fees that are unused when services under the Contract or purchase order are terminated shall be refunded to Customer.

3 Compliance and Electronic and Information Technology Accessibility

State procurement of information technology is subject to certain federal and State laws, rules and regulations related to information technology accessibility, including but not limited to Oklahoma Information Technology Accessibility Standards ("Standards") set forth at <https://oklahoma.gov/omes/services/information-services/is/policies-and-standards/accessibility-standards.html>. Supplier shall provide a Voluntary Product Accessibility Template ("VPAT") describing accessibility compliance via a URL linking to the VPAT and shall update the VPAT as necessary in order to allow a Customer to obtain current VPAT information as required by State law. If products require development or customization, additional requirements and documentation may be required, and compliance shall be necessary by Supplier. Such requirements may be stated in appropriate documents including but not limited to a statement of work, riders, agreement, purchase order or Addendum.

All representations contained in the VPAT provided will be relied upon by the State or a Customer, as applicable, for accessibility compliance purposes.

4 Media Ownership (Disk Drive and/or Memory Chip Ownership)

- 4.1** Any disk drives and memory cards purchased with or included for use in leased or purchased products under the Contract remain the property of the Customer.
- 4.2** Personal information may be retained within electronic media devices and components; therefore, electronic media shall not be released either between Customers or for the resale, of refurbished equipment that has been in use by a Customer, by the Supplier to the general public or other entities. This provision applies to replacement devices and components, whether purchased or leased, supplied by Supplier, its agents or subcontractors during the downtime (repair) of products purchased or leased through the Contract. If a device is removed from a location for repairs, the Customer shall have sole discretion, prior to removal, to determine and implement sufficient safeguards (such as a record of hard drive serial numbers) to protect personal information that may be stored within the hard drive or memory of the device.

5 Offshore Services

No offshore services are provided for under the Contract. State data shall not be used or accessed internationally for troubleshooting or any other use not specifically provided for herein without the prior written permission, which may be withheld in the State's sole discretion, from the appropriate authorized representative of the State. Notwithstanding the above, back office administrative functions of the Supplier may be located offshore and the follow-the-sun support model may be used by the Supplier to the extent allowed by law applicable to any Customer data being accessed or used.

6 Compliance with Technology Policies

- 6.1** The Supplier agrees to adhere to the State of Oklahoma "Information Security Policy, Procedures, and Guidelines" available at [Information Security Policy, Procedures, Guidelines \(oklahoma.gov\)](https://oklahoma.gov/omes/services/information-services/is/policies-and-standards.html)

Supplier's employees and subcontractors shall adhere to the applicable State IT Standard Methodologies and Templates including but not limited to Project Management, Business Analysis, System Analysis, Enterprise and IT Architecture, Quality, Application and Security Methodologies and Templates as set forth at <https://oklahoma.gov/omes/services/information-services/is/policies-and-standards.html>

- 6.2** Supplier shall comply with applicable Federal Information Processing Standards including, without limitation, FIPS 200, FIPS 140-2 or successor standards and all recommendations from the National Institute of Standards and Technology. The confidentiality of Customer Data shall be protected and maintained in accordance with these standards as well as other

applicable Customer standards.

- 6.3** Supplier shall comply with the CJIS Security Policy as more particularly described at Appendix 2 attached hereto and incorporated herein.

7 Emerging Technologies

The State of Oklahoma reserves the right to enter into an Addendum to the Contract at any time to allow for emerging technologies not identified elsewhere in the Contract Documents if there are repeated requests for such emerging technology or the State determines it is warranted to add such technology.

8 Extension Right

In addition to extension rights of the State set forth in the Contract, the State CIO reserves the right to extend any Contract if the State CIO determines such extension to be in the best interest of the State.

9 Source Code Escrow

Pursuant to 62 O.S. § 34.31, if customized computer software is developed or modified exclusively for a State agency, the Supplier has a continuing obligation to comply with such law and place the source code for such software and any modifications thereto into escrow with an independent third-party escrow agent. Supplier shall pay all fees charged by the escrow agent and enter into an escrow agreement, the terms of which are subject to the prior written approval of the State, including terms that provide the State receives ownership of all escrowed source code upon the occurrence of any of the following:

- 9.1** A bona fide material default of the obligations of the Supplier under the agreement with the applicable Customer;
- 9.2** An assignment by the Supplier for the benefit of its creditors;
- 9.3** A failure by the Supplier to pay, or an admission by the Supplier of its inability to pay, its debts as they mature;
- 9.4** The filing of a petition in bankruptcy by or against the Supplier when such petition is not dismissed within sixty (60) days of the filing date;
- 9.5** The appointment of a receiver, liquidator or trustee appointed for any substantial part of the Supplier's property;
- 9.6** The inability or unwillingness of the Supplier to provide the maintenance and support services in accordance with the agreement with the agency;
- 9.7** Supplier's ceasing of maintenance and support of the software; or
- 9.8** Such other condition as may be statutorily imposed by the future amendment or enactment

of applicable Oklahoma law.

10 Commercial Off The Shelf Software

If Supplier specifies terms and conditions or clauses in an electronic license, subscription, maintenance, support or similar agreement that conflict with the terms of this Contract, the additional terms and conditions or conflicting clauses shall not be binding on the State and the provisions of this Contract shall prevail.

11 Ownership Rights

Any software developed by the Supplier under the terms of the Contract is for the sole and exclusive use of the State including but not limited to the right to use, reproduce, re-use, alter, modify, edit, or change the software as it sees fit and for any purpose. Moreover, except with regard to any deliverable based on Supplier Intellectual Property, the State shall be deemed the sole and exclusive owner of all right, title, and interest therein, including but not limited to all source data, information and materials furnished to the State, together with all plans, system analysis, and design specifications and drawings, completed programs and documentation thereof, reports and listing, all data and test procedures and all other items pertaining to the work and services to be performed pursuant to this Contract including all copyright and proprietary rights relating thereto. With respect to Supplier Intellectual Property, the Supplier grants the State, for no additional consideration, a perpetual, irrevocable, royalty-free license, solely for the internal business use of the State, to use, copy, modify, display, perform, transmit and prepare derivative works of Supplier Intellectual Property embodied in or delivered to the State in conjunction with the products.

Except for any Supplier Intellectual Property, all work performed by the Supplier of developing, modifying or customizing software and any related supporting documentation shall be considered as Work for Hire (as defined under the U.S. copyright laws) and, as such, shall be owned by and for the benefit of State.

In the event that it should be determined that any portion of such software or related supporting documentation does not qualify as “Work for Hire”, Supplier hereby irrevocably grants to the State, for no additional consideration, a non-exclusive, irrevocable, royalty-free license to use, copy, modify, display, perform, transmit and prepare derivative works of any such software and any Supplier Intellectual Property embodied in or delivered to the State in conjunction with the products.

Supplier shall assist the State and its agents, upon request, in preparing U.S. and foreign copyright, trademark, and/or patent applications covering software developed, modified or customized for the State. Supplier shall sign any such applications, upon request, and deliver them to the State. The State shall bear all expenses that incurred in connection with such copyright, trademark, and/or patent applications.

If any Acquisition pursuant to this Contract is funded wholly or in part with federal funds, the source code and all associated software and related documentation owned by the State may be

shared with other publicly funded agencies at the discretion of the State without permission from or additional compensation to the Supplier.

12 Intellectual Property Ownership

The following terms apply to ownership and rights related to Intellectual Property:

- 12.1** As between Supplier and Customer, the Work Product and Intellectual Property Rights therein are and shall be owned exclusively by Customer, and not Supplier. Supplier specifically agrees that the Work Product shall be considered “works made for hire” and that the Work Product shall, upon creation, be owned exclusively by Customer. To the extent that the Work Product, under applicable law, may not be considered works made for hire, Supplier hereby agrees that all right, title and interest in and to all ownership rights and all Intellectual Property Rights in the Work Product is hereby effectively transferred, granted, conveyed, assigned and relinquished exclusively to Customer, without the necessity of any further consideration, and Customer shall be entitled to obtain and hold in its own name all Intellectual Property Rights in and to the Work Product. Supplier acknowledges that Supplier and Customer do not intend Supplier to be a joint author of the Work Product within the meaning of the Copyright Act of 1976. Customer shall have access, during normal business hours (Monday through Friday, 8:00 a.m. to 5:00 p.m.) and upon reasonable prior notice to Supplier, to all Supplier materials, premises and computer files containing the Work Product. Supplier and Customer, as appropriate, will cooperate with one another and execute such other documents as may be reasonably appropriate to achieve the objectives herein. No license or other right is granted under the Contract to any Third-Party Intellectual Property, except as may be incorporated in the Work Product by Supplier.
- 12.2** Supplier, upon request and without further consideration, shall perform any acts that may be deemed reasonably necessary or desirable by Customer to evidence more fully the transfer of ownership and/or registration of all Intellectual Property Rights in all Work Product to Customer to the fullest extent possible including, but not limited to, the execution, acknowledgement and delivery of such further documents in a form determined by Customer. In the event Customer shall be unable to obtain Supplier’s signature due to the dissolution of Supplier or Supplier’s failure to respond to Customer’s repeated requests for such signature on any document reasonably necessary for any purpose set forth in the foregoing sentence, Supplier hereby irrevocably designates and appoints Customer and its duly authorized officers and agents as Supplier’s agent and Supplier’s attorney-in-fact to act for and in Supplier’s behalf and stead to execute and file any such document and to do all other lawfully permitted acts to further any such purpose with the same force and effect as if executed and delivered by Supplier, provided however that no such grant of right to Customer is applicable if Supplier fails to execute any document due to a good faith dispute by Supplier with respect to such document. It is understood that such power is coupled with an interest and is therefore irrevocable. Customer shall have the full and sole power to prosecute such applications and to take all other action concerning the Work Product, and Supplier shall cooperate, at Customer’s sole expense, in the preparation and

prosecution of all such applications and in any legal actions and proceedings concerning the Work Product.

- 12.3** Supplier hereby irrevocably and forever waives, and agrees never to assert, any Moral Rights in or to the Work Product which Supplier may now have or which may accrue to Supplier's benefit under U.S. or foreign copyright or other laws and any and all other residual rights and benefits which arise under any other applicable law now in force or hereafter enacted. Supplier acknowledges the receipt of equitable compensation for its assignment and waiver of such Moral Rights.
- 12.4** All documents, information and materials forwarded to Supplier by Customer for use in and preparation of the Work Product shall be deemed the confidential information of Customer, subject to the license granted by Customer to Supplier hereunder. Supplier shall not otherwise use, disclose, or permit any third party to use or obtain the Work Product, or any portion thereof, in any manner without the prior written approval of Customer.
- 12.5** These provisions are intended to protect Customer's proprietary rights pertaining to the Work Product and the Intellectual Property Rights therein and any misuse of such rights would cause substantial and irreparable harm to Customer's business. Therefore, Supplier acknowledges and stipulates that a court of competent jurisdiction may immediately enjoin a material breach of the Supplier's obligations with respect to confidentiality provisions of the Contract and the Work Product and a Customer's Intellectual Property Rights, upon a request by Customer, without requiring proof of irreparable injury, as same is presumed.
- 12.6** Upon the request of Customer, but in any event upon termination or expiration of this Contract or a statement of work, Supplier shall surrender to Customer all documents and things pertaining to the Work Product, generated or developed by Supplier or furnished by Customer to Supplier, including all materials embodying the Work Product, any Customer confidential information and Intellectual Property Rights in such Work Product, regardless of whether complete or incomplete. This section is intended to apply to all Work Product as well as to all documents and things furnished to Supplier by Customer or by anyone else that pertains to the Work Product.
- 12.7** Customer hereby grants to Supplier a non-transferable, non-exclusive, royalty-free, fully paid license to use any Work Product solely as necessary to provide services to Customer. Except as provided in this section, neither Supplier nor any subcontractor shall have the right to use the Work Product in connection with the provision of services to its other customers without the prior written consent of Customer, which consent may be withheld in Customer's sole discretion.
- 12.8** To the extent that any Third-Party Intellectual Property is embodied or reflected in the Work Product or is necessary to provide services, Supplier shall obtain from the applicable third party for the Customer's benefit, an irrevocable, perpetual, non-exclusive, worldwide, royalty-free license, solely for Customer's internal business purposes; likewise, with respect to any Supplier Intellectual Property embodied or reflected in the Work Product or

necessary to provide services, Supplier grants to Customer an irrevocable, perpetual, non-exclusive, worldwide, royalty-free license, solely for the Customer's internal business purposes. Each such license shall allow the applicable Customer to (i) use, copy, modify, display, perform (by any means), transmit and prepare derivative works of any Third-Party Intellectual Property or Supplier Intellectual Property embodied in or delivered to Customer in conjunction with the Work Product and (ii) authorize others to do any or all of the foregoing. Supplier agrees to notify Customer on delivery of the Work Product or services if such materials include any Third-Party Intellectual Property. The foregoing license includes the right to sublicense third parties, solely for the purpose of engaging such third parties to assist or carry out Customer's internal business use of the Work Product. Except for the preceding license, all rights in Supplier Intellectual Property remain in Supplier. On request, Supplier shall provide Customer with documentation indicating a third party's written approval for Supplier to use any Third-Party Intellectual Property that may be embodied or reflected in the Work Product.

- 12.9** Supplier agrees that it shall have written agreement(s) that are consistent with the provisions hereof related to Work Product and Intellectual Property Rights with any employees, agents, consultants, contractors or subcontractors providing services or Work Product pursuant to the Contract, prior to the provision of such services or Work Product and that it shall maintain such written agreements at all times during performance of this Contract which are sufficient to support all performance and grants of rights by Supplier. Copies of such agreements shall be provided to the Customer promptly upon request.
- 12.10** To the extent not inconsistent with Customer's rights in the Work Product or other provisions, nothing in this Contract shall preclude Supplier from developing for itself, or for others, materials which are competitive with those produced as a result of the services provided under the Contract, provided that no Work Product is utilized, and no Intellectual Property Rights of Customer therein are infringed by such competitive materials. To the extent that Supplier wishes to use the Work Product or acquire licensed rights in certain Intellectual Property Rights of Customer therein in order to offer competitive goods or services to third parties, Supplier and Customer agree to negotiate in good faith regarding an appropriate license and royalty agreement to allow for such.
- 12.11** If any Acquisition pursuant to the Contract is funded wholly or in part with federal funds, the source code and all associated software and related documentation and materials owned by a Customer may be shared with other publicly funded agencies at the discretion of such Customer without permission from or additional compensation to the Supplier.

13 Hosting Services

- 13.1** If Supplier or its subcontractor, affiliate or any other person or entity providing products or services under the Contract Hosts Customer Data in connection with an Acquisition, the provisions of Appendix 1, attached hereto and incorporated herein, apply to such Acquisition.

13.2 If the Hosting of Customer Data by Supplier or its subcontractor, affiliate or any other person or entity providing products or services under the Contract contributes to or directly causes a Data Breach, Supplier shall be responsible for the obligations set forth in Appendix 1 related to breach reporting requirements and associated costs. Likewise if such Hosting contributes to or directly causes a Security Incident, Supplier shall be responsible for the obligations set forth in Appendix 1, as applicable.

14 Change Management

When a scheduled change is made to products or services provided to a Customer that impacts the Customer's system related to such product or service, Supplier shall provide two (2) weeks' prior written notice of such change. When the change is an emergency change, Supplier shall provide twenty-four (24) hours' prior written notice of the change. Repeated failure to provide such notice may be an evaluation factor (as indicative of Supplier's past performance) upon renewal or if future bids submitted by Supplier are evaluated by the State.

15 Service Level Deficiency

In addition to other terms of the Contract, in instances of the Supplier's repeated failure to provide an acceptable level of service or meet service level agreement metrics, service credits shall be provided by Supplier and may be used as an offset to payment due.

16 Notices

In addition to notice requirements under the terms of the Contract otherwise, the following individuals shall also be provided the request, approval or notice, as applicable:

Chief Information Officer
3115 N. Lincoln Blvd
Oklahoma City, OK 73105

With a copy, which shall not constitute notice, to:

Information Services Deputy Counsel
3115 North Lincoln Boulevard
Oklahoma City, Oklahoma 73105

Appendix 1 to State of Oklahoma Information Technology Terms

The parties agree to the following provisions in connection with any Customer Data accessed, processed or stored by or on behalf of the Supplier and the obligations, representations and warranties set forth below shall continue as long as the Supplier has an obligation under the Contract

A. Customer Data

1. Customer will be responsible for the accuracy and completeness of all Customer Data provided to Supplier by Customer. Customer shall retain exclusive ownership of all Customer Data. Non-Public Data and Personal Data shall be deemed to be Customer's confidential information. Supplier shall restrict access to Customer Data to their employees with a need to know (and advise such employees of the confidentiality and non-disclosure obligations assumed herein).
2. Supplier shall promptly notify the Customer upon receipt of any requests from unauthorized third parties which in any way might reasonably require access to Customer Data or Customer's use of the Hosted environment. Supplier shall notify the Customer by the fastest means available and also in writing pursuant to Contract notice provisions and the notice provision herein. Except to the extent required by law, Supplier shall not respond to subpoenas, service or process, Freedom of Information Act or other open records requests, and other legal request related to Customer without first notifying the Customer and obtaining the Customer's prior approval, which shall not be unreasonably withheld, of Supplier's proposed responses. Supplier agrees to provide its completed responses to the Customer with adequate time for Customer review, revision and approval.
3. Supplier will use commercially reasonable efforts to prevent the loss of or damage to Customer Data in its possession and will maintain commercially reasonable back-up procedures and copies to facilitate the reconstruction of any Customer Data that may be lost or damaged by Supplier. Supplier will promptly notify Customer of any loss, damage to, or unauthorized access of Customer Data. Supplier will use commercially reasonable efforts to reconstruct any Customer Data that has been lost or damaged by Supplier as a result of its negligence or willful misconduct. If Customer Data is lost or damaged for reasons other than as a result of Supplier's negligence or willful misconduct, Supplier, at the Customer's expense, will, at the request of the State, use commercially reasonable efforts to reconstruct any Customer Data lost or damaged.

B. Data Security

1. Supplier will use commercially reasonable efforts, consistent with industry standards, to provide security for the Hosted environment and Customer Data and to protect against both unauthorized access to the Hosting environment, and unauthorized communications between the Hosting environment and the Customer's browser. Supplier shall implement and maintain appropriate administrative, technical and organizational security measures to safeguard against unauthorized access, disclosure or theft of Personal Data and Non-Public

Data. Such security measures shall be in accordance with recognized industry practice and not less stringent than the measures the service provider applies to its own personal data and non-public data of similar kind.

2. All Personal Data and Non-public Data shall be encrypted at rest and in transit with controlled access. Unless otherwise stipulated, the service provider is responsible for encryption of Personal Data.
3. Supplier represents and warrants to the Customer that the Hosting equipment and environment will be routinely checked with a commercially available, industry standard software application with up-to-date virus definitions. Supplier will regularly update the virus definitions to ensure that the definitions are as up-to-date as is commercially reasonable. Supplier will promptly purge all viruses discovered during virus checks. If there is a reasonable basis to believe that a virus may have been transmitted to Customer by Supplier, Supplier will promptly notify Customer of such possibility in a writing that states the nature of the virus, the date on which transmission may have occurred, and the means Supplier has used to remediate the virus. Should the virus propagate to Customer's IT infrastructure, Supplier is responsible for costs incurred by Customer for Customer to remediate the virus.
4. Supplier shall provide its services to Customer and its users solely from data centers in the U.S. Storage of Customer Data at rest shall be located solely in data centers in the U.S. Supplier shall not allow its personnel or contractors to store Customer Data on portable devices, including personal computers, except for devices that are used and kept only at its U.S. data centers. Supplier shall permit its personnel and contractors to access Customer Data remotely only as required to fulfill Supplier's obligations under the Contract.
5. Supplier shall allow the Customer to audit conformance to the Contract terms. The Customer may perform this audit or contract with a third party at its discretion and at Customer's expense.
6. Supplier shall perform an independent audit of its data centers at least annually at its expense and provide a redacted version of the audit report upon request. Supplier may remove its proprietary information from the redacted version. A Service Organization Control (SOC) 2 audit report or approved equivalent sets the minimum level of a third-party audit.
7. Any remedies provided in this Appendix are not exclusive and are in addition to other rights and remedies available under the terms of the Contract, at law or in equity.

C. Security Assessment

1. The State requires any entity or third-party Supplier Hosting Oklahoma Customer Data to submit to a State Certification and Accreditation Review process to assess initial security risk. Supplier submitted to the review and met the State's minimum security standards at time the Contract was executed. Failure to maintain the State's minimum security standards

during the term of the contract, including renewals, constitutes a material breach. Upon request, the Supplier shall provide updated data security information in connection with a potential renewal. If information provided in the security risk assessment changes, Supplier shall promptly notify the State and include in such notification the updated information; provided, however, Supplier shall make no change that results in lessened data protection or increased data security risk. Failure to provide the notice required by this section or maintain the level of security required in the Contract constitutes a material breach by Supplier and may result in a whole or partial termination of the Contract.

2. Any Hosting entity change must be approved in writing prior to such change. To the extent Supplier requests a different sub-contractor than the third-party Hosting Supplier already approved by the State, the different sub-contractor is subject to the State's approval. Supplier agrees not to migrate State's data or otherwise utilize the different third-party Hosting Supplier in connection with key business functions that are Supplier's obligations under the contract until the State approves the third-party Hosting Supplier's State Certification and Accreditation Review, which approval shall not be unreasonably withheld or delayed. In the event the third-party Hosting Supplier does not meet the State's requirements under the State Certification and Accreditation Review, Supplier acknowledges and agrees it will not utilize the third-party Supplier in connection with key business functions that are Supplier's obligations under the contract, until such third party meets such requirements.

D. Security Incident or Data Breach Notification: Supplier shall inform Customer of any Security Incident or Data Breach.

1. Supplier may need to communicate with outside parties regarding a Security Incident, which may include contacting law enforcement, fielding media inquiries and seeking external expertise as mutually agreed upon, defined by law or contained in the Contract. If a Security Incident involves Customer Data, Supplier will coordinate with Customer prior to any such communication.
2. Supplier shall report a Security Incident to the Customer identified contact set forth herein within five (5) days of discovery of the Security Incident or within a shorter notice period required by applicable law or regulation (i.e. HIPAA requires notice to be provided within 24 hours).
3. Supplier shall:
 - a. Maintain processes and procedures to identify, respond to and analyze Security Incidents;
 - b. Make summary information regarding such procedures available to Customer at Customer's request;
 - c. Mitigate, to the extent practicable, harmful effects of Security Incidents that are known to Supplier; and

d. Document all Security Incidents and their outcomes.

4. If Supplier has reasonable belief or actual knowledge of a Data Breach, Supplier shall (1) promptly notify the appropriate Customer identified contact set forth herein within 24 hours or sooner, unless shorter time is required by applicable law, and (2) take commercially reasonable measures to address the Data Breach in a timely manner.

E. **Breach Responsibilities:** This section only applies when a Data Breach occurs with respect to Personal Data or Non-Public Data within the possession or control of Supplier.

1. Supplier shall (1) cooperate with Customer as reasonably requested by Customer to investigate and resolve the Data Breach, (2) promptly implement necessary remedial measures, if necessary, and (3) document responsive actions taken related to the Data Breach, including any post-incident review of events and actions taken to make changes in business practices in providing the services, if necessary.
2. Unless otherwise stipulated, if a Data Breach is a direct result of Supplier's breach of its obligation to encrypt Personal Data and Non-Public Data or otherwise prevent its release, Supplier shall bear the costs associated with (1) the investigation and resolution of the Data Breach; (2) notifications to individuals, regulators or others required by state law; (3) credit monitoring services required by state or federal law; (4) a website or toll-free numbers and call center for affected individuals required by state law – all not to exceed the agency per record per person cost calculated for data breaches in the United States on the most recent Cost of Data breach Study: Global Analysis published by the Ponemon Institute at the time of the data breach; and (5) complete all corrective actions as reasonably determined by Supplier based on root cause.
3. If a Data Breach is a direct result of Supplier's breach of its obligations to encrypt Personal Data and Non-Public Data or otherwise prevent its release, Supplier shall indemnify and hold harmless the Customer against all penalties assessed to Indemnified Parties by governmental authorities in connection with the Data Breach.

F. **Notices**

In addition to notice requirements under the terms of the Contract and those set forth above, a request, an approval or a notice in connection with this Appendix provided by Supplier shall be provided to:

Chief Information Security Officer

3115 N. Lincoln Blvd

Oklahoma City, OK 73105

and

servicedesk@omes.ok.gov.

G. Supplier Representations and Warranties

Supplier represents and warrants the following:

1. The product and services provided in connection with Hosting services do not infringe a third party's patent or copyright or other intellectual property rights.
2. Supplier will protect Customer's Non-Public Data and Personal Data from unauthorized dissemination and use with the same degree of care that each such party uses to protect its own confidential information and, in any event, will use no less than a reasonable degree of care in protecting such confidential information.
3. The execution, delivery and performance of the Contract and any ancillary documents and the consummation of the transactions contemplated by the Contract or any ancillary documents by Supplier will not violate, conflict with, or result in a breach of any provision of, or constitute a default (or an event which, with notice or lapse of time or both, would constitute a default) under, or result in the termination of, any written contract or other instrument between Supplier and any third parties retained or utilized by Supplier to provide goods or services for the benefit of the Customer.
4. Supplier shall not knowingly upload, store, post, e-mail or otherwise transmit, distribute, publish or disseminate to or through the Hosting environment any material that contains software viruses, malware or other surreptitious code designed to interrupt, destroy or limit the functionality of any computer software or hardware or telecommunications equipment or circumvent any "copy-protected" devices, or any other harmful or disruptive program.

H. Indemnity

Supplier agrees to defend, indemnify and hold the State, its officers, directors, employees, and agents harmless from all liabilities, claims, damages, losses, costs, expenses, demands, suits and actions (including without limitation reasonable attorneys' fees and costs required to establish the right to indemnification), excluding damages that are the sole fault of Customer, arising from or in connection with Supplier's breach of its express representations and warranties in these Information Technology Terms and the Contract. If a third party claims that any portion of the products or services provided by Supplier under the terms of another Contract Document or these Information Technology Terms infringes that party's patent or copyright, Supplier shall defend, indemnify and hold harmless the State and Customer against the claim at Supplier's expense and pay all related costs, damages, and attorney's fees incurred by or assessed to, the State and/or Customer. The State and/or Customer shall promptly notify Supplier of any third party claims and to the extent authorized by the Attorney General of the State, allow Supplier to control the defense and any related settlement negotiations. If the Attorney General of the State does not authorize sole control of the defense and settlement negotiations to Supplier, Supplier shall be granted authorization to equally participate in any proceeding related to this section but Supplier shall remain responsible to indemnify Customer and the State for all associated costs, damages and fees incurred by or assessed to the State and/or Customer. Should the software become, or in Supplier's

opinion, be likely to become the subject of a claim or an injunction preventing its use as contemplated in connection with Hosting services, Supplier may, at its option (i) procure for the State the right to continue using the software or (ii) replace or modify the software with a like or similar product so that it becomes non-infringing.

I. Termination, Expiration and Suspension of Service

1. During any period of service suspension, Supplier shall not take any action to intentionally disclose, alter or erase any Customer Data.

2. In the event of a termination or expiration of the Contract, the parties further agree:

Supplier shall implement an orderly return of Customer Data in a format specified by the Customer and, as determined by the Customer:

a. return the Customer Data to Customer at no additional cost, at a time agreed to by the parties and the subsequent secure disposal of State Data;

b. transitioned to a different Supplier at a mutually agreed cost and in accordance with a mutually agreed data transition plan and the subsequent secure disposal of State Data or

c. a combination of the two immediately preceding options.

3. Supplier shall not take any action to intentionally erase any Customer Data for a period of:

a. 10 days after the effective date of termination, if the termination is in accordance with the contract period;

b. 30 days after the effective date of termination, if the termination is for convenience; or

c. 60 days after the effective date of termination, if the termination is for cause.

After such period, Supplier shall, unless legally prohibited or otherwise stipulated, delete all Customer Data in its systems or otherwise in its possession or under its control.

4. The State shall be entitled to any post termination or expiration assistance generally made available with respect to the services.

5. Disposal by Supplier of Customer Data in all of its forms, such as disk, CD/DVD, backup tape and paper, when requested by the Customer, shall be performed in a secure manner. Data shall be permanently deleted and shall not be recoverable, according to National Institute of Standards and Technology (NIST)-approved methods. Certificates of destruction shall be provided to Customer within thirty (30) calendar day of its request for disposal of data.

Appendix 2 to State of Oklahoma Information Technology Terms

INTRODUCTION

The use and maintenance of all items of software or equipment offered for purchase herein must be in compliance with the most current version of the U.S. Department of Justice, Federal Bureau of Investigation (“FBI”), Criminal Justice Information Services (CJIS) Division’s CJIS Security Policy (“CJIS Security Policy” or “Security Policy” herein).

The Entity or Affiliate acquiring the data or system is hereby ultimately responsible for compliance with the CJIS Security Policy and will be subject to an audit by the State of Oklahoma CJIS Systems Officer (“CSO”) and the FBI CJIS Division’s Audit Staff.

CJIS SECURITY POLICY REQUIREMENTS GENERALLY

The CJIS Security Policy outlines a number of administrative, procedural, and technical controls agencies must have in place to protect Criminal Justice Information (“CJI”). Our experience is that agencies will generally have many of the administrative and procedural controls in place but will need to implement additional technical safeguards in order to be in complete compliance with the mandate. A Criminal Justice Agency (“CJA”) and certain other governmental agencies procuring technology equipment and services that could be used in hosting or connecting or transmitting or receiving CJI data may need to use the check list herein to make sure that the software, equipment, location, security, and persons having the ability to access CJI will meet the CJIS requirements per the then current CJIS Security Policy. A completed Appendix H to said Security Policy will need to be signed by Vendor or a 3rd party if it has access to CJI, such as incident to the maintenance or support of the purchased hardware or software within which resides CJI. **Per Appendix “A” to said Security Policy, “access to CJI is the physical or logical (electronic) ability, right or privilege to view, modify or make use of CJI.”**

DIRECTIVE CONCERNING ACCESS TO CRIMINAL JUSTICE INFORMATION AND TO HARDWARE OR SOFTWARE WHICH INTERACTS WITH CJI and CERTIFICATION

The FBI CJIS Division provides state-of-the-art identification and information services to the local, state, tribal, federal, and international criminal justice communities for criminal justice purposes, as well as the noncriminal justice communities for noncriminal justice purposes.

This Directive primarily concerns access to CJI and access to hardware and software in the use, retention, transmission, reception, and hosting of CJI for criminal justice purposes and not for noncriminal justice purposes. In that regard, this Directive is not only applicable to such data, but also to the hardware and software interacting with such data, their location(s), and persons having the ability to access such data. The CJIS data applicable to the Security Policy is the data described as such in said Policy **plus all data transmitted over the Oklahoma Law Enforcement Telecommunications System (“OLETS”) which is operated by DPS.**

In order to have access to CJI or to the aforesaid hardware or software, the vendor must be familiar with the FBI CJIS Security Policy, including but not limited to the following portions of said Security Policy:

1. the Definitions and Acronyms in §3 & Appendices “A” & “B”;

2. the general policies in §4;
3. the Policies in §5;
4. the appropriate forms in Appendices “D”, “E”, “F” & “H”; and
5. the Supplemental Guidance in Appendices “J” & “K”.

This FBI Security Policy is located and may be downloaded at: <https://www.fbi.gov/services/cjis/cjis-security-policy-resource-center>.

By executing the Contract to which this Directive is attached, the vendor hereby CERTIFIES that the foregoing directive has and will be followed, including but not limited to full compliance with the FBI CJIS Security Policy, as amended and as applicable.

Policy Requirement Checklist		Compliance checklist –
Policy Area 1	Information Exchange Agreements	
Policy Area 2	Security Awareness Training	
Policy Area 3	Incident Response	
Policy Area 4	Auditing and Accountability	
Policy Area 5	Access Control	
Policy Area 6	Identification and Authentication	
Policy Area 7	Configuration Management	
Policy Area 8	Media Protection	
Policy Area 9	Physical Protection	
Policy Area 10	Systems and Communications Protection and Information Integrity	
Policy Area 11	Formal Audits	
Policy Area 12	Personnel Security	

Attachment E-1



Schedule C – Cloud Services – Public Sector

Oracle America, Inc. (“Oracle”, “we”, “us”, or “our”)

500 Oracle Parkway
Redwood Shores, CA 94065

Your Name (“You”):	State of Oklahoma, by and through the Office of Management and Enterprise
General Terms Reference:	US-GMA-80421183
Schedule Reference:	US-GMA-80421183

This Public Sector Cloud Services Schedule (this “Schedule C”) is a Schedule to the General Terms Agreement (“General Terms”) referenced above. This Schedule C shall coterminate with the General Terms; provided that each ordering document issued and executed under the General Terms and this Schedule C shall continue to be in full force and effect, and the terms of the General Terms and this Schedule C shall continue to apply thereto, in each case, unless and until such ordering document has expired or been terminated. For purposes of the Services under this Schedule C, the General Terms (including Attachments B and D) and this Schedule C constitute, collectively, the “Master Agreement”; other Schedules to the General Terms, such as Schedule P (Program Schedule), do not apply to the Services ordered under this Schedule C. As used in this Schedule C, “You” or “Your” shall refer to the Customer placing an order under the General Terms and this Schedule C.

1. USE OF THE SERVICES

1.1 Oracle will make the Oracle services listed in Your order (the “Services”) available to You pursuant to the Master Agreement and Your order. Except as otherwise stated in the Master Agreement or Your order, You have the non-exclusive, worldwide, limited right to use the Services during the period defined in Your order, unless earlier terminated in accordance with the Master Agreement or Your order (the “Services Period”), solely for Your internal business operations. You may allow Your Users (as defined below) to use the Services for this purpose, and You are responsible for their compliance with the Master Agreement and Your order.

1.2 The Service Specifications describe and govern the Services. During the Services Period, we may update the Services and Service Specifications (with the exception of the Data Processing Agreement as described below) to reflect changes in, among other things, laws, regulations, rules, technology, industry practices, patterns of system use, and availability of Third Party Content (as defined below). Oracle updates to the Services or Service Specifications will not materially reduce the level of performance, functionality, security or availability of the Services during the Services Period of Your order.

1.3 You may not, and may not cause or permit others to: (a) use the Services to harass any person; cause damage or injury to any person or property; publish any material that is false, defamatory, harassing or obscene; violate privacy rights; promote bigotry, racism, hatred or harm; send unsolicited bulk e-mail, junk mail, spam or chain letters; infringe property rights; or otherwise violate applicable laws, ordinances or regulations; (b) perform or disclose any benchmarking or availability testing of the Services; (c) perform or disclose any performance or vulnerability testing of the Services without Oracle’s prior written approval, or perform or disclose network discovery, port and service identification, vulnerability scanning, password cracking, or remote access testing of the Services; or (d) use the Services to perform cyber currency or crypto currency mining ((a) through (d) collectively, the “Acceptable Use Policy”). In addition to other rights that we have in the Master Agreement and Your order, we have the right to take remedial action if the Acceptable Use Policy is violated, and such remedial action may include removing or disabling access to material that violates the policy.

2. FEES AND PAYMENT

2.1 Once placed, Your order is non-cancelable and the sums paid nonrefundable, except as provided in the Master Agreement or Your order. Fees for services listed in an order are exclusive of taxes and expenses, unless expressly stated otherwise in Your order. Pursuant to 68 O.S. §§ 1352, 1356, and 1404, State agencies are exempt from the assessment of State sales, use, and excise taxes. Further, State agencies and political subdivisions of the State are exempt from Federal Excise Taxes pursuant to Title 26 of the United States Code.

Attachment E-1

2.2 If You exceed the quantity of Services ordered, then You promptly must purchase and pay fees for the excess quantity.

3. OWNERSHIP RIGHTS AND RESTRICTIONS

3.1 You or Your licensors retain all ownership and intellectual property rights in and to Your Content (as defined below). We or our licensors retain all ownership and intellectual property rights in and to the Services, derivative works thereof, and anything developed or delivered by or on behalf of us under the Master Agreement. For the avoidance of doubt, the Services shall not include development or modification of customized computer software within the meaning of 62 O.S. 34.31.

3.2 You may have access to Third Party Content through use of the Services. Unless otherwise stated in Your order, all ownership and intellectual property rights in and to Third Party Content and the use of such content is governed by separate third party terms between You and the third party.

3.3 You grant us the right to host, use, process, display and transmit Your Content as necessary to provide the Services pursuant to and in accordance with the Master Agreement and Your order. You have sole responsibility for the accuracy, quality, integrity, legality, reliability, and appropriateness of Your Content, and for obtaining all rights related to Your Content required by Oracle to perform the Services.

3.4 You may not, and may not cause or permit others to: (a) modify, make derivative works of, disassemble, decompile, reverse engineer, reproduce, republish, download or copy any part of the Services (including data structures or similar materials produced by programs); (b) access or use the Services to build or support, directly or indirectly, products or services competitive to Oracle; or (c) license, sell, transfer, assign, distribute, outsource, permit timesharing or service bureau use of, commercially exploit, or make available the Services to any third party except as permitted by the Master Agreement or Your order.

4. NONDISCLOSURE

Your Content residing in the Services will be considered Confidential Information subject to the terms of this section, Section 11 of the General Terms and Your order. Oracle will protect the confidentiality of Your Content residing in the Services for as long as such information resides in the Services. Oracle will protect the confidentiality of Your Content residing in the Services in accordance with the Oracle security practices defined as part of the Service Specifications applicable to Your order.

5. PROTECTION OF YOUR CONTENT

5.1 In order to protect Your Content provided to Oracle as part of the provision of the Services, Oracle will comply with the applicable administrative, physical, technical and other safeguards, and other applicable aspects of system and content management, available at <http://www.oracle.com/us/corporate/contracts/cloud-services/index.html>.

5.2 To the extent Your Content includes Personal Information (as that term is defined in the applicable data privacy policies and the Data Processing Agreement (as that term is defined below)), Oracle will furthermore comply with the following:

- a. the relevant Oracle privacy policies applicable to the Services, available at <http://www.oracle.com/us/legal/privacy/overview/index.html>; and
- b. the *Data Processing Agreement for Oracle Services* (the "Data Processing Agreement"), which is attached hereto as Exhibit A and is incorporated herein by reference, unless stated otherwise in Your order. In the event of any conflict between the terms of the Data Processing Agreement and the terms of the Service Specifications (including any applicable Oracle privacy policies), the terms of the Data Processing Agreement shall take precedence.

The Oracle Services Privacy Policy, current as of the Effective Date of the Master Agreement, is attached hereto as Exhibit B. The Oracle Services Privacy Policy is subject to change, but such changes will not materially reduce the level of security of Your Content.

Attachment E-1

5.3 Without prejudice to Sections 5.1 and 5.2 above, You are responsible for (a) any required notices, consents and/or authorizations related to Your provision of, and our processing of, Your Content (including any Personal Information) as part of the Services, (b) any security vulnerabilities, and the consequences of such vulnerabilities, arising from Your Content, including any viruses, Trojan horses, worms or other harmful programming routines contained in Your Content, and (c) any use by You or Your Users of the Services in a manner that is inconsistent with the terms of the Master Agreement. To the extent You disclose or transmit Your Content to a third party, we are no longer responsible for the security, integrity or confidentiality of such content outside of Oracle's control.

5.4 Unless otherwise specified in Your order (including in the Service Specifications), Your Content may not include any sensitive or special data that imposes specific data security or data protection obligations on Oracle in addition to or different from those specified in the Service Specifications. If available for the Services, You may purchase additional services from us (e.g., Oracle Payment Card Industry Compliance Services) designed to address specific data security or data protection requirements applicable to such sensitive or special data You seek to include in Your Content.

6. WARRANTIES, DISCLAIMERS AND EXCLUSIVE REMEDIES

6.1 Each party represents that it has validly entered into the Master Agreement and that it has the power and authority to do so. We warrant that during the Services Period, we will perform the Services using commercially reasonable care and skill in all material respects as described in the Service Specifications. If the Services provided to You were not performed as warranted, You must promptly provide us with a written notice that describes the deficiency in the Services (including, as applicable, the service request number notifying us of the deficiency in the Services).

6.2 WE DO NOT WARRANT THAT THE SERVICES WILL BE PERFORMED ERROR-FREE OR UNINTERRUPTED, THAT WE WILL CORRECT ALL SERVICES ERRORS, OR THAT THE SERVICES WILL MEET YOUR REQUIREMENTS OR EXPECTATIONS. WE ARE NOT RESPONSIBLE FOR ANY ISSUES RELATED TO THE PERFORMANCE, OPERATION OR SECURITY OF THE SERVICES THAT ARISE FROM YOUR CONTENT OR THIRD PARTY CONTENT OR SERVICES PROVIDED BY THIRD PARTIES.

6.3 FOR ANY BREACH OF THE SERVICES WARRANTY, YOUR EXCLUSIVE REMEDY AND OUR ENTIRE LIABILITY SHALL BE THE CORRECTION OF THE DEFICIENT SERVICES THAT CAUSED THE BREACH OF WARRANTY, OR, IF WE CANNOT SUBSTANTIALLY CORRECT THE DEFICIENCY IN A COMMERCIALY REASONABLE MANNER, YOU MAY END THE DEFICIENT SERVICES AND WE WILL REFUND TO YOU THE FEES PAID FOR THE DEFICIENT SERVICES FOR THE PERIOD OF TIME DURING WHICH THE SERVICES WERE DEFICIENT.

6.4 TO THE EXTENT NOT PROHIBITED BY LAW, THESE WARRANTIES ARE EXCLUSIVE AND THERE ARE NO OTHER EXPRESS OR IMPLIED WARRANTIES OR CONDITIONS INCLUDING FOR SOFTWARE, HARDWARE, SYSTEMS, NETWORKS OR ENVIRONMENTS OR FOR MERCHANTABILITY, SATISFACTORY QUALITY AND FITNESS FOR A PARTICULAR PURPOSE.

7. INTENTIONALLY OMITTED

8. INTENTIONALLY OMITTED

9. TERM AND TERMINATION

9.1 Services shall be provided for the Services Period defined in Your order. Notwithstanding anything to the contrary in the Service Specifications, the Services You order will not be automatically renewed.

We may suspend Your or Your Users' access to, or use of, the Services if we believe that: (a) there is a significant threat to the functionality, security, integrity, or availability of the Services or any content, data, or applications in the Services; (b) You or Your Users are accessing or using the Services to commit an illegal act; or (c) there is a violation of the Acceptable Use Policy. When reasonably practicable and lawfully permitted, we will provide You with advance notice of any such suspension. We will use reasonable efforts to re-establish the Services promptly after we determine that the issue causing the suspension has been resolved. During any suspension period, we will make Your Content (as it existed on the suspension date) available to You. Any suspension under this section shall not excuse You from Your obligation to make payments under the Master

Attachment E-1

Agreement; as Oracle will continue to provide certain Services during the period of suspension, including the protection and security of Your Content as provided herein.

9.2 Intentionally omitted.

9.3 Intentionally omitted.

9.4 At the end of the Services Period, we will make Your Content (as it existed at the end of the Services Period) available for retrieval by You during a retrieval period set out in the Service Specifications. As provided in the Cloud Hosting and Delivery policies and except as otherwise provided in the Services Specifications, for a period of 60 days upon termination of the Oracle Cloud Services, Oracle will make available, via secure protocols and in a structured, machine-readable format, Your Content residing in the production Cloud Services environment, or keep the service system accessible, for the purpose of data retrieval by You.. At the end of such retrieval period, and except as may be required by law, we will delete or otherwise render unrecoverable any of Your Content that remains in the Services. Our data deletion practices are described in more detail in the Service Specifications.

10. THIRD-PARTY CONTENT, SERVICES AND WEBSITES

10.1 The Services may enable You to link to, transfer Your Content or Third Party Content to, or otherwise access third parties' websites, platforms, content, products, services, and information ("Third Party Services"). Oracle does not control and is not responsible for such Third Party Services. You are solely responsible for complying with the terms of access and use of Third Party Services, and if Oracle accesses or uses any Third Party Services on Your behalf to facilitate performance of the Services, You are solely responsible for ensuring that such access and use, including through passwords, credentials or tokens issued or otherwise made available to You, is authorized by the terms of access and use for such services. If You transfer or cause the transfer of Your Content or Third Party Content from the Services to a Third Party Service or other location, that transfer constitutes a distribution by You and not by Oracle.

10.2 Any Third Party Content we make accessible is provided on an "as-is" and "as available" basis without any warranty of any kind. You acknowledge and agree that we are not responsible for, and have no obligation to control, monitor, or correct, Third Party Content. We disclaim all liabilities arising from or related to Third Party Content.

10.3 You acknowledge that: (i) the nature, type, quality and availability of Third Party Content may change at any time during the Services Period; and (ii) features of the Services that interoperate with Third Party Services such as Facebook™, YouTube™ and Twitter™, etc. depend on the continuing availability of such third parties' respective application programming interfaces (APIs). We may need to update, change or modify the Services under the Master Agreement as a result of a change in, or unavailability of, such Third Party Content, Third Party Services or APIs. If any third party ceases to make its Third Party Content or APIs available on reasonable terms for the Services, as determined by us in our sole discretion, we may cease providing access to the affected Third Party Content or Third Party Services without any liability to You. Any changes to Third Party Content, Third Party Services or APIs, including their unavailability, during the Services Period does not affect Your obligations under the Master Agreement or the applicable order, and You will not be entitled to any refund, credit or other compensation due to any such changes.

11. SERVICE MONITORING, ANALYSES AND ORACLE SOFTWARE

11.1 We continuously monitor the Services to facilitate Oracle's operation of the Services; to help resolve Your service requests; to detect and address threats to the functionality, security, integrity, and availability of the Services as well as any content, data, or applications in the Services; and to detect and address illegal acts or violations of the Acceptable Use Policy. Oracle monitoring tools do not collect or store any of Your Content residing in the Services, except as needed for such purposes. Oracle does not monitor, and does not address issues with, non-Oracle software provided by You or any of Your Users that is stored in, or run on or through, the Services. Information collected by Oracle monitoring tools (excluding Your Content) may also be used to assist in managing Oracle's product and service portfolio, to help Oracle address deficiencies in its product and service offerings, and for license management purposes.

11.2 We may (i) compile statistical and other information related to the performance, operation and use of the Services, and (ii) use data from the Services in aggregated form for security and operations management, to create statistical analyses, and for research and development purposes (clauses i and ii are

Attachment E-1

collectively referred to as "Service Analyses"). We retain all intellectual property rights in Service Analyses. For the avoidance of doubt, nothing in this Schedule C shall be deemed to transfer or otherwise assign to Oracle Your ownership rights in and to Your Content or Your Applications.

11.3 We may provide You with the ability to obtain certain Oracle Software (as defined below) for use with the Services. If we provide Oracle Software to You and do not specify separate terms for such software, then such Oracle Software is provided as part of the Services and You have the non-exclusive, royalty free, worldwide, limited right to use such Oracle Software, subject to the terms of the Master Agreement and Your order), solely to facilitate Your use of the Services. You may allow Your Users to use the Oracle Software for this purpose, and You are responsible for their compliance with the license terms. Your right to use any Oracle Software will terminate upon the earlier of 30 days after Oracle's notice (by web posting or otherwise) or the end of the Services associated with the Oracle Software. Notwithstanding the foregoing, if Oracle Software is licensed to You under separate terms, then Your use of such software is governed by the separate terms. Your right to use any part of the Oracle Software that is licensed under the separate terms is not restricted in any way by the Master Agreement.

12. ADDITIONAL EXPORT TERMS

You acknowledge that the Services are designed with capabilities for You and Your Users to access the Services without regard to geographic location and to transfer or otherwise move Your Content between the Services and other locations such as User workstations. You are solely responsible for the authorization and management of User accounts across geographic locations, as well as export control and geographic transfer of Your Content.

13. ADDITIONAL NOTICE TERMS

13.1 Any notice required under the Master Agreement shall be provided to the other party in writing as specified in the General Terms.

13.2 We may give notices applicable to our Services customers by means of a general notice on the Oracle portal for the Services, and notices specific to You by electronic mail to Your e-mail address on record in our account information or by written communication sent by first class mail or pre-paid post to Your address on record in our account information.

14. OTHER

14.1 We are an independent contractor, and each party agrees that no partnership, joint venture, or agency relationship exists between the parties.

14.2 Our business partners and other third parties, including any third parties with which the Services have integrations or that are retained by You to provide consulting services, implementation services or applications that interact with the Services, are independent of Oracle and are not Oracle's agents. We are not liable for, bound by, or responsible for any problems with the Services or Your Content arising due to any acts of any such business partner or third party, unless the business partner or third party is providing Services as our subcontractor on an engagement ordered under the Master Agreement and, if so, then only to the same extent as we would be responsible for our resources under the Master Agreement.

14.3 Prior to entering into an order governed by the Master Agreement, You are solely responsible for determining whether the Services meet Your technical, business or regulatory requirements. Oracle will cooperate with Your efforts to determine whether use of the standard Services are consistent with those requirements. Additional fees may apply to any additional work performed by Oracle or changes to the Services. You remain solely responsible for Your regulatory compliance in connection with Your use of the Services.

14.4 Upon forty-five (45) days written notice and no more than once every twelve (12) months, Oracle may audit Your use of Cloud Services to ensure Your use of the Cloud Services is in compliance with the terms of the applicable order and the Master Agreement. Any such audit shall not unreasonably interfere with Your normal business operations. Oracle shall comply with reasonable security and safety rules, policies, and procedures ("security rules") while performing any such audit, provided that (i) such security rules are applicable to the performance of the audit; (ii) You make such security rules available to Oracle prior to the commencement

Attachment E-1

of the audit; and (iii) such security rules do not modify or amend the terms and conditions of this Master Agreement or the applicable order(s).

You agree to cooperate with Oracle's audit and to provide reasonable assistance and access to information reasonably requested by Oracle.

The performance of the audit and data obtained during the audit (including findings or reports that result from the audit) shall be subject to the provisions of section 4 (Nondisclosure) of this Schedule C.

Any usage in excess of Your rights under the applicable order(s) shall be considered a change to the scope of services of the applicable order(s) and You shall be responsible for paying the additional fees related to use of the Services in excess of Your rights. You agree that Oracle shall not be responsible for any of Your costs incurred in cooperating with the audit.

If You in good faith provide Oracle with written notice of an alleged error in the amount of underpaid fees due Oracle as a result of an audit under this section (the "dispute"), then the parties will endeavor to resolve the dispute in accordance with this paragraph. Each party will appoint a Vice President (or equivalent level) to discuss the dispute and no formal proceedings for the judicial resolution of such dispute, except for the seeking of equitable relief, may begin until either Vice President (or equivalent level) concludes, after a good faith effort to resolve the dispute, that resolution through continued discussion is unlikely. The party concluding that resolution through continued discussion is unlikely will provide notice thereof to the other party. In addition, the parties shall refrain from exercising any termination right and shall continue to perform their respective obligations under the General Terms, this Schedule C and the applicable ordering document(s), while they endeavor to resolve the dispute under this paragraph.

14.5 It is expressly agreed that the terms of the Master Agreement and any Oracle order shall supersede the terms in any purchase order, procurement internet portal, or other similar non-Oracle document and no terms included in any such purchase order, portal, or other non-Oracle document shall apply to the Services ordered. In the event of any inconsistencies between the terms of an order and the Master Agreement, the order shall take precedence except as otherwise provided by Section 2.2 of the Master Agreement; however, unless expressly stated otherwise in an order, the terms of the Data Processing Agreement shall take precedence over any inconsistent terms in an order. The Master Agreement and orders hereunder may not be modified and the rights and restrictions may not be altered or waived except in a writing signed or accepted online by authorized representatives of You and of Oracle; however, Oracle may update the Service Specifications, including by posting updated documents on Oracle's websites. No third party beneficiary relationships are created by the Master Agreement. The Uniform Computer Information Transactions Act does not apply to the Master Agreement or to orders placed under it.

15. AGREEMENT DEFINITIONS

15.1 **"Oracle Software"** means any software agent, application or tool that Oracle makes available to You for download specifically for purposes of facilitating Your access to, operation of, and/or use with, the Services.

15.2 **"Program Documentation"** refers to the user manuals, help windows, readme files for the Services and any Oracle Software. You may access the documentation online at <http://oracle.com/contracts> or such other address specified by Oracle.

15.3 **"Service Specifications"** means the following documents, as applicable to the Services under Your order: (a) the Oracle Cloud Hosting and Delivery Policies, the Program Documentation, the Oracle service descriptions, and the Data Processing Agreement described in this Schedule C; (b) Oracle's privacy policies; and (c) any other Oracle documents that are referenced in or incorporated into Your order. The following do not apply to any non-Cloud Oracle service offerings acquired in Your order, such as professional services: the Oracle Cloud Hosting and Delivery Policies and Program Documentation. The following do not apply to any Oracle Software: the Oracle Cloud Hosting and Delivery Policies, Oracle service descriptions, and the Data Processing Agreement.

15.4 **"Third Party Content"** means all software, data, text, images, audio, video, photographs and other content and material, in any format, that are obtained or derived from third party sources outside of Oracle that You may access through, within, or in conjunction with Your use of, the Services. Examples of Third Party Content include data feeds from social network services, rss feeds from blog posts, Oracle data marketplaces and libraries, dictionaries, and marketing data. Third Party Content includes third-party sourced materials accessed or obtained by Your use of the Services or any Oracle provided tools.

Attachment E-1

15.5 **"Users"** means those employees, contractors, and end users, as applicable, authorized by You or on Your behalf to use the Services in accordance with the Master Agreement and Your order. For Services that are specifically designed to allow Your clients, agents, customers, suppliers or other third parties to access the Cloud Services to interact with You, such third parties will be considered "Users" subject to the terms of the Master Agreement and Your order.

15.6 **"Your Content"** means all software, data (including Personal Information), text, images, audio, video, photographs, non-Oracle or third party applications, and other content and material, in any format, provided by You or any of Your Users that is stored in, or run on or through, the Services. Services under the Master Agreement, Oracle Software, other Oracle products and services, and Oracle intellectual property, and all derivative works thereof, do not fall within the meaning of the term "Your Content". Your Content includes any Third Party Content that is brought by You into the Services, by Your use of the Services or any Oracle provided tools.

15.7 Capitalized terms used but not defined in this Schedule C have the meanings set forth in the General Terms.

Exhibit A

Data Processing Agreement

Data Processing Agreement for Oracle Services

("Data Processing Agreement")

Version January 1, 2023

1. Scope and Applicability

This Data Processing Agreement applies to Oracle's Processing of Personal Information on Your behalf as a Processor for the provision of the Services specified in Your Services Agreement. Unless otherwise expressly stated in Your Services Agreement, this version of the Data Processing Agreement shall be effective and remain in force for the term of Your Services Agreement.

2. Responsibility for Processing of Personal Information and Description of Processing Activities

2.1 You are a Controller and Oracle is a Processor for the Processing of Personal Information as part of the provision of the Services. Each party is responsible for compliance with its respective obligations under Applicable Data Protection Law.

2.2 Oracle will Process Personal Information during the term of the Services Agreement solely for the purpose of providing the Services in accordance with the Services Agreement and this Data Processing Agreement.

2.3 In particular and depending on the Services, Oracle may Process Personal Information for hosting and storage; backup and disaster recovery; service change management; issue resolution; applying new product or system versions, patches, updates and upgrades; monitoring and testing system use and performance; IT security purposes including incident management; maintenance and performance of technical support systems and IT infrastructure; and migration, implementation, configuration and performance testing.

2.4 As part of the provision of the Services and depending on the Services, Oracle may Process Personal Information about Your Individuals, including Your end users, employees, job applicants, contractors, collaborators, partners, suppliers, customers and clients.

2.5 Personal Information about Your Individuals may include, but is not limited to, personal contact information such as name, home address, home telephone or mobile number, fax number, email address, and passwords; information concerning family, lifestyle and social circumstances including age, date of birth, marital status, number of children and name(s) of spouse and/or children; employment details including employer name, job title and function, employment history, salary and other benefits, job performance and other capabilities, education/qualification, identification numbers, and business contact details; financial details; goods and services provided; unique IDs collected from mobile devices, network carriers or data providers; geolocation data; IP addresses and online behavior and interest data.

2.6 Unless otherwise specified in the Services Agreement, You may not provide Oracle with any data that imposes specific data security or data protection obligations on Oracle in addition to or different from those

specified in the Data Processing Agreement or Services Agreement (e.g. certain regulated health or payment card information). If available for the Services, You may purchase additional services from Oracle (e.g., Oracle Payment Card Industry Compliance Services) designed to address specific data security or data protection requirements applicable to sensitive or special data You seek to include in Your Content. You remain responsible for compliance with Your specific regulatory, legal or industry data security obligations which may apply to such data.

2.7 Additional or more specific descriptions of Processing activities may be included in the Services Agreement.

2.8 Oracle is a Service Provider in respect to Personal Information processed in performance of the Services. Oracle will not: (a) Sell or Share any Personal Information; (b) retain, use, or disclose any Personal Information (i) for any purpose other than for the Business Purposes specified in the Services Agreement, including for any Commercial Purpose, or (ii) outside of the direct business relationship between Oracle and You; or (c) combine Personal Information received from or on behalf of You with Personal Information received from or on behalf of any third party, or collected from Oracle's own interaction with Individuals, except to perform a Business Purpose that is permitted by the CCPA and the Services Agreement. Oracle will notify You of its use of Oracle Affiliates and Third Party Subprocessors in accordance with Section 5 of this Data Processing Agreement; and ensure Oracle Affiliates and Third Party Subprocessors are subject to applicable written agreements per Section 5 of this Data Processing Agreement. The parties acknowledge that the Personal Information You disclose to Oracle is provided only for the limited and specified Business Purposes set forth in the Services Agreement. Oracle shall provide the same level of protection to Personal Information as required by the CCPA and as more fully set out in the Services Agreement. You may take such reasonable steps as may be necessary (a) to remediate Oracle's unauthorized use of Personal Information, and (b) to ensure that Personal Information is used in accordance with the terms of this Data Processing Agreement by exercising Your rights under Section 8 of this Data Processing Agreement. Oracle shall notify You if it makes a determination that it is not able to meet its obligations under the CCPA in connection with its provision of the Services.

3. Your Instructions

3.1 In addition to Your instructions incorporated into the Services Agreement, You may provide additional instructions in writing to Oracle with regard to Processing of Personal Information in accordance with Applicable Data Protection Law. Oracle will promptly comply with all such instructions to the extent necessary for Oracle to (i) comply with its Processor obligations under Applicable Data Protection Law; or (ii) assist You to comply with Your Controller obligations under Applicable Data Protection Law relevant to Your use of the Services.

3.2 Oracle will follow Your instructions at no additional cost to You and within the timeframes reasonably necessary for You to comply with your obligations under Applicable Data Protection Law. Oracle will immediately inform You if, in its opinion, Your instruction infringes Applicable Data Protection Law. Oracle is not responsible for providing legal advice to You.

3.3 To the extent Oracle expects to incur additional charges or fees not covered by the fees for Services payable under the Services Agreement, such as additional license or third party contractor fees, it will promptly inform You thereof upon receiving Your instructions. Without prejudice to Oracle's obligation to comply with Your instructions, the parties will then negotiate in good faith with respect to any such charges or fees.

4. Privacy Inquiries and Requests from Individuals

4.1 If You receive a request or inquiry from an Individual related to Personal Information Processed by Oracle under the Services Agreement, including Individual requests to access, delete or erase, restrict, rectify, receive and transmit (data portability), block access to or object to Processing of specific Personal Information, You can securely access Your Services environment that holds Personal Information to address the request. Additional information on how to access the Services to address privacy requests or inquiries from Individuals is available in the applicable Oracle Product or Service Feature Guidance documentation available on My Oracle Support (or other applicable primary support tool or support contact provided for the Services).

4.2 To the extent access to the Services is not available to You or otherwise not responsive to the request or inquiry, You can submit a “service request” via My Oracle Support (or other applicable primary support tool or support contact provided for the Services, such as Your project manager) with detailed written instructions to Oracle on how to assist You with such request.

4.3 If Oracle directly receives any requests or inquiries from Individuals that have identified You as the Controller, it will promptly pass on such requests to You without responding to the Individual. Otherwise, Oracle will advise the Individual to identify and contact the relevant controller(s).

5. Oracle Affiliates and Third Party Subprocessors

5.1 You provide Oracle general written authorization to engage Oracle Affiliates and Third Party Subprocessors as necessary to assist in the performance of the Services.

5.2 To the extent Oracle engages such Third Party Subprocessors and/or Oracle Affiliates, it requires that such entities are subject to the same level of data protection and security as Oracle under the terms of this Data Processing Agreement and Applicable Data Protection Law. You will be entitled, upon written request, to receive copies of the relevant privacy and security terms of Oracle’s agreement with any Third Party Subprocessors and Oracle Affiliates that may Process Personal Information. Oracle remains responsible for the performance of the Oracle Affiliates’ and Third Party Subprocessors’ obligations in compliance with the terms of the Services Agreement.

5.3 Oracle maintains lists of Oracle Affiliates and Third Party Subprocessors that may Process Personal Information. These lists are available via [My Oracle Support](#), Document ID 2121811.1 (or other applicable primary support tool, user interface or contact provided for the Services, such as the [NetSuite Support Portal](#) or Your Oracle project manager). To receive notice of any intended changes to these lists of Oracle Affiliates and Third Party Subprocessors, You can (i) sign up per the instructions on My Oracle Support, Document ID 2288528.1; or (ii) Oracle will provide you notice of intended changes where a sign up mechanism is not available. For ACS and Consulting Services, any additional Third Party Subprocessors that Oracle intends to use will be listed in Your order for ACS or Consulting Services, or in a subsequent “Oracle Subprocessor Notice”, which Oracle will send to you by e-mail as necessary.

5.4 Within thirty (30) calendar days of Oracle providing such notice to You under Section 5.3 above, You may object to the intended involvement of a Third Party Subprocessor or Oracle Affiliate in the performance of the Services by submitting a “service request” via (i) My Oracle Support (or other applicable primary support tool) or (ii) for ACS and Consulting Services, the project manager for the Services. You and Oracle

will work together in good faith to find a mutually acceptable resolution to address such objection, including but not limited to reviewing additional documentation supporting the Third Party Subprocessor's or Oracle Affiliate's compliance with the Data Processing Agreement or Applicable Data Protection Law, or delivering the Services without the involvement of such Third Party Subprocessor. To the extent You and Oracle do not reach a mutually acceptable resolution within a reasonable timeframe, You shall have the right to terminate the relevant Services (i) upon serving thirty (30) days prior notice; (ii) without liability to You or Oracle and (iii) without relieving You from Your payment obligations under the Services Agreement up to the date of termination. If the termination in accordance with this Section 5.4 only pertains to a portion of Services under an order, You will enter into an amendment or replacement order to reflect such partial termination.

6. Cross-border data transfers

6.1 For Cloud Services, Personal Information will be stored in the data center region specified in Your order for such Services or, if applicable, the geographic region that You have selected when activating the production instance of such Services.

6.2 Without prejudice to Section 6.1 above, Oracle may Process Personal Information globally as necessary to perform the Services, such as for support, incident management or data recovery purposes.

6.3 To the extent such global access involves a transfer of Personal Information subject to cross-border transfer restrictions under Applicable European Data Protection Law to countries outside Europe not covered by an adequacy decision, such transfers are subject to (i) Oracle's Binding Corporate Rules for Processors or BCR-p (also referred to as the Oracle Processor Code) and (ii) the terms of Module 2 (Controller to Processor) of the EU Standard Contractual Clauses 2021/914 of 4 June 2021.

The most current version of Oracle's Binding Corporate Rules for Processors (Oracle Processor Code) is available on <https://www.oracle.com/corporate/contracts/cloud-services/contracts.html#data-processing>, and is incorporated by reference into the Services Agreement and this Data Processing Agreement. Oracle has obtained EEA authorization for its Binding Corporate Rules for Processors (Processor Code) and will maintain such authorization for the duration of the Services Agreement. Transfers to Third Party Subprocessors shall be subject to security and data privacy requirements consistent with Oracle's Binding Corporate Rules for Processors (Oracle Processor Code), the terms of Module 2 (Controller to Processor) of the EU Standard Contractual Clauses 2021/914 of 4 June 2021, this Data Processing Agreement and the Services Agreement.

6.4 To the extent such global access involves a transfer of Personal Information subject to cross-border transfer restrictions under Applicable UK Data Protection Law, to countries outside the United Kingdom not covered by an Adequacy Decision by the UK ICO, such transfers are subject to (i) the terms of Module 2 (Controller to Processor) of the EU Standard Contractual Clauses 2021/914 of 4 June 2021 as supplemented by the International Data Transfer Addendum to the EU Commission Standard Contractual Clauses version B1.0 (the "IDTA"), which are incorporated herein by reference; and (ii) when approved by the UK ICO, the approved UK Binding Corporate Rules for Processors, in the form that will be approved by the UK ICO for use in the UK and will be published on Oracle's public websites. The IDTA will be read in conjunction with the Services Agreement and the Data Processing Agreement.

6.5 The parties will review any supplemental measures, which may be required based on applicable Data Protection Law for the transfer of Personal Information to countries that do not offer an adequate level of

protection. The parties will work together in good faith to find a mutually acceptable resolution to address such supplementary measures, including but not limited to reviewing technical documentation for the Services, and discussing additional available technical safeguards and security services.

6.6 To the extent such global access involves a transfer of Personal Information subject to cross-border transfer restrictions under other Applicable Data Protection Laws globally, such transfers shall be subject to (i) for transfers to Oracle Affiliates, the terms of the Oracle Intra-Company Data Transfer and Mandate Agreement, which requires all transfers of Personal Information to be made in compliance with Applicable Data Protection Law and all applicable Oracle security and data privacy policies and standards globally; and (ii) for transfers to Third Party Subprocessors, security and data privacy requirements consistent with the relevant requirements of this Data Processing Agreement and Applicable Data Protection Law.

7. Security and Confidentiality

7.1 Oracle has implemented and will maintain appropriate technical and organizational security measures for the Processing of Personal Information designed to prevent accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Personal Information. These security measures govern all areas of security applicable to the Services, including physical access, system access, data access, transmission and encryption, input, data backup, data segregation and security oversight, enforcement and other security controls and measures. Additional details regarding the specific security measures that apply to the Services You have ordered are set out in the relevant security practices for these Services:

- For **all Services**: Oracle's Corporate Security Practices, available at <https://www.oracle.com/corporate/security-practices/>;
- For **Cloud Services**: Oracle's Hosting & Delivery Policies, available at <http://www.oracle.com/us/corporate/contracts/cloud-services/index.html>;
- For **NetSuite (NSGBU) Services**: NetSuite's Terms of Service, available at: <http://www.netsuite.com/portal/resource/terms-of-service.shtml>;
- For **Global Customer Support Services**: Oracle's Global Customer Support Security Practices available at: <https://www.oracle.com/support/policies.html>;
- For **Consulting and Advanced Customer Support (ACS) Services**: Oracle's Consulting and ACS Security Practices available at: <http://www.oracle.com/us/corporate/contracts/consulting-services/index.html>.

7.2 All Oracle and Oracle Affiliates employees, and Third Party Subprocessors that Process Personal Information, are subject to appropriate written confidentiality arrangements, including confidentiality agreements, regular training on information protection, and compliance with Oracle policies concerning protection of confidential information.

8. Audit Rights and Assistance with Data Protection Impact Assessments

8.1 You may audit Oracle's compliance with its obligations under this Data Processing Agreement up to once per year, including inspections of the applicable Services data center facility that hosts Personal Information. In addition, to the extent required by Applicable Data Protection Law, You or Your Regulator may perform more frequent audits.

8.2 If You engage a third party auditor, the third party must be mutually agreed to by You and Oracle

(except if such third party is a Regulator). Oracle will not unreasonably withhold its consent to a third party auditor requested by You. The third party must execute a written confidentiality agreement acceptable to Oracle or otherwise be bound by a statutory or legal confidentiality obligation.

8.3 To request an audit, You must submit a detailed proposed audit plan to Oracle at least two weeks in advance of the proposed audit date. The proposed audit plan must describe the proposed scope, duration, and start date of the audit. Oracle will review the proposed audit plan and provide You with any concerns or questions. Oracle will work cooperatively with You to agree on a final audit plan within a reasonable timeframe.

8.4 The audit must be conducted during regular business hours at the applicable facility, subject to the agreed final audit plan and Oracle's health and safety or other relevant policies, and may not unreasonably interfere with Oracle business activities.

8.5 Upon completion of the audit, You will provide Oracle with a copy of the audit report, which is subject to the confidentiality terms of Your Services Agreement. You may use the audit reports only for the purposes of meeting Your regulatory audit requirements and/or confirming compliance with the requirements of this Data Processing Agreement.

8.6 Each party will bear its own costs in relation to the audit, unless Oracle promptly informs you upon reviewing Your audit plan that it expects to incur additional charges or fees in the performance of the audit that are not covered by the fees payable under Your Services Agreement, such as additional license or third party contractor fees. The parties will negotiate in good faith with respect to any such charges or fees.

8.7 Without prejudice to the rights granted in Section 8.1 above, if the requested audit scope is addressed in a SOC, ISO, NIST, PCI DSS, HIPAA or similar audit report issued by a qualified third party auditor within the prior twelve months and Oracle provides such report to You confirming there are no known material changes in the controls audited, You agree to accept the findings presented in the third party audit report in lieu of requesting an audit of the same controls covered by the report.

8.8 You may also request that Oracle audit a Third Party Subprocessor or provide confirmation that such an audit has occurred (or, where available, obtain or assist You in obtaining a third-party audit report concerning the Third Party Subprocessor's operations) to verify compliance with the Third Party Subprocessor's obligations.

8.9 Oracle provides You with information and assistance reasonably necessary for You to conduct Your data protection impact assessments or consult with Your Regulator(s), by granting You electronic access to a record of Processing activities and Oracle Product/Service privacy & security functionality guides for the Services. This information is available via (i) My Oracle Support, Document ID 111.1 or other applicable primary support tool provided for the Services, such as the [NetSuite Support Portal](#), or (ii) upon request, if such access to My Oracle Support (or other primary support tool) is not available to You.

9. Incident Management and Breach Notification

9.1 Oracle has implemented controls and policies designed to detect and promptly respond to incidents that create suspicion of or indicate destruction, loss, alteration, unauthorized disclosure or access to Your Content (as such term is defined in the Services Agreement) transmitted, stored or otherwise Processed. Oracle will promptly define escalation paths to investigate such incidents in order to confirm if an

Information Breach has occurred, and to take reasonable measures designed to identify the root cause(s) of the Information Breach, mitigate any possible adverse effects and prevent a recurrence.

9.2 Oracle will notify you of a confirmed Information Breach without undue delay but at the latest within 24 hours. As information regarding the Information Breach is collected or otherwise reasonably becomes available to Oracle, Oracle will also provide You with (i) a description of the nature and reasonably anticipated consequences of the Information Breach; (ii) the measures taken to mitigate any possible adverse effects and prevent a recurrence; and (iii) where possible, information about the types of information that were the subject of the Information Breach. You agree to coordinate with Oracle on the content of Your intended public statements or required notices for the affected Individuals and/or notices to the relevant Regulators regarding the Information Breach.

10. Return and Deletion of Personal Information

10.1 Upon termination of the Services, Oracle will promptly return, including by providing available data retrieval functionality, and subsequently delete any remaining copies of Personal Information on Oracle systems or Services environments, except as otherwise stated in the Services Agreement.

10.2 For Personal Information held on Your systems or environments, or for Services for which no data retrieval functionality is provided by Oracle as part of the Services, You are advised to take appropriate action to back up or otherwise store separately any Personal Information while the production Services environment is still active prior to termination.

11. Legal Requirements

11.1 Oracle may be required by law to provide access to Personal Information, such as to comply with a subpoena or other legal process, or to respond to government requests, including public and government authorities for national security and/or law enforcement purposes.

11.2 Oracle will promptly inform You of requests to provide access to Personal Information and use reasonable efforts to redirect the authority that made the request to You, unless otherwise required by law.

11.3 To the extent Oracle is required to respond to the request, it will first assess on a case-by-case basis whether the request is legally valid and binding on Oracle, including whether the request is consistent with Applicable Data Protection Law. Any request that is not legally valid and binding on Oracle will be resisted in accordance with applicable law.

12. Data Protection Officer

12.1 Oracle has appointed a Chief Privacy Officer and a local Data Protection Officer in certain countries. Further details on how to contact Oracle's Chief Privacy Officer and, where applicable, the local Data Protection Officer, are available at <https://www.oracle.com/legal/privacy/index.html>.

12.2 If You have appointed a Data Protection Officer, You may request Oracle to include the contact details of Your Data Protection Officer in the relevant Services order.

13. Definitions

“Applicable Data Protection Law” means all data privacy or data protection laws or regulations globally that apply to the Processing of Personal Information under this Data Processing Agreement, including Applicable European Data Protection Law, Applicable UK Data Protection Law, the California Consumer Privacy Act as amended (“CCPA”) and other US State laws.

“Applicable European Data Protection Law” means (i) the EU General Data Protection Regulation EU/2016/679, as supplemented by applicable EU Member State law and as incorporated into the EEA Agreement; and (ii) the Swiss Federal Act of 19 June 1992 on Data Protection, as amended.

“Applicable UK Data Protection Law” means (i) the UK GDPR, meaning the EU General Data Protection Regulation EU/2016/679, as it forms part of the law of England and Wales, Scotland and Northern Ireland by virtue of section 3 of the European Union (Withdrawal) Act 2018 pursuant to amendments to the EU General Data Protection Regulation EU/2016/679 made by The Data Protection, Privacy and Electronic Communications (Amendments etc.) (EU Exit) Regulations 2019 and 2020; and (ii) the UK Data Protection Act 2018, as amended.

“Europe” means for the purposes of this Data Processing Agreement (i) the European Economic Area, consisting of the EU Member States, Iceland, Liechtenstein and Norway; and (ii) Switzerland.

“Individual” shall have the same meaning as the term “data subject” or the equivalent term under Applicable Data Protection Law.

“Information Breach” means a breach of security leading to the misappropriation or accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Your Content transmitted, stored or otherwise Processed on Oracle systems or the Services environment that compromises the security, confidentiality or integrity of Your Content.

“Process/Processing”, “Controller”, “Processor” and “Binding Corporate Rules” (or the equivalent terms) have the meaning set forth under Applicable Data Protection Law.

“Service Provider”, “Sell”, “Share”, “Business Purpose”, and “Commercial Purpose” have the meaning set forth under the CCPA.

“Oracle Affiliate(s)” means the subsidiar(y)(ies) of Oracle Corporation that may Process Personal Information as set forth in this Data Processing Agreement.

“Oracle Intra-Company Data Transfer and Mandate Agreement” means the Oracle Intra-Company Data Transfer and Mandate Agreement for Customer Services Personal Information entered into between Oracle Corporation and the Oracle Affiliates.

“Oracle Binding Corporate Rules for Processors” or “Oracle Processor Code” means the EU or UK Oracle’s Privacy Code for Processing Personal Information of Customer Individuals, as the case may be.

“Oracle” means the Oracle Affiliate that has executed the Services Agreement.

“Personal Information” shall have the same meaning as the term “personal data”, “personally identifiable

information (PII)” or the equivalent term under Applicable Data Protection Law.

“**Regulator**” shall have the same meaning as the term “supervisory authority”, “data protection authority” or the equivalent term under Applicable Data Protection Law.

“**Services**” or the equivalent terms “Service Offerings” or “services” means the Cloud, Advanced Customer Support, Consulting, or Global Technical Support services specified in the Services Agreement.

“**Services Agreement**” means (i) the applicable order for the Services you have purchased from Oracle; (ii) the applicable master agreement referenced in the applicable order, and (iii) the Service Specifications.

“**Third Party Subprocessor**” means a third party, other than an Oracle Affiliate, which Oracle subcontracts with and which may Process Personal Information as set forth in this Data Processing Agreement.

“**You**” means the customer entity that has executed the Services Agreement.

Other capitalized terms have the definitions provided for them in the Services Agreement.

Exhibit B

Oracle Services Privacy Policy

Oracle Legal /

Oracle Legal

Legal Notices

[Privacy Policies](#)[Terms of Use](#)[Copyright](#)[Trademarks](#)[Logos](#)[More](#)[Privacy Policies Menu](#)

Privacy @ Oracle

Oracle General Privacy Policy

1. INTRODUCTION

This **General Oracle Privacy Policy** (also referred to as the '**Privacy Policy**') provides information on the collection, use, and sharing (collectively referred to '**processing**' or '**process**') as of personal information by Oracle Corporation and its affiliates ("Oracle", "we" or "us") in connection with your use of Oracle websites, mobile applications, and social media pages that link to this Privacy Policy, your interactions with Oracle during in-person meetings at Oracle facilities or at Oracle events, and in the context of other online or offline sales and marketing activities. This Privacy Policy also explains the privacy rights you have in relation to these processing activities.

This Privacy Policy was last updated on July 7, 2023. However, the Privacy Policy can change over time, for example to comply with legal requirements or to meet changing business needs. The most up-to-date version can be found on this [website](#). In case there is an important change that we want to highlight to you, we will also inform you in another appropriate way (for example via a pop-up notice or statement of changes on our website). See the [previous version](#) of this Privacy Policy.

As used in this Privacy Policy, 'personal information' or 'personal data' means information that relates to an identified individual or to an identifiable individual. For example, this could include among other things your name, address, email address, business contact details, or information gathered through your interactions with us via our websites or at events. Personal information is also referred to as '**information about you.**' For more detail about the types of information about you that we may process, please refer to [Section 4](#) below.

[SCOPE OF THE PRIVACY POLICY](#)[See More](#)

This Privacy Policy applies to the processing of personal information by Oracle visitors and users of the various Oracle sites, attendees of Oracle events, customers and prospective customers and their representatives; subscribers to Oracle publications or newsletters; visitors to Oracle facilities and suppliers and business partners and their representatives.

WHO IS RESPONSIBLE FOR PROCESSING YOUR PERSONAL INFORMATION?

[See More](#)

Oracle Corporation and its affiliated entities are responsible for the processing of your personal information as described in this Privacy Policy.

WHICH CATEGORIES OF PERSONAL INFORMATION DO WE PROCESS?

[See More](#)

Oracle processes information about you that directly identifies you, such as name, email, and address, and information about you that may only indirectly identify you such as device identifiers or online activity when not associated with your name.

WHERE DO WE SOURCE YOUR PERSONAL INFORMATION?

[See More](#)

Oracle can process information about you collected directly from you both offline and online, including when you create an Oracle account to access Oracle products and services or attend an Oracle-sponsored event. Information about you may also be provided by third party sources, such as data aggregators who may not have a relationship with you or by third parties who collect information about you on behalf of Oracle such as when you download a whitepaper.

WHY AND HOW DO WE USE YOUR PERSONAL INFORMATION?

[See More](#)

We use your personal information to respond to your requests; to deliver functionality on our sites; to administer our subscriptions; to market and tailor products and services to your or your company's interests; to engage in transactions with and process orders; to develop, improve the performance of, and secure our sites, products and services; and to comply with applicable laws such as to comply with an opt-out request.

HOW CAN WE DISCLOSE YOUR PERSONAL INFORMATION?

[See More](#)

Your personal information is disclosed for business and commercial purposes throughout Oracle's organization and with third parties such as distributors or resellers, event co-hosts and sponsors, service providers, and, when required by law, public, government, judicial and law enforcement entities.

WHAT ARE YOUR PRIVACY RIGHTS?

[See More](#)

You have privacy rights for the information we process about you. You can choose to opt-out of third party sharing, object to, or restrict our use of your personal information, delete, change or correct your personal information or access your personal information by filling out our [inquiry form](#). If your inquiry relates to an Oracle service account or support of Oracle products or services, please go to the [Contact Oracle](#) page for resources and contact information to administer service account data.

HOW TO CONTACT ORACLE IF YOU HAVE QUESTIONS, COMMENTS OR COMPLAINTS?

[See More](#)

If you believe your personal information has been used in a way that is not consistent with the Privacy Policy, please contact the Global Data Protection Officer.

2. SCOPE

This Privacy Policy applies to the processing of personal information by Oracle of:

- visitors and users of the various Oracle sites, including our websites on [oracle.com](#), computer or mobile software applications and our social media pages that link to this Privacy Policy (collectively referred to as the **sites**);
- attendees of Oracle events, such as Oracle CloudWorld, or Oracle-sponsored events;
- customers and prospective customers and their representatives;
- subscribers to Oracle publications and newsletters;
- visitors to Oracle facilities; and
- suppliers and business partners and their representatives.

The Privacy Policy does not apply to the following activities:

Personal information collected about you by Oracle customers. Oracle customers are responsible for their own personal information collection and processing practices, including when customers use Oracle products or services to process your personal information. To find out more about our customers' use of personal information about you, you are encouraged to review the relevant privacy policy of the company who collected your information from you. Please consult that company directly if you have any further questions about its use of information about you.

Personal information processed by Oracle to provide Cloud, Technical Support, Consulting/ACS or other services to Oracle customers. "Services personal information" is personal information processed by Oracle on behalf of a customer in order to provide and perform contracted services. If you are an Oracle customer and Oracle is processing personal information on behalf of your company, please refer to the Services Privacy Policy for information on how Oracle processes services personal information, available at <https://www.oracle.com/legal/privacy/services-privacy-policy.html>.

Personal information you provide on third party sites not controlled by Oracle. When interacting with our websites, you also have the ability to link or connect with non-Oracle websites, services, social networks, applications or other features. Enabling these features will lead to other parties than Oracle processing information about you. Oracle does not have any control over these features of other parties. We encourage you to review the privacy policies of these parties before using these features.

3. WHO IS RESPONSIBLE FOR YOUR PERSONAL INFORMATION?

Oracle Corporation and its affiliated entities are responsible for processing your personal information described in this Privacy Policy. See the list of [Oracle entities](#). Please select a region and country to view the registered address and contact details of the Oracle entity or entities located in each country.

4. WHICH CATEGORIES AND SPECIFIC PIECES OF PERSONAL INFORMATION DO WE PROCESS?

Oracle can process information about you collected directly from you both offline and online, including when you create an Oracle account to access Oracle products and services or attend an Oracle-sponsored event. Information about you may also be provided to Oracle by selected third party sources, such as data aggregators who may not have a direct relationship with you or by third parties who collect information about you on behalf of Oracle such as when you download an Oracle whitepaper.

Specific pieces of information about you that Oracle may collect and process depending on your interaction with Oracle, includes:

- name and physical address, email addresses, and telephone numbers;
- demographic attributes, when tied to personal information that identifies you;
- photographs that identify you and testimonials;
- public information about your work and education history, including professional affiliations;
- information you provide on your public social media profiles related to your professional and educational history, such as LinkedIn;
- transactional data, including products and services ordered, financial details and payment methods;
- company data such as the name, size and location of the company you work for and your role within the company as well as publicly available company information and activity associated with company data;
- data from surveys conducted by Oracle or by third parties on behalf of Oracle and publicly available information, such as social media posts;
- call recording and chat transcript data from Sales and customer support calls and live chat sessions or interviews;
- unique IDs such as your mobile device identifier or cookie ID on your browser;
- IP address and information that may be derived from IP address, such as geographic location;
- information about a device you use, such as browser, device type, operating system, the presence or use of “apps”, screen resolution, and the preferred language;
- certain location or geolocation information you provide directly or through automated means, if you choose to enable location based services from your device or Oracle app; and

behavioral data of the internet connected computer or device you use when interacting with the sites, such as advertisements clicked or viewed, sites and content areas, date and time of activities or the web search used to locate and navigate to a site.

Certain online information about you or device information may originate from the use of cookies and similar technologies (for example, pixel tags and device identifiers) on our sites or sites of third parties. For more information on cookies and similar technologies, please see [Section 11](#) below.

Please note that Oracle does not control the content that you may post to Oracle Communities forums or social networks; in some cases, such content may be publicly available on the Internet. You should carefully consider whether you wish to submit personal information to these forums or social networks and whether you wish to make your profile available to other users, and you should tailor any content you may submit accordingly.

5. WHY AND HOW DO WE USE YOUR PERSONAL INFORMATION?

We may use personal information for the following business purposes:

- to communicate and respond to your requests and inquiries to Oracle;
- to create and administer an Oracle single sign-on (SSO) account (also referred to as an 'Oracle Account') and to deliver functionality on our sites and for their technical and functional management;
- to engage in transactions with customers, suppliers and business partners and to process orders for Oracle products and services;
- to analyze, develop, improve and optimize the use, function and performance of our sites and products and services;
- to manage the security and operation of our sites, facilities, and networks and systems; and
- to comply with applicable laws and regulations and to operate our business.

We may use personal information for the following commercial purposes:

- to administer subscriptions of Oracle publications and newsletters;
- to market our products and services or related products and services, and to tailor our marketing and sales activities to your or your company's interests; and
- to provide select business-to-business services to Oracle customers using publicly available information about companies which may include personal information such as the name of a company's CEO that is publicly available.

These purposes are described below in further detail.

To communicate and respond to your requests and inquiries to Oracle

If you get in touch with us (such as by submitting contact forms on our sites, reaching out to us via Oracle Sales chat, attending Oracle events or other occasions, sending an email or by visiting social media platforms), we process information about you to communicate with you and to respond to your requests or other inquiries. We can also process personal information to interact with you on third party social networks.

To create an Oracle SSO account and deliver functionality on our sites and for their technical and functional management

When you choose to register with us (such as to make use of our communities), we need to process the personal information provided by you so that we can create an Oracle account for you. Please note, this only applies to personal information controlled by Oracle, not personal information Oracle processes on behalf of our customers.

To engage in transactions with customers, suppliers and business partners and to process purchases of our products and services

If you place an order for our products and services, or if you provide services to Oracle, our employees, customers or partners as a supplier or business partner, Oracle processes information about you to engage in and administer the relevant transactions (such as by sending invoices and making payments), administer your order, and help you get started and adopt our products and services (e.g., by contacting you to activate your Cloud services credits). If you download products or services from our sites, Oracle uses information about you to confirm certain information about your order (for example, that you did not experience problems in the download process).

To analyze, develop, improve and optimize the use, function and performance of our sites and products and services

We may process personal information in order to analyze, develop, improve and optimize the use, function and performance of our sites and products and services, including for quality assurance and training purposes, as well as for marketing and sales campaigns. This includes processing personal information to conduct surveys to improve Oracle products and services. In case the sites permit you to participate in interactive discussions, create a profile, post comments, opportunities or other content, or communicate directly with another user or otherwise engage in networking activities on Oracle sites, Oracle may process personal information when moderating these activities.

To manage the security of our sites, facilities, networks and systems

We may collect site use data for security and operations management to help keep our sites, facilities, networks and systems secure, or to investigate and prevent potential fraud, including ad fraud and cyber-attacks and to detect bots.

To comply with applicable laws and regulations and to operate our business

In some cases, we have to process personal information to comply with applicable laws and regulations. For example, to respond to a request from a regulator or to defend a legal claim. We may also process personal information in the performance and operation of our business, such as to conduct internal audits and investigations or for finance and accounting and archiving and insurance purposes.

To administer subscriptions of Oracle publications and newsletters

If you subscribe to our magazines (such as “Oracle” or “Profit”), we process information about you to administer your subscription to our magazines (including the renewal process) and newsletters.

To market our products, services, events, or related products and services and to tailor marketing and sales activities

Oracle may use information about you to notify you about new product releases and service developments, events, alerts, updates, prices, terms, special offers and associated campaigns and promotions (including via newsletters). Oracle may also use personal information to advertise Oracle’s products and services or related products and services, and also to have our distributors, resellers or partners notify you about our products or services or their related products or services (such as via joint sales or product promotions). We do our best to tailor your website visit, marketing experience and our communications to your expressed interests. This happens,

for example, if you sign up for an Oracle community or program like the Oracle Partner Network or Oracle Technology Network.

If you attend an event, Oracle may process information about you gathered in relation to the event and can share information about your attendance with your company. Oracle may also permit designated event partners or conference sponsors to send you up to two communications related to your event attendance. Please note that our partners or conference sponsors may directly request information about you at their conference booths or presentations, and their use of your information that you provide to them will be subject to their privacy policies.

We may also process your personal information to post testimonials on our sites, but will first obtain your consent to use your name and testimonial.

To provide select services to Oracle customers using publicly-available information which may include personal information such as the name of a company's CEO

For some business-to-business services, we may collect the publicly available names of company directors and officials to better understand the status of these companies and help inform our services which relate to providing customers information about other companies.

6. WHAT IS OUR BASIS FOR PROCESSING INFORMATION ABOUT YOU?

For personal information collected about you in the EU/EEA, the UK and other relevant jurisdictions, our basis for processing is the following:

We rely on our **legitimate interest** in processing contact and related information about you in order to communicate adequately with you, to respond to your requests, and to tailor our marketing and sales activities to your professional interests.

In order to engage in transactions with customers, suppliers and business partners, and to process purchases and downloads of our products and services, we need to process information about you **as necessary to enter into or perform a contract** with you.

We process personal information for marketing and sales activities (including events) based on your **consent** where so indicated on our sites at the time your personal information was collected, or further to our **legitimate interest** to keep you updated on developments around our products and services which may be of interest to you.

We rely on our **legitimate interest** to analyze, develop, improve and optimize our sites, facilities, products and services, and to maintain the security of our sites, networks and systems.

In order **to comply with applicable laws and regulations**, such as to comply with a subpoena or other legal process, or to process an opt-out request.

7. FOR WHAT PERIOD DO WE RETAIN PERSONAL INFORMATION

Oracle maintains personal information for the following retention periods:

Information about you we collect to engage in transactions with our customers, suppliers and business partners, and to process purchases of our products and services, will be retained for the duration of the transaction or services period, or longer as necessary for record retention and legal compliance purposes.

If you have registered for an Oracle SSO account (Oracle Account) to access Oracle sites or to sign up for Oracle marketing materials, your account information will be retained for as long as you maintain an active

account. Your account and account information will be deleted if you do not log in for 18 consecutive months. Oracle retains records of that deletion for 90 days.

If you opened an Oracle Cloud account, your account information will be retained for as long as you maintain an active account. After service termination, minimal account information will be held for records retention purposes. Please note the Oracle Privacy team cannot delete, correct, or access service account data or terminate your contracted Oracle product or service account. Please refer to the [Contact Oracle](#) page for resources and contact information to administer service account data.

If you have registered for our newsletters and blogs, including Oracle magazine or Profit magazine, your subscription data will be retained for as long as you are subscribed to our distribution lists. Oracle retains records of that deletion for 30 days.

Contact information such as your email address or phone number collected online on our sites or offline from our interactions with you at Oracle events and conferences, and used for direct marketing and sales activities will be retained for as long as we have an active (customer) relationship with you.

If you have reached out to us via Oracle Sales chat, we will delete all chat transcripts 90 days after the chat has concluded.

If you have reached out to us via our support line and you have not opted out of call recording, we will delete call recordings 60 days after the call has concluded unless otherwise specified during the call.

If you have visited an Oracle facility, the personal information needed to allow you to enter the facility will be held for one year after your last visit for records retention purposes.

Personal information needed to retain your opt-out preferences is retained for 20 years (or longer as necessary to comply with applicable law).

8. WHEN AND HOW CAN WE DISCLOSE YOUR PERSONAL INFORMATION?

Sharing within Oracle

As a global organization, information about you may be shared globally throughout Oracle's worldwide organization. See the list of [Oracle entities](#). Please select a region and country to view the registered address and contact details of the Oracle entity or entities located in each country.

Oracle employees are authorized to access personal information only to the extent necessary to serve the applicable purpose(s) and to perform their job functions.

Disclosing personal information to third parties

We may disclose personal information with the following third parties for a business purpose:

Third-party service providers (for example, credit card processing services, order fulfillment, analytics, event/campaign management, website management, information technology and related infrastructure provision, customer service, e-mail delivery, auditing, and other similar service providers) in order for those service providers to perform business functions on behalf of Oracle;

Relevant third parties in the event of a reorganization, merger, sale, joint venture, assignment, transfer or other disposition of all or any portion of our business, assets or stock (including in connection with any bankruptcy or similar proceedings);

As required by law, such as to comply with a subpoena or other legal process, when we believe in good faith that disclosure is necessary to protect our rights, protect your safety or the safety of others,

investigate fraud, or respond to government requests, including public and government authorities outside your country of residence, for national security and/or law enforcement purposes.

We may share personal information with the following third parties for a commercial purpose:

Oracle distributors or resellers for further follow-up related to your interests, specific partners that offer complementary products and services or with third parties to facilitate interest-based advertising; and

Event partners or conference sponsors for Oracle events such as when you scan your badge at a sponsored booth.

When third parties are given access to personal information, we will take appropriate contractual, technical and organizational measures designed to ensure that personal information is processed only to the extent that such processing is necessary, consistent with this Privacy Policy, and in accordance with applicable law.

9. HOW IS PERSONAL INFORMATION HANDLED GLOBALLY?

Oracle is a global corporation with operations in over 80 countries and personal information is processed globally as necessary in accordance with this policy. If personal information is transferred to an Oracle recipient in a country that does not provide an adequate level of protection for personal information, Oracle will take adequate measures designed to protect the personal information, such as ensuring that such transfers are subject to the terms of the EU Model Clauses or other adequate transfer mechanism as required under relevant data protection laws. Additional country-specific information on data transfers may be provided if you sign up for an Oracle SSO account (Oracle Account) or register for an event.

10. HOW IS YOUR PERSONAL INFORMATION SECURED?

Oracle has implemented appropriate technical, physical and organizational measures designed to protect personal information against accidental or unlawful destruction or accidental loss, damage, alteration, unauthorized disclosure or access, as well as all other forms of unlawful processing.

11. WHAT COOKIES AND SIMILAR TECHNOLOGIES DO WE USE ON OUR SITES?

Cookies and similar technologies (e.g., pixels tags and device identifiers) are used by Oracle and our advertising technology partners to recognize you and/or your device(s) on, off and across different services and devices for the purposes specified in [Section 5](#) above.

When do we use cookies and similar technologies?

Cookies are small text files that contain a string of characters and uniquely identify a browser on a device connected to the Internet. We place cookies in your browser when you visit Oracle sites and non-Oracle sites that host our plugins or tags. Depending on your jurisdiction, you may be presented with different consent options, including the option to reject all non-essential cookies, prior to Oracle placing cookies on your browser. Visitors from all jurisdictions are provided with functionality to opt out of non-required cookies using the [cookie preferences tool](#).

We use cookies and other technologies on all our sites to ensure the best possible and secure experience on our sites and to provide you with tailored information on products and services. Oracle also uses cookies or similar technologies on its sites to collect online information such as your mobile device ID, IP address, and other

information about your device, as well as behavioral data of your device usage on our sites (e.g. pages viewed, links clicked, documents downloaded).

How can I manage my cookie preferences?

If you are a visitor to our sites, you can use our [cookie preferences tool](#) to opt out of cookies that are not required to enable core site functionality, such as advertising and functional cookies.

You can also access the [Oracle Advertising opt-out tool](#) to opt out of interest based advertising by Oracle and other participating advertising technology companies serving interest-related ads to you on behalf of Oracle. Please note that the Oracle Advertising opt-out tool will only work on the Internet browser on which they are deposited, and they will only function only if your browser is set to accept third-party cookies.

If you do not want to receive cookies, you can also change your **browser settings** on your computer or other device you are using to access our services. Most browsers also provide functionality that lets you review and delete cookies, including Oracle cookies.

12. WHAT ARE YOUR PRIVACY RIGHTS?

You can exercise your privacy rights in accordance with applicable laws as specified on our [Privacy Choices page](#), or by filling out our [inquiry form](#). You have multiple privacy rights, subject to applicable law, in respect of the information we process about you:

Opt-out of our use or sharing of your personal information

You may withdraw consent you have previously provided for the processing of information about you, including for email marketing by Oracle.

Delete personal information

You can ask us to erase or delete all or some of the information about you.

Change or correct personal information

You can edit some of the information about you by. You can also ask us to change, update or fix information about you in certain cases, particularly if it is inaccurate.

Object to, or limit or restrict use of personal information

You can ask us to stop using all or some of the information about you (for example, if we have no legal right to keep using it) or to limit our use of it (for example, if the information about you is inaccurate).

Right to access and/or have your information provided to you

You can also ask us for a copy of information about you and can ask for a copy of information about you provided in machine readable form if you reside in the EU, California or other jurisdiction that provides you this right as a matter of law.

If you are authorized to make an access or deletion request on behalf of a data subject, please reach out to us via the inquiry form and indicate that you are an authorized agent. We will provide you with instructions on how to submit a request as an authorized agent on behalf of a data subject.

In the event you have previously created an account for a certain [Oracle portal](#), you can access and manage your personal information stored in these portals (i) by clicking the links and following the corresponding instructions, and (ii) taking the actions within each portal with regards to your personal information, such as updating your contact details, deleting certain entries or records, or downloading a copy of your profile. Please note that these actions are available to the extent permitted by each portal's functionality.

If your inquiry relates to your company's service account or support of Oracle products or services, please note the Oracle Privacy team cannot delete, correct, or access service account data or terminate your contracted Oracle

product or service account. Please go to the [Contact Oracle](#) page for resources and contact information to administer service account data.

13. DO YOU COLLECT SENSITIVE INFORMATION AND INFORMATION FROM CHILDREN?

Sensitive personal information

We ask that you do not send us, and do not share any sensitive personal information (for example, government-issued IDs, information related to racial or ethnic origin, political opinions, religion or other beliefs, health, genetic, or biometric data, criminal background or trade union membership).

Children's privacy

As a company focused on serving the needs of businesses, Oracle's sites are not directed to minors and Oracle does not promote or market its services to minors, except in very limited circumstances as part of specific educational outreach programs with parental permission. If you believe that we have mistakenly or unintentionally collected personal information of a minor through our sites without appropriate consent, please notify us through our inquiry form so that we may immediately delete the information from our servers and make any other necessary corrections. Additionally, please use this same form to request removal of content or information that was posted to our sites when the registered user was under the age of 16. Please note that such requests may not ensure complete or comprehensive removal of the content or information, as, for example, some of the content may have been reposted by another user.

14. WHAT ARE MY RIGHTS AS A CALIFORNIA RESIDENT?

Under the California Consumer Privacy Act (CCPA), as amended, California residents may request that we:

1. disclose to you the following information:

the categories and specific pieces of personal information we collected about you and the categories of personal information we sold (see [Section 4](#));

the categories of sources from which we collected such personal information (see [Section 4](#));

the business or commercial purpose for collecting or selling personal information about you (see [Section 5](#)); and

the categories of third parties to whom we sold or otherwise disclosed personal information (see [Section 8](#)).

2. delete personal information we collected from you or correct inaccurate personal information about you (see [Section 12](#)); or

3. opt-out of any future sale of personal information about you (see [Section 12](#)).

We will respond to your request consistent with applicable law. If you are an authorized agent making an access or deletion request on behalf of a Californian resident, please reach out to us via the [inquiry form](#) and indicate that you are an authorized agent. We will provide you with instructions on how to submit a request as an authorized agent on behalf of a Californian resident.

If you are a California resident, you may obtain information about exercising your rights, as described above, by contacting us at 1-800-633-0748. For information on the CCPA requests Oracle received, complied with, or denied for the previous calendar year, please visit Oracle's Annual Consumer Privacy Reporting page, available [here](#).

15. DATA PROTECTION OFFICER

Oracle has appointed a **Global Data Protection Officer**. If you believe your personal information has been used in a way that is not consistent with the Privacy Policy or your choices, or if you have further questions, comments or suggestions related to this Privacy Policy, please contact the Global Data Protection Officer by filling out an [inquiry form](#).

Written inquiries to the Global Data Protection Officer may be addressed to:

Oracle Corporation
Global Data Protection Officer
Willis Tower
233 South Wacker Drive
45th Floor
Chicago, IL 60606
U.S.A.

For personal information collected about you in the EU/EEA or other relevant regions, the EU Data Protection Officer can be contacted by filling out an inquiry form and selecting “Contact Oracle’s external EU DPO” in the dropdown menu. Written inquiries may be addressed to:

Robert Niedermeier
Hauptstraße 4
D-85579 Neubiberg / München
Germany

For personal information collected from individuals INSIDE Brazil, written inquiries to the Brazilian Data Protection Officer may be addressed to:

Alexandre Sarte
Rua Dr. Jose Aureo Bustamante, 455
Vila São Francisco
São Paulo, BR

16. FILING A COMPLAINT

If you have any complaints regarding our compliance with this Privacy Policy, please contact us. We will investigate and attempt to resolve complaints and disputes regarding use and disclosure of personal information in accordance with this Privacy Policy and in accordance with applicable law. You also have the right to file a complaint with a competent data protection authority (see [Contact information for Data Protection Authorities and Country Specific Disclosures](#)).

17. ORACLE CORPORATE HEADQUARTERS

Oracle’s corporate headquarters are located at:

2300 Oracle Way
Austin, TX 78741
USA

Tel: +1.737.867.1000

Previous versions: [12/16/22](#) | [08/03/22](#) | [05/05/22](#) | [04/05/21](#) | [01/19/21](#) | [01/04/21](#) | [10/20/20](#) | [12/23/19](#) | [3/25/19](#)

Learn More

Privacy Inquiries

Resources for	Why Oracle	Learn	News and Events	Contact Us
Careers	Analyst Reports	What is cloud computing?	News	US Sales: +1.800.633.0738
Developers	Best cloud-based ERP	What is CRM?	Oracle CloudWorld	How can we help?
Investors	Cloud Economics	What is Docker?	Oracle CloudWorld Tour	Subscribe to emails
Partners	Social Impact	What is Kubernetes?	Oracle Health Summit	Integrity Helpline
Researchers	Culture and Inclusion	What is Python?	Oracle DevLive	
Students and Educators	Security Practices	What is SaaS?	Search all events	

Country/Region

Attachment E-2



Public Sector Schedule P - Program

Oracle America, Inc. ("Oracle")
500 Oracle Parkway
Redwood Shores, CA 94065

Your Name:	State of Oklahoma by and through the Office of Management and Enterprise Services
General Terms Reference:	US-GMA-80421183

This Public Sector Program Schedule (this "Schedule P") is a Schedule to the General Terms referenced above. The General Terms and this Schedule P, together with any other Schedules that reference the General Terms, are the Master Agreement. This Schedule P shall coterminate with the General Terms provided, however, that each ordering document issued and executed under the General Terms and this Schedule P shall continue to be in full force and effect, and the terms of the General Terms and this Schedule P shall continue to apply thereto, in each case, unless and until such ordering document has expired or been terminated. As used in this Schedule P, "You" or "Your" shall refer to the Customer placing an order under the General Terms and this Schedule P.

1. DEFINITIONS

1.1 "**Commencement Date**" refers to the date of shipment of tangible media or the effective date of the order if shipment of tangible media is not required.

1.2 Capitalized terms used but not defined in this Schedule P have the meanings set forth in the General Terms.

2. RIGHTS GRANTED

2.1 Upon the full signing of Your order by both Oracle and You, You have the non-exclusive, non-assignable, royalty free, perpetual (unless otherwise specified in the order), limited right to use the Programs and receive any Program-related Service Offerings You ordered solely for Your internal operations and subject to the terms of the Master Agreement, including the definitions and rules set forth in the order and the Program Documentation.

2.2 Upon payment for Program-related Service Offerings, You have the non-exclusive, non-assignable, royalty free, perpetual, limited right to use for Your internal operations anything developed by Oracle and delivered to You under this Schedule P ("deliverables"); however, certain deliverables may be subject to additional license terms provided in the order.

2.3 You may allow Your agents and contractors (including, without limitation, outsourcers) to use the Programs and deliverables for Your internal operations and You are responsible for their compliance with the General Terms and this Schedule P in such use. For Programs that are specifically designed to allow Your customers and suppliers to interact with You in the furtherance of Your internal business operations, such use is allowed under the General Terms and this Schedule P.

2.4 You may make a sufficient number of copies of each Program for Your licensed use and one copy of each Program media.

3. RESTRICTIONS

3.1 The Programs may contain or require the use of third party technology that is provided with the Programs. Oracle may provide certain notices to You in Program Documentation, readmes or notice files in connection with such third party technology. Third party technology will be licensed to You either under the terms of the Master Agreement or, if specified in the Program Documentation, readmes or notice files, under Separate Terms. Your rights to use Separately Licensed Third Party Technology under Separate Terms are not restricted in any way by the Master Agreement. However, for clarity, notwithstanding the existence of a notice, third party technology that is not Separately Licensed Third Party Technology shall be deemed part of the Programs and is licensed to You under the terms of the Master Agreement. For purposes of clarification, a Customer who acquires Separately Licensed Third Party Technology under an order shall be the licensee of such Separately Licensed Third Party Technology and therefore, the recipient of the applicable notices and any associated source code for Separately Licensed Third Party Technology. Your entry into this Master Agreement does not constitute Your waiver of any rights or defenses available to You under applicable law with respect to Your use of Separately Licensed Third Party Technology.

Attachment E-2

If You are permitted under an order to distribute the Programs, You must include with the distribution all such notices and any associated source code for Separately Licensed Third Party Technology as specified, in the form and to the extent such source code is provided by Oracle, and You must distribute Separately Licensed Third Party Technology under Separate Terms (in the form and to the extent Separate Terms are provided by Oracle). Notwithstanding the foregoing, Your rights to the Programs are solely limited to the rights granted in Your order.

3.2 You may not:

- a. remove or modify any Program markings or any notice of Oracle's or its licensors' proprietary rights;
- b. make the Programs or materials resulting from the Service Offerings available in any manner to any third party for use in the third party's business operations (unless such access is expressly permitted for the specific Program license or materials from the Service Offerings you have acquired);
- c. cause or permit reverse engineering (unless required by law for interoperability), disassembly or decompilation of the Programs (the foregoing prohibition includes but is not limited to review of data structures or similar materials produced by Programs);
- d. disclose results of any Program benchmark tests without Oracle's prior written consent, except as required by applicable law, provided that You give Oracle prior notice and an opportunity to oppose such disclosure (unless prohibited by law).

3.3 The prohibition on the assignment or transfer of the Programs or any interest in them under the General Terms shall apply to all Programs licensed under this Schedule P, except to the extent that such prohibition is rendered unenforceable under applicable law.

4. TRIAL PROGRAMS

You may order trial Programs, or Oracle may include additional Programs with Your order which You may use for trial, non-production purposes only. You may not use the trial Programs to provide or attend third party training on the content and/or functionality of the Programs. You have 30 days from the Commencement Date to evaluate these Programs. To use any of these Programs after the 30 day trial period, You must obtain a license for such Programs from Oracle or an authorized reseller. If You decide not to obtain a license for any Program after the 30 day trial period, You will cease using and promptly delete any such Programs from Your computer systems. Programs licensed for trial purposes are provided "as is" and Oracle does not provide technical support or offer any warranties for these Programs.

5. TECHNICAL SUPPORT

5.1 For purposes of an order, technical support consists of Oracle's annual technical support services You may have ordered from Oracle or an authorized reseller for the Programs. If ordered, annual technical support (including first year and all subsequent years) is provided under Oracle's technical support policies in effect at the time the technical support services are provided. You agree to cooperate with Oracle and provide the access, resources, materials, personnel, information and consents that Oracle may require in order to perform the technical support services. The technical support policies are incorporated in this Schedule P and are subject to change at Oracle's discretion; however, Oracle policy changes will not result in a material reduction in the level of technical support services provided for supported Programs during the period for which fees for technical support have been paid. You should review the policies prior to entering into the order for the applicable technical support services. You may access the current version of the technical support policies at <http://oracle.com/contracts>.

5.2 If You decide to purchase technical support for any Program license within a license set, You are required to purchase technical support at the same level for all licenses within that license set. You may desupport a subset of licenses in a license set only if You agree to terminate that subset of licenses. The technical support fees for the remaining licenses will be priced in accordance with the technical support policies in effect at the time of termination or as otherwise agreed in writing by Oracle and You. Oracle's license set definition is available in the current technical support policies. If You decide not to purchase technical support, You may not update any unsupported Program licenses with new versions of the Program.

6. PROGRAM-RELATED SERVICE OFFERINGS

In addition to technical support, You may order a limited number of Program-related Service Offerings under this Schedule P as listed in the Program-Related Service Offerings document, which is at <http://oracle.com/contracts>. You agree to provide Oracle with all information, access and full good faith cooperation reasonably necessary to enable Oracle to deliver these Service Offerings and You will perform the actions identified in the order as Your responsibility. If while performing these Service

Attachment E-2

Offerings Oracle requires access to another vendor's products that are part of Your system, You will be responsible for acquiring all such products and the appropriate license rights necessary for Oracle to access such products on Your behalf. Service Offerings provided may be related to Your license to use Programs owned or distributed by Oracle which You acquire under a separate order. The agreement referenced in that order shall govern Your use of such Programs.

7. WARRANTIES, DISCLAIMERS AND EXCLUSIVE REMEDIES

7.1 Oracle warrants that a Program licensed to You will operate in all material respects as described in the applicable Program Documentation for a period of one year after delivery (i.e., via physical shipment or electronic download). You must notify Oracle of any Program warranty deficiency within one year after delivery. Oracle also warrants that technical support services and Program-related Service Offerings (as referenced in section 6 above) ordered and provided under this Schedule P will be provided in a professional manner consistent with industry standards. You must notify Oracle of any technical support service or Program-related Service Offerings warranty deficiencies within 90 days from performance of the deficient technical support service or Program-related Service Offerings.

7.2 ORACLE DOES NOT GUARANTEE THAT THE PROGRAMS WILL PERFORM ERROR-FREE OR UNINTERRUPTED OR THAT ORACLE WILL CORRECT ALL PROGRAM ERRORS.

7.3 FOR ANY BREACH OF THE ABOVE WARRANTIES, YOUR EXCLUSIVE REMEDY AND ORACLE'S ENTIRE LIABILITY SHALL BE: (A) THE CORRECTION OF PROGRAM ERRORS THAT CAUSE BREACH OF THE WARRANTY; OR, IF ORACLE CANNOT SUBSTANTIALLY CORRECT THE ERRORS OF THE APPLICABLE PROGRAM LICENSE IN A COMMERCIALY REASONABLE MANNER, YOU MAY END YOUR PROGRAM LICENSE AND RECOVER THE FEES YOU PAID TO ORACLE FOR THE PROGRAM LICENSE AND ANY UNUSED, PREPAID TECHNICAL SUPPORT FEES YOU HAVE PAID FOR THE PROGRAM LICENSE; OR (B) THE REPERFORMANCE OF THE DEFICIENT PROGRAM-RELATED SERVICE OFFERINGS; OR, IF ORACLE CANNOT SUBSTANTIALLY CORRECT THE DEFICIENCY IN A COMMERCIALY REASONABLE MANNER, YOU MAY END THE DEFICIENT PROGRAM-RELATED SERVICE OFFERINGS AND RECOVER THE FEES YOU PAID TO ORACLE FOR THE DEFICIENT PROGRAM-RELATED SERVICE OFFERINGS.

7.4 TO THE EXTENT NOT PROHIBITED BY LAW, THIS WARRANTY IS EXCLUSIVE AND THERE ARE NO OTHER EXPRESS OR IMPLIED WARRANTIES OR CONDITIONS, INCLUDING WARRANTIES OR CONDITIONS OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE.

8. AUDIT

Upon 45 days written notice, Oracle may audit Your use of the Programs to ensure Your use of the Programs is in compliance with the terms of the applicable order and the Master Agreement. Any such audit shall not unreasonably interfere with Your normal business operations. You agree to cooperate with Oracle's audit and provide reasonable assistance and access to information. Such assistance shall include, but shall not be limited to, the running of Oracle data measurement tools on Your servers and providing the resulting data to Oracle. Oracle shall comply with reasonable security and safety rules, policies, and procedures, including but not limited to any facility or system access rules applicable to outside parties ("security rules") while performing any such audit, provided that such security rules are applicable to the performance of the audit; You make such security rules available to Oracle prior to the commencement of the audit; and such security rules do not modify or amend the terms and conditions of the Master Agreement or the applicable order. If the audit identifies non-compliance, You shall be responsible for remedying such non-compliance, which may include, without limitation, the payment of any fees for additional licenses for Programs or the discontinuation of noncompliant use. If the remedy requires You to pay fees, You will submit a contract modification to document the amount of such fees. The performance of the audit and non-public data obtained during the audit (including findings or reports that result from the audit) shall be subject to the provisions of (Nondisclosure) of the General Terms. You agree that Oracle shall not be responsible for any of Your costs incurred in cooperating with the audit.

If You in good faith provide Oracle with written notice of an alleged error in the amount of underpaid fees due Oracle as a result of an audit under this section (the "dispute"), then the parties will endeavor to resolve the dispute in accordance with this paragraph. Each party will appoint a Vice President (or equivalent level) to discuss the dispute and no formal proceedings for the judicial resolution of such dispute, except for the seeking of equitable relief, may begin until either Vice President (or equivalent level) concludes, after a good faith effort to resolve the dispute, that resolution through continued discussion is unlikely. The party concluding that resolution through continued discussion is unlikely will provide notice thereof to the other party. In addition, the parties shall refrain from exercising any termination right and shall continue to perform their respective obligations under the General Terms, this Schedule P and the applicable ordering document(s), while they endeavor to resolve the dispute under this paragraph.

9. ORDER LOGISTICS

Attachment E-2

9.1 Delivery and Installation

9.1.1 You are responsible for installation of the Programs unless the Programs have been pre-installed by Oracle on the Hardware You are purchasing under the order or unless You purchase installation services from Oracle for those Programs.

9.1.2 Oracle has made available to You for electronic download at the electronic delivery web site located at the following Internet URL: <http://edelivery.oracle.com> the Programs listed in the Programs and Program Support Service Offerings section of the applicable order. Through the Internet URL, You can access and electronically download to Your location the latest production release as of the effective date of the applicable order of the software and related Program Documentation for each Program listed. Provided that You have continuously maintained technical support for the listed Programs, You may continue to download the Programs and related Program Documentation. Please be advised that not all Programs are available on all hardware/operating system combinations. For the most recent Program availability please check the electronic delivery web site specified above. You acknowledge that Oracle is under no further delivery obligation with respect to Programs under the applicable order, electronic download or otherwise unless otherwise stated in Your Order.

9.1.3 Intentionally omitted

9.2 Territory

The Programs shall be used in the United States.

9.3 Pricing, Invoicing and Payment Obligation

9.3.1 In entering into payment obligations under an order, You agree and acknowledge that You have not relied on the future availability of any Program or updates. However, (a) if You order technical support, the preceding sentence does not relieve Oracle of its obligation to provide such technical support under the Master Agreement, if and when available, in accordance with Oracle's then current technical support policies, and (b) the preceding sentence does not change the rights granted to You under an order and the Master Agreement.

9.3.2 Program fees are invoiced as of the Commencement Date.

9.3.3 Program-related Service Offering fees are invoiced after the performance of the Program-related Service Offering performance; specifically, technical support fees are invoiced quarterly in arrears. The period of performance for all Program-related Service Offerings is effective upon the Commencement Date.

9.3.4 . Neither a Customer nor the State shall be liable to Vendor, its employees or its agents, for the payment of taxes.



Public Sector Schedule S - Services

Oracle America, Inc. ("Oracle")
500 Oracle Parkway
Redwood Shores, CA 94065

Your Name:	State of Oklahoma by and through the Office of Management and Enterprise Services
General Terms Reference:	US-GMA-80421183

This Public Sector Services Schedule (this "Schedule S") is a Schedule to the General Terms referenced above. The General Terms and this Schedule S, together with any other Schedules that reference the General Terms, are the Master Agreement. This Schedule S shall coterminate with the General Terms provided, however, that each ordering document issued and executed under the General Terms and this Schedule S shall continue to be in full force and effect, and the terms of the General Terms and this Schedule S shall continue to apply thereto, in each case, unless and until such ordering document has expired or been terminated. As used in this Schedule S, "You" or "Your" shall refer to the Customer placing an order under the General Terms and this Schedule S.

1. DEFINITIONS

- 1.1 **"Services"** refers to consulting, advanced customer support services, education or other services which you have ordered from Oracle under this Schedule S.
- 1.2 Capitalized terms used but not defined in this Schedule S have the meanings set forth in the General Terms.

2. RIGHTS GRANTED / RESTRICTIONS

- 2.1 Upon payment for Services, You have the non-exclusive, non-assignable, royalty free, perpetual, limited right to use for Your internal operations anything developed by Oracle and delivered to You under this Schedule S ("deliverables"); however, certain deliverables may be subject to additional license terms provided in the order.
- 2.2 You may allow Your agents and contractors (including, without limitation, outsourcers) to use deliverables for Your internal operations and You are responsible for their compliance with the General Terms and this Schedule S in such use.
- 2.3 Services provided may be related to Your right to use cloud or hosted/managed services or Products owned or distributed by Oracle which You acquire under a separate order. The agreement referenced in that order shall govern Your use of such Products and nothing in this Schedule S is intended to grant a right to use such services or Products in excess of the terms of that order, such as the services period or number and type of environments specified in a cloud or hosted/managed services order.

3. WARRANTIES, DISCLAIMERS AND EXCLUSIVE REMEDIES

- 3.1 Oracle warrants that Services will be provided in a professional manner consistent with industry standards. You must notify Oracle of any warranty deficiencies within 90 days from performance of the deficient Services.
- 3.2 **FOR ANY BREACH OF THE WARRANTY, YOUR EXCLUSIVE REMEDY AND ORACLE'S ENTIRE LIABILITY SHALL BE THE RE-PERFORMANCE OF THE DEFICIENT SERVICES, OR, IF ORACLE CANNOT SUBSTANTIALLY CORRECT THE DEFICIENCY IN A COMMERCIALY REASONABLE MANNER, YOU MAY END THE DEFICIENT SERVICES AND RECOVER THE FEES YOU PAID TO ORACLE FOR THE DEFICIENT SERVICES.**
- 3.3 **TO THE EXTENT NOT PROHIBITED BY LAW, THIS WARRANTY IS EXCLUSIVE AND THERE ARE NO OTHER EXPRESS OR IMPLIED WARRANTIES OR CONDITIONS, INCLUDING WARRANTIES OR CONDITIONS OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE.**

4. SUBCONTRACTING

- a) If Oracle is permitted to utilize subcontractors in support of the Services, Oracle shall remain solely responsible for its obligations under the terms of the General Terms and this Schedule S, for its actions and omissions and those of its agents, employees and subcontractors and for payments to such persons or entities.
- b)
 - (i) With respect to any order for Oracle Customer Success Services (as identified in the Service Descriptions posted for Customer Success Services posted at www.oracle.com/contracts) placed by the State, prior to a subcontractor being utilized by Oracle, Oracle shall either (i) restrict subcontractor access so that Customer Data will not be viewed or downloaded by such subcontractor or (ii) obtain written approval of the State or Customer, as applicable, to such subcontractor, and to the extent required by an applicable ordering document or statement of work, each employee of such subcontractor, proposed for use by Oracle. Such approval shall not be unreasonably withheld. The proposed subcontractor shall be identified by entity name, and by employee name, if required by the applicable ordering document, in the applicable approval request and shall include the nature of the Services to be performed. As of the date hereof, Service Descriptions for Customer Success Services at www.oracle.com/contracts can be accessed at <https://www.oracle.com/contracts/services/> by selecting Customer Success Services in the "Product" dropdown menu.
 - (ii) Any approval under subsection 4(b)(i) above shall be conditioned upon execution of a written agreement by Oracle and subcontractor setting forth the subcontractor's agreement to perform the covenants and conditions applicable to the subcontractor's Services under the Contract Documents, and to make any certifications required of subcontractors under the applicable Contract Documents. Oracle shall provide confirmation of execution of such an agreement upon request. Oracle shall confirm as part of such approval request that the subcontractor shall be contractually required to i) carry insurance in the types and amounts specified in Section 8.2 of the General Terms and provide proof of coverage upon request, ii) if applicable, carry such other alternate insurance coverage as the State or Customer may approve for a specified subcontractor approval request or iii) submit to the State Certification and Accreditation Review process identified in the Information Technology Terms, Appendix 1, Section C, Security Assessment. Supplier agrees that maintaining such agreement with any subcontractor and obtaining any required prior written approval by the State or Customer of any subcontractor (and, if required under the applicable order, associated subcontractor employees) shall be a continuing obligation. The State or Customer further reserves the right to revoke its approval of a subcontractor or an employee thereof in instances of poor performance, misconduct or for other similar reasons. No payment shall be made to the Supplier for performance by any subcontractor or employee who is disapproved as provided in the foregoing sentence following such disapproval, or who is not approved as required by any applicable approval requirements of this Schedule S or the applicable ordering document or statement of work.

Attachment E-4



Schedule OSSS – Oracle Open Source Support Services

Oracle America, Inc. ("Oracle")
500 Oracle Parkway Redwood Shores,
CA 94065

Your Name:	State of Oklahoma by and through the Office of Management and Enterprise Services
General Terms Reference:	US-GMA-80421183

This Oracle Open Source Support Services Schedule (this "Schedule OSSS") is a Schedule to the General Terms referenced above. The General Terms and this Schedule OSSS, together with any other Schedules that reference the General Terms, are the Master Agreement. This Schedule OSSS shall co-terminate with the General Terms provided, however, that each ordering document issued and executed under the General Terms and this Schedule OSSS shall continue to be in full force and effect, and the terms of the General Terms and this Schedule OSSS shall continue to apply thereto, in each case, unless and until such ordering document has expired or been terminated. As used in this Schedule OSSS, "You" or "Your" shall refer to the Customer placing an order under the General Terms and this Schedule OSSS.

1. DEFINITIONS

1.1 "**Covered Programs**" is defined as the specific set of software products listed on the document titled Oracle Linux and Oracle VM Covered Programs (available at <http://www.oracle.com/us/support/library/enterprise-linux-indemnification-069347.pdf>) for which You have ordered Oracle Linux Service Offering(s) and/or Oracle VM Service Offering(s), including any related program documentation and patches and bug fixes acquired through such Oracle Linux Service Offering(s) and/or Oracle VM Service Offering(s).

1.2 "**Oracle Linux Service Offering(s)**", "**Oracle VM Service Offering(s)**" and "**Oracle Verrazzano Service Offering(s)**" refer to Oracle Linux, Oracle VM and Oracle Verrazzano support services respectively as defined under the Oracle Open Source Support Policies referenced in Section 2.2 below.

1.3 "**Oracle Open Source Service Offering(s)**" means the Oracle Linux Service Offering(s), the Oracle VM Service Offering(s), and the Oracle Verrazzano Service Offering(s).

1.4 "**Support Term**" is defined as the duration for which You have acquired the applicable Oracle Open Source Service Offering(s).

1.5 "**Program Documentation**" refers to the program user manual and program installation manuals. Program Documentation may be delivered with the Oracle Linux, Oracle VM and Oracle Verrazzano programs. You may access the documentation online at <http://oracle.com/documentation>.

1.6 Capitalized terms used but not defined in this Schedule OSSS have the meanings set forth in the General Terms.

2. ORACLE OPEN SOURCE SERVICE OFFERING(S)

2.1. Upon Oracle's acceptance of Your order, You have the limited right to receive the applicable Oracle Open Source Service Offering(s) solely for Your business operations and subject to the terms of this Schedule OSSS including availability rules and metric definitions set forth in the order and the Program Documentation.

2.2. For purposes of the order, the Oracle Open Source Service Offering(s) consists of Oracle's technical support services level You may have ordered from Oracle or an authorized reseller for the Oracle Open Source Service Offering(s). If ordered, the

Attachment E-4

Oracle Open Source Service Offering(s) (including initial year and all subsequent years) are provided under the Oracle Open Source Support Policies in effect at the time the Oracle Open Source Service Offering(s) are provided. The Oracle Open Source Support Policies, which are incorporated in this Schedule OSSS, are subject to change at Oracle's discretion; however, Oracle will not materially reduce the level of technical support services provided during the period for which fees for the Oracle Open Source Service Offering(s) have been paid. Oracle Open Source Service Offering(s) are available for certain systems, and may be subject to additional restrictions as set forth in the Oracle Open Source Support Policies. You should review the Oracle Open Source Support Policies prior to entering into the order for the applicable Oracle Open Source Service Offering(s). You may access the current version of the Oracle Open Source Support Policies at <http://oracle.com/contracts>.

2.3. The Oracle Open Source Service Offering(s) are effective upon the effective date of the order unless otherwise stated in Your order. If Your order was placed through the Oracle Store, the effective date is the date Your order was accepted by Oracle.

2.4. The Oracle Open Source Service Offering(s) provided under this Schedule OSSS are in support of licenses You acquired separately. All patches, bug fixes and other code received as part of the Oracle Open Source Service Offering(s) under this Schedule OSSS shall be provided under the applicable license terms for the Oracle Linux, Oracle VM and/or Oracle Verrazzano program(s) that You have downloaded and/or installed. The Oracle Open Source Service Offering(s) may also include the right to use certain additional software or tools during the Support Term for which fees for Oracle Open Source Service Offering(s) have been paid. The license terms for any such software or tools, as well as any limitations associated with them, will be referenced in the Program Documentation.

3. ORACLE LINUX AND ORACLE VM INDEMNIFICATION

3.1. Provided You are a current subscriber to the Oracle Linux Service Offering(s) and/or Oracle VM Service Offering(s), if a third party makes a claim against You that any Covered Programs furnished by Oracle, and used by You for Your business operations infringes its intellectual property rights (including patents and copyrights, trade and service marks), Oracle, at its sole cost and expense, will defend You against the claim and indemnify You from the damages, liabilities, costs and expenses (including without limitation reasonable attorneys' fees) awarded by the court to the third party claiming infringement or the settlement agreed to by Oracle, if You do the following:

- a. Notify Oracle promptly in writing, not later than 30 days after You receive notice of the claim (or sooner if required by applicable law);
- b. Give Oracle sole control of the defense and any settlement negotiations; and
- c. Give Oracle the information, authority, and reasonable assistance it needs to defend against or settle the claim; reasonable out-of-pocket expenses incurred by You in providing such assistance will be reimbursed by Oracle.

3.2. If Oracle believes or it is determined that any Covered Programs may have violated a third party's intellectual property rights, Oracle may choose to either modify the Covered Programs to be non-infringing (while substantially preserving their utility or functionality) or obtain a license to allow for continued use, or if these alternatives are not commercially reasonable, then Oracle may, upon 30 days notice to You, terminate Your right to receive indemnification for Your further use of the Covered Programs and refund any unused, prepaid service fees, You have paid for the Covered Programs.

3.3. Notwithstanding the above, Oracle will not defend or indemnify You in connection with claims, damages, liabilities, costs or expenses arising out of, or caused by, or related to: (a) Your distribution of the Covered Programs; (b) Your alteration of the Covered Programs; (c) Your use of a version of the Covered Programs which has been superseded, if the infringement claim could have been avoided by using the current version of the Covered Programs; (d) Your use of the Covered Programs outside the scope of use identified in the user documentation or the Oracle Open Source Support Policies; (e) Your use of the Covered Programs when You were not a subscriber to the Oracle Linux Service Offering(s) and/or Oracle VM Service Offering(s); (f) any information, design, specification, instruction, software, data, or material not furnished by Oracle; (g) the combination of any Covered Programs with any products or services not provided by Oracle; (h) Your claim, lawsuit, or action against a third party. For avoidance of doubt, this section 3 specifically excludes, and no indemnification is provided for, the Verrazzano programs. **This section provides Your exclusive remedy for any infringement claims or damages, liabilities, costs or expenses.**

4. WARRANTIES, DISCLAIMERS AND EXCLUSIVE REMEDIES

4.1. Oracle warrants that the Oracle Open Source Service Offering(s) will be provided in a professional manner consistent with industry standards. You must notify Oracle of any Oracle Open Source Service Offering(s) warranty deficiencies within 90 days from performance of the defective Oracle Open Source Service Offering(s).

4.2. TO THE EXTENT PERMITTED BY LAW, THIS WARRANTY IS EXCLUSIVE AND THERE ARE NO OTHER EXPRESS OR IMPLIED WARRANTIES OR CONDITIONS, INCLUDING WARRANTIES OR CONDITIONS OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE.

Attachment E-4

4.3. ORACLE DOES NOT GUARANTEE THAT ANY PROGRAMS ASSOCIATED WITH THE ORACLE OPEN SOURCE SERVICE OFFERING(S) (INCLUDING BUT NOT LIMITED TO THE ORACLE LINUX, ORACLE VM OR ORACLE VERRAZZANO PROGRAMS) WILL PERFORM ERROR-FREE OR UNINTERRUPTED OR THAT ORACLE WILL CORRECT ALL PROGRAM ERRORS. FOR ANY BREACH OF THE ABOVE WARRANTIES, YOUR EXCLUSIVE REMEDY, AND ORACLE'S ENTIRE LIABILITY, SHALL BE THE REPERFORMANCE OF THE DEFICIENT ORACLE OPEN SOURCE SERVICE OFFERING(S), OR IF ORACLE CANNOT SUBSTANTIALLY CORRECT A BREACH IN A COMMERCIALY REASONABLE MANNER, YOU MAY END THE RELEVANT ORACLE OPEN SOURCE SERVICE OFFERING(S) AND RECOVER THE FEES PAID TO ORACLE FOR THE DEFICIENT ORACLE OPEN SOURCE SERVICE OFFERING(S).

5. LIMITATION OF LIABILITY FOR INFRINGEMENT CLAIMS

For purposes of this Schedule OSSS, the limitation of liability in the General Terms referenced above shall not be construed to limit Oracle's indemnification obligation or Your exclusive remedy for any infringement claims or damages, liabilities, costs or expenses under Section 3 of this Schedule OSSS.

6. GOVERNING LAW AND JURISDICTION

Intentionally Omitted.

7. AUDIT

Upon 45 days written notice, Oracle may audit Your use of the Oracle Open Source Service Offering(s) to ensure Your use of the Oracle Open Source Service Offering(s) is in compliance with the terms of the applicable order and the Master Agreement. Any such audit shall not unreasonably interfere with Your normal business operations.

You agree to cooperate with Oracle's audit and provide reasonable assistance and access to information reasonably requested by Oracle.

The performance of the audit and non-public data obtained during the audit (including findings or reports that result from the audit) shall be subject to the provisions of the Nondisclosure section of the Master Agreement.

If the audit identifies non-compliance, You agree to remedy (which may include, without limitation, the payment of any fees applicable to Your use of the Oracle Open Source Service Offering(s) in excess of Your service rights) such noncompliance. If You do not remedy the non-compliance, Oracle can end (a) Oracle Open Source Service Offering(s), (b) Oracle Open Source-related Service Offering(s) and/ or (c) the Master Agreement. You agree that Oracle shall not be responsible for any of Your costs incurred in cooperating with the audit. If the remedy requires You to pay fees, You will submit a contract modification to document the amount of such fees.

If You in good faith provide Oracle with written notice of an alleged error in the amount of underpaid fees due Oracle as a result of an audit under this section (the "dispute"), then the parties will endeavor to resolve the dispute in accordance with this paragraph. Each party will appoint a Vice President (or equivalent level) to discuss the dispute and no formal proceedings for the judicial resolution of such dispute, except for the seeking of equitable relief, may begin until either Vice President (or equivalent level) concludes, after a good faith effort to resolve the dispute, that resolution through continued discussion is unlikely. The party concluding that resolution through continued discussion is unlikely will provide notice thereof to the other party. In addition, the parties shall refrain from exercising any termination right and shall continue to perform their respective obligations under the General Terms, this Schedule OSSS and the applicable ordering document(s), while they endeavor to resolve the dispute under this paragraph.

8. ORDER LOGISTICS

8.1. Once placed, Your order shall be non-cancelable and the sums paid nonrefundable, except as provided in the Master Agreement.

8.2. Oracle Open Source Service Offering(s) fees are invoiced in advance of the performance of the Oracle Open Source Service Offering(s); specifically, Oracle Open Source Service Offering(s) fees are invoiced annually in advance. The period of performance for all Oracle Open Source Service Offering(s) is effective upon the effective date of Your order.

8.3. Intentionally Omitted.

ATTACHMENT E-5 Pricing

I. PRODUCT/CLOUD SERVICE PRICE LIST

The following pricing and discounts may be applied to the orders for the following Products and Cloud Services placed under the Contract pursuant to the terms and conditions of the applicable ordering documents. The "Price Lists" shall be defined as the price lists posted at Supplier's website as described below in Section III (Vendor Website for Contract and Prices) of this Attachment. From the effective date of the Contract, the Price Lists shall be updated at least once annually.

A. Pricing and Discounts for New Program Licenses and First-Year Technical Support

1. Provided that Customer has continuously maintained technical support for its existing program licenses, Customer may acquire any programs listed on the Price Lists and the related technical support, provided that such program are available in production release when ordered, by paying Supplier the fees specified for such Programs on the Price Lists less the discount determined by the discount schedule set forth below. Customer may also acquire first-year technical support (e.g., Software Updates & License Support ("SULS")) for programs by paying Supplier the fees specified for such technical support on the Price Lists less the discount determined by the discount schedule set forth below.
2. Discounts. Unless otherwise specified at Supplier's website as described in Section III below, and except as provided in section A.3 below, the following discount schedule shall apply to the list fees specified on the Price Lists for program and related technical support acquired pursuant to the Contract:

	Discount
a. Program Licenses and First-Year Technical Support	24.24%
b. Campus Wide Program Licenses and First-Year Technical Support	89.90% for eligible Customers and eligible Oracle Technology programs as set forth in the attached Exhibit 1 (Campus Wide Programs)

3. Exceptions. Any discounts provided in this section A shall not apply toward (a) any third-party products included in any of the Price Lists, (b) any products on controlled availability, or (c) any Cloud Service products. All Price List minimums apply.

B. Pricing for Cloud Services

Customer may acquire the Cloud Services listed on the Price Lists, provided that such products are available in production release when ordered, by paying Oracle the fees specified for such Cloud service products on the Price Lists less the discount(s), if any, set forth in the applicable ordering documents.

II. SERVICES/PRICE LIST

The following pricing and discounts may be applied to the orders for the following Service Offerings placed under the Contract pursuant to the terms and conditions set forth in the applicable ordering documents.

A. Pricing and discounts for Oracle Consulting Services (OCS)

Level of Resource	Country	Daily Rates	Hourly Rates
9 - Sr. Practice/Tech Director	USA	\$2,657.78	\$332.22
8 - Practice/Tech Director	USA	\$2,416.16	\$302.02
7 - Practice/Tech Manager	USA	\$2,083.94	\$260.49
6T - Senior Principal Consultant	USA	\$1,932.93	\$241.62
5 - Principal Consultant	USA	\$1,691.31	\$211.41
4 - Senior Consultant	USA	\$1,389.29	\$173.66
3 - Staff Consultant	USA	\$1,208.08	\$151.01
2 - Associate Consultant	USA	\$906.06	\$113.26

Level	Daily Rates	Hourly Rates
NACI-IN-L8 Director-Remote	\$1,001.26	\$125.16
NACI-IN-L7 Tech.Mgr-Remote	\$734.04	\$91.76
NACI-IN-L6 Sen.Prin-Remote	\$574.49	\$71.81
NACI-IN-L5 Principal-Remote	\$421.52	\$52.69
NACI-IN-L4 Senior-Remote	\$321.06	\$40.13
NACI-IN-L3 Staff-Remote	\$279.70	\$34.96
NACI-IN-L2 Associate-Remote	\$231.77	\$28.97

B. Customer Success Services (CSS)

B.1 Pricing for CSS Managed Cloud Services - The "Price Lists" shall be defined as the price lists posted at Supplier's website as described in Section III below (Supplier Website for Contract and Prices). From the effective date of the Contract, the Price Lists shall be updated at least once annually. There will be a 15% discount on all Managed Cloud Services.

B.2 Pricing and Discounts for CSS Time & Materials Rate Card for Custom Projects

Rates and orders placed on the effective date of contract for Years 1 and 2	Standard Hourly Rate	75-150 Days	151+ Days
Title			
ACS Engineer	\$331.96	\$313.09	\$301.79
Sr. ACS Engineer	\$398.35	\$375.71	\$362.14
Technical Account Manager	\$331.96	\$313.09	\$301.79
ACS Engineer-Remote	\$90.46	\$90.46	\$90.46
ACS Security Account Manager	\$435.90	\$411.13	\$396.28

Except for Oklahoma State Entity Customers, Travel and Expense will be billed as separate line item for each project for on-site support. By exception, Blended Rates may be made available for projects.

To be eligible to purchase installation services, packaged services, or other ACS engineering services, Customers must be current on technical support (Software Update License and Support, or "SULS") for their licensed programs, current on technical support (Premier Support for Systems) for hardware, and all supported software environments must comply with current Oracle Certification Matrices.

C. Pricing and Discount Terms for Education (Training) Services – Oracle University

For five (5) years from the effective date of the Contract, the Customer may purchase Oracle University products and services at a 14.14% discount off the Oracle University Price List in effect at the time customer places the student registration for training. Oracle University's Price List is available at <http://education.oracle.com>. These discounts may not be used in conjunction with any other discounts or special promotions offered by Oracle University.

III. SUPPLIER WEBSITE FOR CONTRACT AND PRICES

Within thirty (30) calendar days of the Effective Date of the Contract, Supplier will make available and maintain a website specific to the Products and Service Offerings, as applicable, available under the contract which is clearly distinguished from contract offerings for other customers at Supplier's website. The website must include the Products and Service Offerings, as applicable; associated price lists or other pricing information, and applicable discounts; contact information for Supplier, instructions for obtaining quotes and placing orders; and instructions to initiate and pursue a warranty claim or return products. The website shall list the Oklahoma statewide contract number and contain a link to the State website for the Contract.

IV. CHANGES IN ADMINISTRATIVE FEE

The pricing and discounts provided for herein assume a contract management fee of one percent (1%) of invoiced net sales, in accordance with Attachment C, Section 6.2 of the Contract, and are subject to change as provided in the Contract in the event of a change in the contract management fee.

Exhibit 1 to Attachment E-5 Campus Wide Program

The discount specified in section I.A.2.b of Attachment E-5 is available for Customers who qualify as educational providers under the terms of Oracle's standard Academic Practices policies ("**Higher Education Institutions**"). Any discounts provided in this Contract shall not apply toward any third-party products included in any of the Price Lists and any products on controlled availability. Notwithstanding the existence of separate license pricing terms for educational programs, the terms and conditions of this Contract that Oracle determines to be applicable shall apply to all purchases of Oracle software and associated products offered herein under educational licenses. Higher Education Institutions purchasing under this Contract may acquire licenses on a campus-side basis, which means licensing all full-time and part-time students, faculty and staff ("**Campus Wide Program**") in accordance with the following:

(a) Eligible Programs. The following programs in the Oracle Technology Global Price List are eligible:

Oracle Database:

- Standard Edition
- Enterprise Edition
- NoSQL Enterprise Edition

Enterprise Edition

Options:

- Multitenant
- Real Application Clusters
- Real Application Clusters One Node
- Database in-Memory
- Partitioning
- Active Data Guard
- Real Application Testing
- Advanced Compression
- Advanced Security Option
- Label Security
- Database Vault
- OLAP
- Advanced Analytics
- Audit Vault and Database Firewall

Enterprise Management

Options:

- Diagnostics Pack

- Tuning Pack
- Lifecycle Management Pack
- Data Masking and Subsetting PackTest Data Management Pack
- Cloud Management Pack

Application Server:

- Weblogic Server Standard
- Weblogic Server Enterprise Edition
- Weblogic Suite
- Web Tier
- Internet Application Server Standard
- Internet Application Server Enterprise
- SOA Suite for Middleware

Application Server

Enterprise Management

Options:

- Weblogic Management Pack
- SOA Management Pack

- Management Pack for GoldenGate

Data Integration:

- Data Integrator Enterprise
- GoldenGate
- GoldenGate for Non-Oracle Database
- Golden Gate for Big Data Targets
- Golden Gate Foundation Suite
- Database Gateway for SQL Server

Other Products:

- Webcenter Suite Plus
- Webcenter Portal
- Management Pack for Webcenter
- Identity and Access Management Suite
- Identity Governance Suite
- Directory Services Plus
- Management Pack for Identity Mgmt
- Real User Experience Insight

(b) Internet Access. Higher Education Institutions may allow an unlimited number of internet users to access any of the Campus Wide Program licenses licensed under an Oracle Order From, provided the access is for viewing, querying, or adding data associated with the Higher Education Institution's administrative, teaching, research or community service functions. Higher Education Institutions may charge a fee for such internet access provided the fee is designed to only reimburse the Higher Education Institution for its costs incurred in developing and administering the Higher Education Institution's business program.

- (c) OAI and WDP Membership. As of the effective date of an order placed under this Contract, teaching departments at the Higher Education Institution may participate in the Oracle Academic Initiative (OAI) and/or the Oracle Workforce Development Program (WDP) or successor programs that may replace OAI/WDP. The OAI/WDP membership fee will be waived for any department that elects to incorporate Oracle programs into its classroom teaching.
- (d) Campus Wide Program licenses may not be used for non-medical school functions of an associated medical center or university hospital (e.g., patient management and billing).
- (e) On the yearly anniversary of the effective date of an order, you must report any additional full-time and part-time students, faculty and staff to Oracle and ensure your license quantity is sufficient to cover the additional population in order to extend the rights listed above (Internet Access, OAI and WDP Membership, User Minimums) for a subsequent year.

**Attachment F to
STATE OF OKLAHOMA CONTRACT WITH ORACLE AMERICA, INC.
RESULTING FROM SOLICITATION NO. 0000000199**

Negotiated Exceptions and Additional Terms to the Contract

The Contract is hereby amended as set forth below. This Attachment F supersedes all prior terms and exceptions submitted by **Oracle America, Inc.** or discussed by the parties. For clarity, this Attachment F serves as an Addendum to the Contract Documents to which the exceptions below are made.

Requested Exceptions and Additional Terms not addressed below are declined by the State of Oklahoma.

Term & Section	Language
ATTACHMENT B – State of Oklahoma General Terms	
General Terms, Scope and Contract Renewal, Section 1	Section 1.2 is deleted in its entirety and replaced with the following: 1.2 At no time during the performance of the Contract shall the Supplier have the authority to obligate any Customer for payment for any products or services (a) when a corresponding encumbering document (e.g., Supplier ordering document or Customer purchase order) is not signed or (b) over and above any maximum limit provided for in an ordering document. Likewise, Supplier is not entitled to compensation for a product or service provided by or on behalf of Supplier that is neither requested nor accepted as satisfactory.
Scope and Contract Renewal, Section 1	Section 1.4 is deleted in its entirety and replaced with the following: The State and Supplier, upon mutual agreement, may extend the Contract for ninety (90) days beyond a final renewal term at the Contract compensation rate for the extended period, to facilitate the finalization of related terms and conditions of a new award or as needed to transition to a new Supplier. If the parties exercise such option to extend the Contract ninety (90) days, this Agreement shall be amended in accordance with Section 3 below.
General Terms, Contract Effectiveness and Order of Priority, Section 2.2	Section 2.2 is deleted in its entirety and replaced with the following: Contract Documents shall be read to be consistent and complementary. Any conflict among the Contract Documents shall be resolved by giving priority to Contract Documents in the following order of precedence: A any Addendum, which shall take precedence over the Contract Document that it restates or modifies; B any statement of work, work order, or other similar ordering document as applicable;

Term & Section	Language
	<p>C the Contract-specific State terms, including, without limitation, information technology terms, contained in Attachments C and D;</p> <p>D The applicable Schedule (Schedule C, Attachment E-1; Schedule P, Attachment E-2; Schedule S, Attachment E-3, or Schedule OSSS, Attachment E-4);</p> <p>E the terms contained in this Contract Document, Attachment B;</p> <p>F the applicable Solicitation;</p> <p>G other mutually agreed Contract Documents.</p> <p>Notwithstanding the foregoing, and notwithstanding any order of precedence stated in any Contract Document, in the event of any inconsistencies or conflicts between a Contract Document, including information contained in any URLs, hyperlinks or policies, and any of the following terms, the following terms (the "Prevailing Terms") will control and take precedence and priority unless otherwise agreed upon via Attachment F-1:</p> <ul style="list-style-type: none"> A. General Terms, Invoices and Payment, Section 7 B. General Terms, Maintenance of Insurance, Payment of Taxes, and Workers' Compensation, Section 8 (8.1 through 8.6) C. General Terms, Audits and Records Clause, Section 10 D. General Terms, Confidentiality, Section 11 E. General Terms Section 13, Assignment and Permitted Subcontractors; F. General Terms, Indemnification, Intellectual Property Infringement Indemnification, Section 16.1 G. General Terms, Bodily Injury and Tangible Personal Property Indemnity, Section 16.2 H. General Terms, Indemnification, Limitation of Liability, Section 16.3 I. General Terms, Section 17, Termination for Funding Insufficiency J. General Terms, Termination for Cause, Section 18 K. General Terms, Termination for Convenience, Section 19 L. General Terms, Force Majeure, Section 23 M. General Terms, Miscellaneous, Choice of Law and Venue, Section 26.1 N. General Terms, Miscellaneous, Sovereign Immunity Section 26.12 O. Oklahoma Statewide Terms, Contract Management Fee and Usage Report, Sections 6.1, 6.2, 6.3 P. Information Technology Terms, Definitions Section 1.3 Q. Information Technology Terms, Offshore Services, Section 5 R. For orders to which it applies, Section 4 of Schedule S, Attachment E-3

Term & Section	Language
	<p>S. Information Technology Terms, Appendix 1, Section C, Security Assessment</p> <p>T. For orders to which it applies, the terms of the Data Processing Agreement, as defined in Schedule C, Attachment E-1 (the “Data Processing Agreement”)</p> <p>Furthermore, no financial obligation of the State or Customers to Supplier shall be negatively affected by any change in any URLs.</p>
General Terms, Contract Effectiveness and Order of Priority, Section 2.3	<p>Section 2.3 is deleted in its entirety and replaced with:</p> <p>Reserved.</p>
General Terms, Modification of Contract Terms and Contract Documents, Section 3	<p>Section 3.1 is deleted in its entirety and replaced with the following:</p> <p>The Contract may only be modified, amended, or expanded by an Addendum. Any change to the Contract, including the addition of work or materials, the revision of payment terms, or the substitution of work or materials made unilaterally by the Supplier or the State, is a material breach of the Contract. Notwithstanding the foregoing, a Contract Document that is a Supplier Ordering Document, statement of work, or other similar order-specific document executed between the Supplier and a Customer that is an Affiliate may be amended by an Addendum signed by Supplier and the Customer. Unless otherwise specified by applicable law or rules, such changes, including without limitation, any unauthorized written Contract modification, shall be void and without effect and the Supplier nor State shall not be entitled to any claim under the Contract based on those changes. No oral statement of any person shall modify or otherwise affect the terms, conditions, or specifications stated in the Contract.</p>
General Terms, Modification of Contract Terms and Contract Documents, Section 3	<p>Section 3.2 is deleted in its entirety and replaced with the following:</p> <p>Any additional terms on an ordering document provided by Supplier are of no effect and are void unless mutually executed by the parties to such ordering document or through a purchase order provided by the State. OMES bears no liability for performance, payment or failure thereof by the Supplier or by a Customer other than OMES in connection with an Acquisition.</p>
General Terms, Definitions, Section 4	<p>Section 4.2 is deleted in its entirety and replaced with the following:</p> <p>Addendum means a written modification to a Contract Document mutually executed by the parties to the Contract Document.</p>

Term & Section	Language
General Terms, Definitions, Section 4	<p>Section 4.6 is deleted in its entirety and replaced with the following:</p> <p>Contract means the written, mutually agreed and binding legal relationship resulting from the Contract Documents and an appropriate encumbering document (which will include any Supplier Ordering Document or purchase order) as may be amended from time to time, which evidences the final agreement between the parties with respect to the subject matter of the Contract.</p>
General Terms, Definitions, Section 4	<p>Section 4.7 is deleted in its entirety and replaced with the following:</p> <p>Contract Document means this document; the information which is incorporated into this document or a Supplier ordering document, in each case, by written reference (including reference to information contained in a URL, specifically identified in this Contract (which, for the avoidance of doubt, includes information contained in any URLs linked to the original ULR, or subsequent URLs) or referenced policy specifically identified in this Contract or such Supplier ordering document); attachments to this Contract; any master or enterprise agreement terms entered into between the parties that are mutually agreed in writing to be applicable to the Contract; any statement of work, work order, or other similar mutually executed ordering document; other mutually executed documents under this Contract and any Addendum.</p>
General Terms, Definitions, Section 4	<p>Section 4.8 is deleted in its entirety and replaced with the following:</p> <p>Customer means OMES for all State Entity Acquisitions, and for Acquisitions by an Affiliate, means the Affiliate placing the order relating to the Acquisition. During the term of this Contract, any Affiliate, as defined herein, may utilize this Contract. Under this Contract, the State of Oklahoma bears no liability for an Affiliate's actions and the privities of contract exist solely between the Supplier and the Affiliate.</p>
General Terms, Definitions, Section 4	<p>Section 4.11 is deleted in its entirety and replaced with the following:</p> <p>Indemnified Parties means the State and Customer and/or its officers, directors, employees and representatives.</p>
General Terms, Definitions, Section 4	<p>Section 4.12, Inspection, is deleted in its entirety.</p>
General Terms, Definitions, Section 4	<p>Section 4.13, Moral Rights, is deleted in its entirety.</p>

Term & Section	Language
General Terms, Definitions, Section 4	<p>Section 4.16, Solicitation, is deleted and replaced with the following:</p> <p>Solicitation means the document, attached as Attachment A to the Contract, inviting Bids.</p>
General Terms, Definitions, Section 4	<p>Section 4.17 is deleted in its entirety and replaced with the following:</p> <p>State means the government of the state of Oklahoma, including where it is acting through its employees and authorized representatives, including without limitation any department, agency, or other unit of the government of the state of Oklahoma.</p>
General Terms, Modification of Contract Terms and Contract Documents, Section 4	<p>Section 4.18 is deleted in its entirety and replaced with the following:</p> <p>Supplier means Oracle America, Inc.</p>
General Terms, Modification of Contract Terms and Contract Documents, Section 4	<p>Section 4.21 (Work Product) is deleted in its entirety.</p>
General Terms, Modification of Contract Terms and Contract Documents, Section 4	<p>New Section 4.22 is added as follows:</p> <p>Affiliate means any governmental entity specified as a political subdivision of the State pursuant to the Governmental Tort Claims Act including any associated institution, instrumentality, board, commission, committee department or other entity designated to act on behalf of the political subdivision; and tribal entities authorized to utilize contracts awarded by the State via a multistate or multi governmental contract.</p>
General Terms, Modification of Contract Terms and Contract Documents, Section 4	<p>New Section 4.23 is added as follows:</p> <p>State Entity means any agency, authority, office, bureau, board, council, court, commission, department, district, institution, unit, division, body or house of any branch of the State government.</p>

Term & Section	Language
Modification of Contract Terms and Contract Documents, Section 4	<p>The following additional definitions are inserted in Section 4:</p> <p>4.24. Ordering Document means the Supplier ordering document pursuant to which a Product or Service Offering is ordered.</p> <p>4.25 Products refers to Programs.</p> <p>4.26 Program Documentation refers to the Program user manual and Program installation manuals. Program Documentation may be delivered with the Programs. Customer may access the documentation online at http://oracle.com/documentation.</p> <p>4.27 Schedules refers to the Supplier Schedules attached to this document or added via an Addendum; as of the effective date of the Contract, the Schedules are as follows: Schedule C, Attachment E-1; Schedule P, Attachment E-2; Schedule S, Attachment E-3, Schedule OSSS, Attachment E-4.</p> <p>4.28 Separate Terms refers to separate license terms that are specified in the Program Documentation, readmes or notice files and that apply to Separately Licensed Third Party Technology.</p> <p>4.29 Separately Licensed Third Party Technology refers to third party technology that is licensed under Separate Terms and not under the terms of the Contract.</p> <p>4.30 Service Offerings refers to technical support, education, hosted/outsourcing services, cloud services, consulting, advanced customer support services, or other services which Customer has ordered. Such Service Offerings are further described in the applicable Schedule.</p>
General Terms, Ordering, Inspection and Acceptance, Section 6	<p>Section 6.1 is deleted in its entirety and replaced with the following:</p> <p>Any product or service furnished under the Contract shall be ordered by issuance of a valid purchase order or other appropriate payment mechanism, by use of a valid Purchase Card (subject to Supplier's Invoicing Standards Policy, which may be accessed at http://oracle.com/contracts, and applicable law), and by execution of an Ordering Document for such Acquisition of Supplier products and services by the Customer. All orders and transactions are governed by the terms and conditions of the Contract. Any Ordering Document dated prior to termination or expiration of the Contract shall be performed unless mutually agreed in writing otherwise.</p>
General Terms, Ordering, Inspection and Acceptance, Section 6	<p>Section 6.2 is deleted in its entirety and replaced with the following:</p> <p>Service Offerings will be performed in accordance with the terms of the applicable Schedule and Ordering Document. The Schedules set forth terms and conditions that apply specifically to certain types of Supplier offerings which may be different than, or in addition to this Attachment B. For fixed price consulting engagements only, Supplier and the Customer may, in the applicable Ordering Document, negotiate and agree to an acceptable provision regarding the delivery of applicable deliverables.</p> <p>Subject to OAC 260:115-9, acceptance of Supplier products and services are described in the Ordering Document and applicable Schedules attached to the Contract.</p>

Term & Section	Language
	Supplier shall deliver products in accordance with the terms of the applicable Schedule and Ordering Document, subject to, in the case of fixed price consulting engagements, the terms of the applicable acceptance provision.
General Terms, Ordering, Inspection and Acceptance, Section 6	Section 6.3 is deleted in its entirety.
General Terms, Ordering, Inspection and Acceptance, Section 6	Section 6.4 is deleted in its entirety.
General Terms, Invoices and Payment, Section 7	<p>Section 7.1 is deleted in its entirety and replaced with the following:</p> <p>Supplier shall be paid upon submission of a proper invoice(s) at the prices stipulated in the Contract in accordance with 74 O.S. §85.44B which requires that payment be made only after products have been provided and accepted or services rendered and accepted. For purposes of 74 O.S. §85.44B, products and services shall be deemed to have been accepted upon receipt unless the State has provided written notice within seven (7) calendar days thereafter that such product or service does not meet acceptance criteria provided for in this Contract or the applicable order.</p> <p>The following terms additionally apply:</p> <p>A An invoice shall contain the purchase order number, description of products or services provided and the dates of such provision.</p> <p>B Failure to provide a timely and proper invoice may result in delay of processing the invoice for payment. Proper invoice is defined at OAC 260:10-1-2.</p> <p>C Payment of all fees under the Contract shall be due NET 30 days; however, Supplier acknowledges and agrees that payment received in accordance with applicable Oklahoma law allowing forty-five (45) days to pay Contractor shall not entitle Contractor to late payment fees or interest. Interest on late payments are governed by 62 O.S. §34.72. Such interest is the sole and exclusive calculation for late payments by a State agency and no other late fees are authorized to be assessed pursuant to Oklahoma law. Notwithstanding the foregoing, any assessment and/or payment of interest shall not preclude Supplier from invoking any termination rights provided under this Contract.</p> <p>D Reserved.</p>

Term & Section	Language
	<p>E If an overpayment or underpayment has been made to Supplier any subsequent payments to Supplier under the Contract may be adjusted to correct the account. A written explanation of the adjustment will be issued to Supplier.</p> <p>F Supplier shall not be entitled to apply fees owed on one transaction under this Contract to a separate transaction under this Contract, unless expressly agreed to by the parties to such transactions.</p> <p>G Supplier agrees to make commercially reasonable efforts to submit invoices in a timely fashion which, for the avoidance of doubt, shall be the time period prescribed by applicable law. The State may be prohibited by applicable law from paying invoices submitted after the time period prescribed by applicable law.</p> <p>H The Supplier shall accept payment by Purchase Card as allowed by Oklahoma law and subject to Supplier's Invoicing Standards Policy, which may be accessed at http://oracle.com/contracts.</p> <p>I Customer understands that Customer may receive multiple invoices for the Products and Service Offerings Customer ordered. Invoices will be submitted to Customer pursuant to Supplier's Invoicing Standards Policy, which may be accessed at http://oracle.com/contracts, and applicable law.</p>
General Terms, Maintenance of Insurance, Payment of Taxes, and Workers' Compensation, Section 8	<p>Section 8.1 is deleted in its entirety and replaced with new Sections 8.1 through 8.5 as follows:</p> <p><u>8.1.</u> As a condition of this Contract, Supplier shall procure at its own expense, and provide proof of, insurance coverage with the applicable liability limits set forth below or have the ability to pay applicable claims. For subcontractors, see Attachment E-2, Schedule S Services, as applicable. The required insurance shall be underwritten by an insurance carrier with an A.M. Best rating of A- or better.</p> <p><u>8.2</u> Upon State's or Customer's request, Supplier shall provide a certificate of insurance showing the coverage noted below in this Section 8.2 except Workers' Compensation if provided by the government. Supplier may not commence performance hereunder until such proof has been provided. Additionally, Supplier shall endeavor to provide a thirty (30) day notice of cancellation and name the State and its agencies as certificate holder and shall promptly provide proof to the State of any renewals, additions, or changes to such insurance coverage. Supplier's obligations under this Section 8 are continuing obligations until Supplier has no further obligation to provide Products or perform Service Offerings under the Contract. Any combination of primary and excess or umbrella insurance may be used to satisfy the limits of coverage for Commercial General Liability, Auto Liability and Employers' Liability. Unless agreed between the parties and approved by the State Purchasing Director</p>

Term & Section	Language
	<p>or the Chief Information Officer in a Contract Addendum, Supplier maintains the following insurance at its expense or has the ability to pay applicable claims to cover Supplier's performance of Service Offerings:</p> <p>A Workers' Compensation Insurance as required by the statute of states where Service Offerings are performed;</p> <p>B Employer's Liability Insurance \$1,000,000 per occurrence;</p> <p>C Commercial General Liability Insurance \$5,000,000 per occurrence/aggregate bodily injury and \$5,000,000 per occurrence/aggregate tangible property damage;</p> <p>D Automobile Liability Insurance \$5,000,000 per occurrence, bodily injury and tangible property damage;</p> <p>E Supplier maintains the following insurance at its expense or has the ability to pay applicable claims: professional liability/errors and omission insurance (including privacy and computer network security (also known as cyber) liability insurance) with US \$5,000,000 per claim/aggregate covering Supplier's errors and omissions while providing Service Offerings under the Contract. Upon State's or Customer's request, Supplier shall provide documentation showing the foregoing errors and omissions insurance coverage;</p> <p>F Additional coverage may be required in an Ordering Document in connection with a particular Acquisition.</p> <p>G Supplier may select a new insurance carrier or carriers or may obtain new or amended policies at any time. This provision is not intended to, and does not, increase or decrease Supplier's liability under the Limitation of Liability section of this Contract.</p>
General Terms, Maintenance of Insurance, Payment of Taxes, and Workers' Compensation, Section 8	<p>Section 8.2 is renumbered as Section 8.6 and is deleted in its entirety and replaced with the following:</p> <p>Supplier or its subcontractors shall be entirely responsible during the existence of the Contract for the liability and payment of taxes payable by or assessed to, as applicable, Supplier, such subcontractors or their respective employees, and of whatever kind, in connection with the Contract. Supplier further agrees to comply with all state and federal laws applicable to its engagement of any such persons, including laws regarding wages, taxes, insurance, and Workers' Compensation where applicable. Neither Customer nor the State shall be liable to the Supplier, its employees, agents, or others for the payment of taxes or the provision of unemployment insurance and/or Workers' Compensation or any benefit available to a State or Customer employee.</p>

Term & Section	Language
General Terms, Maintenance of Insurance, Payment of Taxes, and Workers' Compensation, Section 8	Delete Section 8.3 in its entirety.
General Terms, Compliance with Applicable Laws, Section 9	<p>Sections 9.1 and 9.2 are deleted in their entirety and replaced with the following:</p> <p>As long as Supplier has an obligation under the terms of the Contract and in connection with performance of its obligations, the Supplier represents, to the best of its knowledge, its present compliance, and shall have an ongoing obligation to comply, with all applicable federal, State, and local laws, rules, regulations, ordinances, and orders, as amended (collectively, "legal requirements") i) to the extent such legal requirements, by their terms, impose obligations directly upon Supplier in its capacity as an information technology service provider with respect to the provision of Products and Service Offerings hereunder or ii) as otherwise expressly agreed upon by the parties in an applicable Ordering Document. Such legal requirements may include, but are not limited to the following:</p> <p>A Drug-Free Workplace Act of 1988 set forth at 41 U.S.C. §81.</p> <p>B Section 306 of the Clean Air Act, Section 508 of the Clean Water Act, Executive Order 11738, and Environmental Protection Agency Regulations which prohibit the use of facilities included on the EPA List of Violating Facilities under nonexempt federal contracts, grants or loans;</p> <p>C Prospective participant requirements set at 45 C.F.R. part 76 in connection with Debarment, Suspension and other responsibility matters;</p> <p>D 1964 Civil Rights Act, Section 504 of the Rehabilitation Act of 1973, Americans with Disabilities Act of 1990, and Executive Orders 11246 and 11375;</p> <p>E Anti-Lobbying Law set forth at 31 U.S.C. §1325 and as implemented at 45 C.F.R. part 93;</p> <p>F Reserved</p> <p>G Requirements of the Oklahoma Taxpayer and Citizen Protection Act of 2007, 25 O.S. §1312 and applicable federal immigration laws and regulations and be registered and participate in the Status Verification System. The Status Verification System is defined at 25 O.S. §1312, includes but is not limited to the free Employment</p>

Term & Section	Language
	<p>Verification Program (E-Verify) through the Department of Homeland Security, and is available at www.dhs.gov/E-Verify;</p> <p>H Reserved; and</p> <p>I Legal requirements to be registered as a business entity licensed to do business in the State, have obtained a sales tax permit, and be current on franchise tax payments to the State, as applicable.</p> <p>9.2 Reserved.</p>
General Terms, Compliance with Applicable Laws, Section 9	<p>Section 9.4 is deleted in its entirety and replaced with the following:</p> <p>In addition to compliance under subsection 9.1 above, Supplier shall have a continuing obligation to comply with applicable Customer-specific mandatory contract provisions required in connection with the receipt of federal funds or other funding source that are included on the applicable statement of work or Ordering Document.</p>
General Terms, Compliance with Applicable Laws, Section 9	<p>Section 9.5 is deleted in its entirety and replaced with the following:</p> <p>The Supplier is responsible to review and inform its employees, agents, and subcontractors who provide a product or perform a service under the Contract of the Supplier's obligations under the Contract and Supplier is responsible for its employees' and each such subcontractor's compliance with minimum requirements and applicable provisions of the Contract. At the request of the State, Supplier shall promptly provide adequate evidence that such persons are its employees, agents or approved subcontractors and have been informed of their obligations under the Contract.</p>
General Terms, Compliance with Applicable Laws, Section 9	<p>Section 9.6 is deleted in its entirety and replaced with the following:</p> <p>To the extent applicable to Supplier's performance of Service Offerings under the Contract, Supplier agrees to comply with the Governor's Executive Orders related to the use of any tobacco product, electronic cigarette or vaping device on any and all properties owned, leased, or contracted for use by the State, including but not limited to all buildings, land and vehicles owned, leased, or contracted for use by agencies or instrumentalities of the State.</p>
General Terms, Compliance with Applicable Laws, Section 9	<p>Section 9.9 is deleted in its entirety and replaced with the following:</p> <p>Supplier represents that, to the best of its knowledge, Supplier is not aware of any litigation or claim or any threat thereof that negatively impacts the ability of the Supplier to comply with the terms of or fulfill any obligations under this Contract or any order(s) placed under this Contract.</p>
General Terms, Compliance with Applicable Laws, Section 9	<p>Section 9.10 is deleted in its entirety and replaced with the following:</p> <p>See Section 3, Compliance and Electronic and Information Technology Accessibility, of Attachment D, Information Technology Terms.</p>

Term & Section	Language
General Terms, Audits and Records Clause, Section 10	<p>Section 10.1 is deleted in its entirety and replaced with the following:</p> <p>Customer shall be permitted to inspect and audit records relating to the performance of this Contract on the following conditions: (i) such inspection and audit shall be limited to the data and records of Supplier that are related to the performance of this Contract and necessary to determine compliance under this Contract; (ii) such inspection and audit does not violate any nondisclosure or confidentiality agreements Supplier may have with third parties; (iii) such inspection and audit is conducted during Supplier's normal business hours and does not unreasonably interfere with Supplier's business operations; (iv) such inspection and audit is conducted on a reasonable basis; and (v) such inspection and audit is conducted after reasonable advance written notice has been provided to Supplier.</p>
General Terms, Audits and Records Clause, Section 10	<p>Section 10.2 is deleted in its entirety and replace it with the following:</p> <p>For a period of seven (7) years from the effective date of an Ordering Document under this Contract, the Customer, the State or any federal government entity (provided said federal entity is authorized to perform such audit under an applicable law or regulation), shall have the right to audit records and payments for Products and Service Offerings provided to the State thereunder, upon reasonable written notice to Supplier, no more than one time per year, at the State's or Customer's cost, and provided that such audit does not unreasonably interfere with Supplier's normal business operations. The Supplier is required to retain records relative to the Contract for the duration of the Contract and for a period of seven (7) years following completion or termination of an Acquisition except as otherwise provided by the terms of the Contract (e.g., provisions requiring deletion of certain information). If a claim, audit, litigation or other action involving such records is started before the end of the seven-year period, the records are required to be maintained for two (2) years from the date that all issues arising out of the action are resolved, or until the end of the seven (7) year retention period, whichever is later. The State or Customer shall have the right to contract a third-party audit firm to conduct such an audit, provided that such third-party audit firm agrees to Supplier's standard nondisclosure terms, to the extent it does not conflict with applicable law or prohibit the disclosure of audit findings to the State or Customer contracting with the auditor, and to utilize standard audit software.</p>
General Terms, Confidentiality, Section 11	<p>Section 11 is deleted in its entirety and replace with the following:</p> <p>11.1 By virtue of the Contract, the parties may have access to information that is confidential to one another as clearly identified in writing as confidential at the time of disclosure ("Confidential Information"). The parties agree to disclose Confidential Information to employees and subcontractors only to the extent required for the performance of obligations under the Contract. If the receiving Party determines that there has been an unauthorized disclosure of the disclosing Party's Confidential Information, an unauthorized use that compromises the</p>

Term & Section	Language
	<p>confidentiality or integrity of the Confidential Information, or unauthorized access to a Party's systems holding the Confidential Information that compromises the confidentiality or integrity of the Confidential Information, receiving Party will use reasonable efforts to promptly notify disclosing Party of such disclosure or loss, use, and/or access (provided that with respect to Customer Data in any Cloud Service (as defined in Schedule C), the provisions of Attachment D and the Data Processing Agreement shall control).</p> <p>11.2 A party's Confidential Information shall not include information that: (a) is or becomes a part of the public domain through no act or omission of the other party; (b) was in the other party's lawful possession prior to the disclosure and had not been obtained by the other party either directly or indirectly from the disclosing party; (c) is lawfully disclosed to the other party by a third party without restriction on the disclosure; (d) is independently developed by the other party; or (e) terms or pricing under the Contract, orders made under the Contract, or other Contract Documents.</p> <p>11.3 Subject to applicable law, the parties agree not to disclose each other's Confidential Information to any third party other than those set forth in the following sentence for a period of seven years from the date of the disclosing party's disclosure of the Confidential Information to the receiving party. Confidential Information may be disclosed only to those third parties who necessarily need the Confidential Information in order to perform obligations under the Contract and such third parties shall be required to protect it against additional disclosure. The Customer shall only provide Supplier with Confidential Information as required to allow Supplier to provide the services contemplated under the agreement. Nothing shall prevent either party from disclosing the terms or pricing under the Contract or orders submitted under the Contract in any legal proceeding arising from or in connection with the Contract or disclosing the Confidential Information to a governmental entity as required by law. Upon written request of the disclosing party (a party disclosing confidential information under this Contract), the recipient (a party receiving confidential information under this Contract) shall, to the extent permitted by law, promptly return or destroy any of the disclosing party's confidential information in the recipient's possession and control.</p> <p>11.4 The Supplier further agrees to evidence its confidentiality obligation in a separate writing if required under applicable federal or State laws, rules and regulations. If Supplier utilizes a subcontractor, Supplier shall obtain specific written assurance, and provide confirmation to the State or Customer, as applicable, upon request, that the subcontractor shall maintain this same level of security of all data and records entrusted to or accessed by the subcontractor and agree to the same obligations as Supplier, to the extent applicable.</p>

Term & Section	Language
	<p>11.5 In the event any party receives a valid legal request for Confidential Information of another party (whether related to a legal proceeding, governmental entity request, or otherwise), the party receiving the request shall, to the extent permitted by law, provide the other party with reasonable notice of such request and give an opportunity to object to or limit any such disclosure and shall, to the extent the parties' interests are aligned, reasonably cooperate with efforts to protect the security and confidentiality of the Confidential Information.</p> <p>11.6 To the extent a Customer requires Supplier to access personal information (including without limitation health, payment card or other sensitive personal information) to perform Service Offerings under an order, the parties agree to specify any security measures applicable to Supplier's treatment of such data in the order for such Service Offerings.</p> <p>11.7 Supplier acknowledges that all State agencies and certain other Customers are subject to the Oklahoma Open Records Act set forth at 51 O.S. 24A.1 <i>et seq.</i>, as may be amended (the "Act"). Supplier also acknowledges that such Customers will comply with the Act and with all opinions of the Oklahoma Attorney General concerning the Act. Customer agrees, to the extent permitted by law, to provide Supplier reasonable notice prior to disclosing any of Supplier's Confidential Information in response to a valid request made pursuant to the Oklahoma Open Records Act to allow Supplier to seek injunctive relief or such other relief as may be appropriate.</p>
General Terms, Conflict of Interest, Section 12	<p>Delete Section 12 in its entirety and replace with the following:</p> <p>In addition to any requirement of law or of a professional code of ethics or conduct, the Supplier and its employees are required to disclose any outside activity or interest that creates a direct conflict of interest with the State. Prompt disclosure is required under this section if the activity or interest is related, directly to any person or entity currently under contract with the State, and its employees. No Supplier personnel performing work under this Contract may voluntarily acquire any personal interest that conflicts with the Supplier's responsibilities under this Contract. Additionally, Supplier will not knowingly permit any public official or public employee who has any responsibilities related to this Contract to acquire an interest in anything or any entity under the Supplier's control, if such an interest would conflict with that official's or employee's duties. Supplier will disclose to the State knowledge of any such person who acquires an incompatible or conflicting personal interest related to this Contract. Supplier will take all reasonable steps to ensure that such a person does not participate in any action affecting the work under this Contract, unless the State has determined that, in light of the personal interest disclosed, that person's participation in any such action would not be contrary to the public interest.</p>

Term & Section	Language
General Terms Section 13, Assignment and Permitted Subcontractors	Delete Section 13.2 in its entirety and replace with the following: Notwithstanding the foregoing, the Contract may be assigned by Supplier to any corporation or other entity in connection with a merger, consolidation, acquisition, internal restructuring, sale of all equity interests of the Supplier, or a sale of all or substantially all of the assets of the Supplier to which the Contract relates. In any such case, said corporation or other entity shall by operation of law or expressly in writing assume all obligations of the Supplier as fully as if it had been originally made a party to the Contract. Supplier shall give the State and all affected Customers written notice of said assignment. Any assignment or delegation in violation of this Section 13 shall be void.
General Terms Section 13, Assignment and Permitted Subcontractors	Delete Section 13.3 in its entirety and replace with the following: See Attachment E-2, Schedule S Services. No resellers shall be authorized under this Contract until otherwise agreed upon in an Addendum to this Contract.
General Terms Section 13, Assignment and Permitted Subcontractors	Delete Section 13.4 in its entirety and replace with the following: All payments under the Contract shall be made directly to the Supplier except as provided in subsection 13.1 above regarding the Supplier's assignment of payment.
General Terms Section 13, Assignment and Permitted Subcontractors	Delete Section 13.5 in its entirety and replace with the following: State or Customer, as applicable, may not assign the Contract or give or transfer the Programs and/or any Service Offerings or an interest in them to another individual or entity without Supplier's prior written consent, provided, however, where the transferee is a State Entity ("State Entity transferee"), no written consent from Supplier or additional cost is necessary in the event of a legislative mandate to transfer the Contract, or a portion thereof, from one State Entity to the State Entity transferee. With respect to any assignment to a State Entity transferee, the State agrees (i) to provide Supplier prior notice of such assignment and (ii) that upon such assignment, the State Entity transferee shall agree in writing to the terms and conditions of the Contract (including any Ordering Document or statement of work applicable to the Acquisition). If State or Customer grants a security interest in the Programs and/or any Service Offerings deliverables, the secured party has no right to use or transfer the Programs and/or any Service Offerings deliverables, and if State or Customer decides to finance State's acquisition of any Products and/or any Service Offerings, State or Customer, to the extent it does not conflict with applicable law, will follow Supplier's policies regarding financing which are at http://oracle.com/contracts . The foregoing shall not be construed to limit the rights State or any Customer may otherwise have with respect to the Linux operating system, third party technology or Separately Licensed Third Party Technology licensed under open source or similar license terms.

Term & Section	Language
General Terms, Section 14, Background Checks and Criminal History Investigations	<p>Delete Section 14, Background Checks and Criminal History Investigations, in its entirety and replace with the following:</p> <ul style="list-style-type: none"> <li data-bbox="440 415 1406 1087">A. Supplier, or its agent, has performed a background check on Supplier employees hired on or after January 1, 2003 in the United States. As of the effective date of the Contract, the background check is used to attempt to (i) ascertain an employee's previous employment with up to three (3) employers within the five (5) year period preceding the date of the check; (ii) ascertain an employee's highest degree earned; (iii) assess any public criminal records uncovered for an employee, within the seven (7) years preceding the date of the check; and (iv) check for matches on the Office of Foreign Asset Control's Specially Designated Nationals and Foreign Sanctions Evaders Lists. The background check is adjudicated by Supplier. While all criminal records are individually assessed in accordance with applicable laws and agency guidance, generally, significant crimes involving violence, dishonesty, and certain drug-related offenses are considered disqualifiers, except where a diversion program was successfully completed and/or the case was discharged or judicially dismissed. Processing and procedural variances may apply to students/interns, university recruiting hires, and to employees of companies acquired by Supplier. <li data-bbox="440 1142 1406 1276">B. Supplier's current Services Provider Agreement ("SPA") requires entities providing Services to Oracle under the SPA to perform background checks on resources employed or retained by those entities to provide services under the SPA. <li data-bbox="440 1310 1406 1520">C. To the extent required by an Ordering Document, at Customer's request, Supplier will provide confirmation to Customer that a background investigation has been completed for any Supplier employee performing professional services under the Ordering Document, and that the results of the investigation would not disqualify the individual from providing services to the Customer. <li data-bbox="440 1554 1406 1715">D. The Supplier and the Customer may negotiate and agree on additional background checks in an Ordering Document or Contract Document, including terms governing the removal reassignment or rejection of employees or subcontractors who have failed such specified checks.

Term & Section	Language
	<p>Delete Section 15 in its entirety and replace with the following:</p> <p>Without exception, a product or deliverable price shall include all royalties or costs owed by the Supplier to any third party arising from the use of a patent, intellectual property, copyright or other property right held by such third party.</p>
General Terms, Indemnification, Section 16	Section 16.1 shall be deleted in its entirety.
General Terms, Indemnification, Section 16	<p>Section 16.2, Infringement, shall be renumbered as Section 16.1 and retitled as Intellectual Property Infringement Indemnification, and shall be deleted in its entirety and replaced with the following:</p> <p><u>Intellectual Property Infringement Indemnification</u></p> <p>A Supplier shall indemnify the Indemnified Parties, as applicable, for all liability, damages, costs and expenses, (including without limitation reasonable attorneys' fees awarded by a court to any third party claiming infringement or included in the settlement with such third party that is agreed to by the Supplier) for actions, claims, demands, and suits by a third party alleging infringement of any patents, copyrights, trade and service marks, and any other intellectual property right in connection with a Products or Service Offerings provided under the Contract; provided that the Customer:</p> <p>(i) notifies Supplier promptly in writing, not later than 30 days after Customer receives notice of the claim (or sooner if required by applicable law);</p> <p>(ii) to the extent permitted by law, and pursuant to approval from the State's Attorney General, gives Supplier sole control of the defense and any settlement negotiations; provided, however, that without Customer's written consent, Supplier may not (a) admit that Customer has any liability, (b) obligate Customer to pay any sum or (c) make any admission of a wrongdoing by Customer in conjunction with the defense or as a result of the settlement of the claim.</p> <p>(iii) gives Supplier the information, authority and reasonable assistance Supplier needs to defend against or settle the claim; reasonable out-of-pocket expenses incurred by the Customer in providing such assistance will be reimbursed by Supplier.</p> <p>B Should it be determined that that any Product or Service Offering provided by Supplier under the Contract infringes a third party's intellectual property rights, Supplier shall obtain a license for continued use or modify the affected Product or Service Offering to be non-infringing (while substantially preserving its utility or functionality) or, if these alternatives are not commercially reasonable, Supplier may end the license for, and require return of,</p>

Term & Section	Language
	<p>the applicable Product or Service Offering, or portion thereof (the "Infringing Material"), and refund any fees the Customer may have paid for it and any unused, prepaid technical support fees Customer has paid to Supplier for the license of the infringing Program, if any; provided, however, that if the program documentation for another Program licensed by the Customer under the same Ordering Document as the Infringing Material (the "Other Program") specifies that the Other Program is functionally dependent upon the Infringing Material, then the Customer may also recover fees paid to Supplier for such Other Program license, provided that the Customer agrees to end the license for such Other Program and return it to Supplier.</p> <p>C Supplier will not indemnify Customer if Customer alters the Program or Service Offering (to the extent that such claim is based on such alteration) or uses it outside the scope of use identified in Supplier's user documentation (to the extent that such claim arises from such use), or if Customer uses a version of the Program or Service Offering which has been superseded, if the infringement claim could have been avoided by using an unaltered current version of the Program or Service Offering which was provided to Customer, or if Customer continues to use the applicable the Program or Service Offering after the end of the license to use that Program or Service Offering. Supplier will not indemnify Customer to the extent that an infringement claim is based upon any information, design, specification, instruction, software, data, or material (collectively, "Material") not furnished by Supplier. Supplier will not indemnify Customer for any portion of an infringement claim that is based upon the combination of any Program or Service Offering with any products or services not provided by Supplier. Solely with respect to Separately Licensed Third Party Technology that is part of or is required to use a Program and that is used: (a) in unmodified form; (b) as part of or as required to use a Program; and (c) in accordance with the license grant for the relevant Program and all other associated terms and conditions of the Contract, Supplier will indemnify Customer for infringement claims for Separately Licensed Third Party Technology to the same extent as Supplier is required to provide infringement indemnification for the Program under the terms of the Contract. Supplier will not indemnify Customer for infringement caused by Customer's actions against any third party if the Program(s) as delivered to Customer and used in accordance with the terms of the Contract would not otherwise infringe any third party intellectual property rights. User documentation includes any Service Specifications (as defined in Schedule C) referenced in Customer's order for Service Offerings.</p> <p>D Supplier will not indemnify Customer to the extent that an infringement claim is based on Third Party Content (as defined in Schedule C) or any Material (as defined in Subsection C above) from a third party portal or other external source that is accessible or</p>

Term & Section	Language
	<p>made available to Customer within or by the Service Offerings (e.g., a social media post from a third party blog or forum, a third party Web page accessed via a hyperlink, marketing data from third party data providers, etc.).</p> <p>E This Section 16.1 states Supplier's entire liability and exclusive remedy with respect to infringement.</p>
General Terms, Indemnification, Section 16	<p>Section 16.3, Notice of Cooperation, is renumbered as Section 16.2 and retitled as Bodily Injury and Tangible Personal Property Indemnity and is deleted in its entirety and replaced with the following:</p> <p>Supplier shall defend and indemnify the Indemnified Parties for all liability, damages, costs and expenses, (including without limitation reasonable attorneys' fees awarded by a court to the third party claimant or included in the settlement with such third party that is agreed to by the Supplier) against any and all third party actions, claims, demands, and suits for bodily injury and/or tangible personal property damage caused solely by Supplier's intentional wrongful conduct while performing Services on Customer's premises, provided that:</p> <p>(a) Customer notifies Supplier promptly in writing, not later than thirty (30) calendar days after Customer receive notice of the claim (or sooner if required by law)</p> <p>(b) Customer gives Supplier sole control of the defense and any settlement negotiations, to the extent permitted by law and pursuant to approval from the State's Attorney General; provided, however, that without Customer's written consent, Supplier may not (i) admit that Customer has any liability, (ii) obligate Customer to pay any sum or (iii) make any admission of a wrongdoing by Customer in conjunction with the defense or as a result of the settlement of the claim. and</p> <p>(c) Customer gives Supplier the information, authority and assistance Supplier needs to defend against or settle the claim; reasonable out-of-pocket expenses incurred by the Customer in providing such assistance will be reimbursed by Supplier.</p> <p>As used in this section, the term "tangible personal property" shall not include software, documentation, data or data files. To the extent not prohibited by law, Supplier shall have no liability for any claim of bodily injury or tangible personal property damage arising from its use of software or hardware. To the extent not prohibited by law, this section states Supplier's entire liability and Customer's exclusive remedy for bodily injury and property damage for third party actions, claims, demands and suits for Supplier's intentional wrongful conduct while performing Services on Customer's premises.</p>
General Terms, Indemnification, Section 16	Section 16.4, Coordination of Defense, is deleted in its entirety.

Term & Section	Language
General Terms, Indemnification, Section 16	<p>Section 16.5, Limitation of Liability, is renumbered as Section 16.3 and is deleted in its entirety and replaced with the following:</p> <p>Limitation of Liability</p> <p>A With respect to any claim or cause of action arising under or related to the Contract, neither party nor any Customer shall be liable for lost profits, lost sales, loss of data or data use, lost revenue, or business expenditures, investments, or commitments in connection with any business, loss of any goodwill, or for any other indirect, incidental, punitive, special or consequential damages, even if advised of the possibility of such damages.</p> <p>B Notwithstanding anything to the contrary in the Contract, no provision shall limit damages, expenses, costs, actions, claims, and liabilities arising from or related to acts for which applicable law does not allow exemption from liability under a contract.</p> <p>C The limitation of liability and disclaimers set forth in the Contract will apply regardless of whether Customer has accepted a Product or Service Offering.</p> <p>D Except for liability related to indemnity obligations set forth in Sections 16.1 and 16.2 above, Supplier's maximum liability for any damages arising out of or related to the Contract or any order, whether in contract or tort, or otherwise, shall be (i) with respect to Cloud Services (as defined in Schedule C attached hereto as Attachment E-1) the total amounts actually paid by the Customer to Supplier for the Cloud Services under the order giving rise to such liability in the thirty-six (36) month period immediately preceding the event giving rise to the liability and (ii) for all other Products and Service Offerings, the amount of fees the Customer paid Supplier under the applicable Contract Document (i.e., Schedule and Ordering Document) giving rise to the liability and if such damages result from the Customer's use of Products or Service Offerings, such liability shall be limited to the fees the Customer paid Supplier for the deficient Product or Service Offering giving rise to the liability. Customer and Supplier may negotiate higher limitations of liability in a Supplier Ordering Document.</p> <p>E Notwithstanding Section 16.3(D) above, in no event shall the aggregate liability of Supplier and the Oracle Affiliates (as defined in the Data Processing Agreement) arising out of or related to this Contract or any Order placed under this Contract for misappropriation or unauthorized disclosure of Customer Data (as defined in Attachment D) that is caused solely by Supplier's breach of its security practices described in the Service Specifications exceed the lesser of (i) Twenty Million Dollars (\$20,000,000) or (ii) four (4) times the total amounts actually paid to Oracle under this Contract for Cloud Services (as defined in Schedule C, Attachment</p>

Term & Section	Language
	E-1) in the twelve (12) months immediately preceding the event giving rise to the liability.
General Terms, Section 17, Termination for Funding Insufficiency	<p>Section 17 is deleted in its entirety and replaced with the following:</p> <p>17.1 Any amount paid to Supplier in the form of prepaid fees that are unused when the applicable Ordering Documents are terminated shall be refunded.</p> <p>17.2 The State may terminate the Contract or a Ordering Document when its obligation to pay amounts due thereunder in a subsequent fiscal period if funds sufficient to pay such amounts are not (a) appropriated by the applicable state legislature, federal government or other appropriate government entity in such fiscal period or (b) received in such fiscal period from a previously committed federal grant. Similarly, a Customer may terminate any Ordering Document if funds sufficient to pay amounts due thereunder in a subsequent fiscal period are not (x) appropriated by the applicable state legislature, federal government or other appropriate government entity in such fiscal period or (y) received in such fiscal period from a previously committed federal or State grant. In the event of such insufficiency, Supplier will be provided fifteen (15) calendar days prior written notice of intent to terminate, together with reasonable details regarding the non-appropriation of funds, as reasonably requested by Supplier or as mandated by applicable law. The determination by the State or Customer, as applicable, as to whether sufficient appropriations are available shall be accepted by Supplier as final and binding. Notwithstanding the foregoing, (1) with each executed order, Customer must have provided both of the following: (a) a signed Ordering Document referencing the Contract, and (b) a purchase order; and (2) Customer's signature on an Ordering Document referencing the Contract and issuance of a purchase order by Customer shall signify to Supplier that all funds for the order, which funds are or will become, pursuant to such order, due and payable in the then current fiscal year, have been fully appropriated (or, in the case of a federal or State grant, have been fully received) and are available and no longer subject to any appropriations contingency. In the event of such termination, the Customer will not be considered to be in default or breach under the Contract nor shall it be liable for any further payments ordinarily due under the Contract, nor shall it be liable for any damages or any other amounts which are caused by or associated with such termination. Notwithstanding the foregoing, (i) each Customer agrees to pay for all Products delivered and Service Offerings performed (subject to, in the case of fixed price consulting engagements, the terms of the applicable acceptance provision (if any)) prior to the termination date stated in such Customer's notice of non-appropriations and (ii) the State's or applicable Customer's right to use any part of the Products shall terminate on such termination date.</p>

<p>General Terms, Termination for Cause, Section 18</p>	<p>Delete Section 18.1 in its entirety and replace with the following:</p> <p>A Supplier may terminate the Contract if (i) it has provided the State with written notice of material breach and (ii) the State fails to cure such material breach within thirty (30) days of receipt of written notice. If there is more than one Customer, material breach by a Customer does not give rise to a claim of material breach as grounds for termination by Supplier of the Contract as a whole. Notwithstanding the foregoing, in the event of a material breach by a Customer, Supplier shall have the right to 1) terminate any orders with the breaching Customer, provided that for breaches arising out of nonpayment for State Entity Acquisitions where OMES has placed an order on behalf of another State Entity and payment obligations are identified in the order as shifted to that State Entity, Supplier may only terminate orders placed by that State Entity (or by OMES on behalf of that State Entity); and 2) decline to accept orders from an Affiliate who is a breaching Customer for the term of the Contract.</p> <p>B The State may terminate the Contract in whole or in part if (i) it has provided Supplier with written notice of material breach, including any event identified in OAC 260: 115-9-1(j) that would constitute a material breach of this Contract, and (ii) Supplier fails to cure such material breach within thirty (30) days of receipt of written notice. Similarly, a Customer may terminate its obligations, in whole or in part, to Supplier if it has provided Supplier with written notice of a breach of a material term of the Contract, and Supplier fails to cure such breach within thirty (30) days of receipt of written notice. Supplier may terminate an Ordering Document in the event (i) it has provided the Customer with written notice of breach of a material term of the Ordering Document and (ii) the Customer fails to cure such breach within thirty (30) days of receipt of written notice. Any amount paid to Supplier in the form of prepaid fees that are unused when the Contract or certain obligations are terminated shall be refunded.</p> <p>C The non-breaching party may agree in its sole discretion to extend the 30 day period for so long as the breaching party continues reasonable efforts to cure the breach.</p> <p>D The State and Customer agree that if State or Customer is in default under the Contract, the State or Customer may not use those Products or Service Offerings ordered if the breach remains uncured after the cure period. If the State or Customer has used a contract with Supplier or an affiliate of Supplier to pay for the fees due under an order and State or Customer is in default under that contract, State or Customer may not use the Products and/or Service Offerings that are subject to such contract. Notwithstanding the foregoing, Customer must pay in accordance with the payment terms detailed in Section 7 (Invoices and Payment) of this Attachment B all amounts that have accrued prior to such termination of an order, as well as all sums remaining unpaid for the Service Offerings rendered and accepted.</p>
---	---

Term & Section	Language
	E Any partial termination of the Contract under this section shall not be construed as a waiver of, and shall not affect, the rights and obligations of any party regarding portions of the Contract that are not terminated.
General Terms, Termination for Cause, Section 18	Delete Section 18.2 in its entirety and replace it with the following: Any amount paid to Supplier under an Ordering Document in the form of prepaid fees that are unused when the Ordering Document is terminated shall be refunded.
General Terms, Termination for Cause, Section 18	Delete Section 18.3 in its entirety.
General Terms, Termination for Cause, Section 18	Delete Section 18.4 in its entirety.
General Terms, Termination for Convenience, Section 19	Delete Section 19.1 in its entirety and replace with the following: The State may terminate the Contract for convenience if it is determined that termination is in the State's best interest. In the event of a termination for convenience, Supplier will be provided at least thirty (30) days' written notice of termination.
General Terms, Termination for Convenience, Section 19	Delete Section 19.2 in its entirety.

Term & Section	Language
General Terms, Suspension of Supplier, Section 20	<p>Delete Section 20 in its entirety and replace with the following:</p> <p>20.1 Pursuant to OAC 260:115-3-21 Supplier may be subject to Suspension and shall receive a written Suspension notice as required by law. Upon receipt of a notice pursuant to this section, Supplier shall take reasonable steps to minimize the incurrence of costs allocable to the work affected notice. Supplier shall, unless otherwise prohibited by law, comply with the notice terms. Supplier may request clarification and/or modification of the scope of suspension with the State, which the parties shall memorialize.</p> <p>20.2 Upon receipt of Suspension notice, Supplier may appeal a suspension in writing to the State Purchasing Director within five (5) business days of receipt of the suspension notice; however, the Supplier shall be suspended pending a determination of the appeal.</p> <p>20.3 Such Suspension may be removed, and suspended activity may resume, upon written notice of Supplier reinstatement. This subsection is not intended to operate as an affirmative statement that such resumption will occur.</p> <p>20.4. Notwithstanding the foregoing, Suspension of the Supplier shall not relieve the State or any Customer, as applicable, of any payment obligations for all services rendered and accepted prior to the Suspension date in accordance with the terms of the applicable order, or for services excepted from Suspension but there shall not be any liability for services that are covered by a Suspension that are rendered during a period of Suspension. Any amount paid to Supplier under an Ordering Document in the form of prepaid fees attributable to a period of Suspension or suspended activity under the Ordering Document shall be refunded. In the case of an order for Cloud Services (as defined in Schedule C attached hereto as Attachment E-1), for purposes of clarity around data retention and deletion requirements, any Suspension that applies to the provision of Cloud Services under the order shall give each of the Supplier and the Customer, as applicable, a right to immediately terminate the order. Such termination shall be deemed to be a termination for convenience, but shall not relieve any party of liability for claims arising under the Contract or the Ordering Document, or constitute a waiver of any rights or remedies available under this Contract or applicable law.</p> <p>20.5 A right exercised under this section shall not be an exclusive remedy. but shall be in addition to any other rights and remedies provided for by law.</p>

Term & Section	Language
General Terms, Certification Regarding Debarment, Suspension and Other Responsibility Matters, Section 21	<p>Delete the first sentence of Section 21 in its entirety and replace with the following:</p> <p>Any certification made by Supplier in this Contract with respect to Debarment, Suspension, certain indictments, convictions, civil judgments and terminated public contracts is a material representation of fact upon which reliance was placed when entering into the Contract. Any certification made by Supplier in any Contract Document entered into with respect to this Contract's renewal is a material representation of fact upon which reliance will be placed into entering into the renewal of the Contract.</p>
General Terms, Certification Regarding State Employees Prohibition from Fulfilling Services, Section 22	<p>Delete Section 22 in its entirety. and replace with the following:</p> <p>To comply with the provisions of 74 O.S. § 85.42, Supplier certifies that no person involved in any manner in development of the Contract while employed by the State shall be employed to fulfill any services provided under the Contract.</p> <p>The parties acknowledge that the foregoing certification is solely for the State's benefit, and does not restrict, and Supplier does not seek to restrict in any manner, the ability of the State or any Customer to solicit or hire individuals employed by Supplier.</p>
General Terms, Force Majeure, Section 23	<p>Delete Section 23.1 in its entirety and replace with the following:</p> <p>Either party shall be temporarily excused from performance to the extent delayed as a result of unforeseen causes beyond its reasonable control including fire or other similar casualty, act of God, strike or labor dispute, war or other violence, pandemic, electrical, internet, or telecommunication outage that is not caused by the obligated party, or any law, order or requirement of any governmental agency or authority (including the denial or cancellation of any export, import or other license), provided the party experiencing the force majeure event has used commercially reasonable efforts to continue performance and to shorten duration of the event to the extent possible. If a party's performance of its obligations is materially hindered as a result of a force majeure event, such party shall promptly notify the other party of its reasonable assessment of the nature and duration of the force majeure event and steps it is taking, and plans to take, to mitigate the effects of the force majeure event. The party shall use commercially reasonable efforts to continue performance to the extent possible during such event and resume full performance as soon as reasonably practicable.</p>

Term & Section	Language
General Terms, Force Majeure, Section 23	<p>Delete Section 23.2 in its entirety and replace with the following:</p> <p>Subject to the conditions set forth above, non-performance as a result of a force majeure event shall not be deemed a default. If such event continues for more than thirty (30) days, either a Customer or the Supplier may cancel unperformed Service Offerings and affected orders upon written notice. This section does not excuse any party's obligation to take reasonable steps to follow its normal disaster recovery procedures or, except as otherwise provided by law, the Customer's obligation to pay for Products and Service Offerings although, for the avoidance of doubt, the timeliness of payment could be affected by a force majeure event.</p>
General Terms, Section 23, Force Majeure	Delete Section 23.3 in its entirety.
General Terms, Security of Property and Personnel, Section 24	<p>Delete Section 24, Security of Property and Personnel, in its entirety and replace with the following:</p> <p>To the extent State's, Customer's or Supplier's employees are required to be on-site at another party's premises for the performance of services under this contract each party agrees to comply with the other party's safety and security policies while on the other party's premises to the extent that such policies do not violate any law, statute, ordinance, rule or regulation of any government or governmental body and provided that the other party provides such policies in writing in advance to the party (with adequate time to review said policies), that such policies do not require drug testing or background checks beyond those required (if any) under the Contract, and that such policies are not part of and do not modify or amend the Contract.</p>

Term & Section	Language
General Terms, Notices, Section 25	<p>Delete Section 25, Notices, in its entirety and replace with the following:</p> <p>All legal notices, approvals or requests allowed or required by the terms of any Contract Document shall be in writing, reference the Contract with specificity and deemed delivered upon receipt or upon refusal of the intended party to accept receipt of the notice. In addition to other notice requirements in the Contract and the designated Supplier contact provided in a successful Bid, notices shall be sent to the State at the physical address set forth below. Notice information may be updated in writing to the other party as necessary. Notwithstanding any other provision of the Contract, confidentiality, breach and termination-related notices shall not be delivered solely via e-mail.</p> <p><u>If sent to the State:</u></p> <p>State Purchasing Director 2401 North Lincoln Boulevard, Second Floor Oklahoma City, Oklahoma 73105</p> <p>And</p> <p>Chief Information Officer 3115 N. Lincoln Blvd Oklahoma City, OK 73105</p> <p><u>With a copy, which shall not constitute notice, to:</u></p> <p>Purchasing Division Deputy General Counsel 2401 North Lincoln Boulevard, Second Floor Oklahoma City, Oklahoma 73105</p> <p>Information Services Deputy General Counsel 3115 N. Lincoln Blvd Oklahoma City, OK 73105</p> <p><u>If sent to Supplier:</u></p> <p>Oracle America, Inc. 500 Oracle Parkway Redwood Shores, CA 94065 Attention: Legal Department 650.506.5600</p>

Term & Section	Language
General Terms, Miscellaneous, Section 26	<p>Delete Section 26.1, Choice of Law and Venue, and replace with the following:</p> <p>Any claim, dispute, or litigation relating to the Contract Documents, in the singular or in the aggregate, shall be governed by the laws of the State without regard to application of choice of law principles. Venue for any action, claim, dispute, or litigation relating in any way to the Contract Documents, shall be in Oklahoma County, Oklahoma.</p>
General Terms, Miscellaneous, Section 26	<p>Delete Section 26.4, Transition Services, in its entirety and replace with the following:</p> <p>If transition services are needed at the time of Contract expiration or termination, Supplier and Customer shall agree to commence discussions to provide additional services on a month-to-month basis, at a mutually agreed rate. Any agreement regarding such transition services shall be documented in an Addendum or other written agreement between Supplier and Customer.</p>
General Terms, Miscellaneous, Section 26	<p>Delete Section 26.7, Failure to Enforce, in its entirety and replace with the following:</p> <p>Failure by the Supplier, State or a Customer at any time to enforce a provision of, or exercise a right under, the Contract shall not be construed as a waiver of any such provision. Such failure to enforce or exercise shall not affect the validity of any Contract Document, or any part thereof, or the right of the Supplier, State or a Customer to enforce any provision of, or exercise any right under, the Contract at any time in accordance with its terms. Likewise, a waiver of a breach of any provision of a Contract Document shall not affect or waive a subsequent breach of the same provision or a breach of any other provision in the Contract.</p>

Term & Section	Language
General Terms, Miscellaneous, Section 26	<p>Delete Section 26.8, Mutual Responsibilities, in its entirety and replace with the following:</p> <ul style="list-style-type: none"> A. No party to the Contract grants the other the right to use any trademarks, trade names, other designations in any promotion or publication without the express written consent by the other party. B. The Contract is a non-exclusive contract and each party is free to enter into similar agreements with others. C. The Customer and Supplier each grant the other only the licenses and rights specified in the Contract and all other rights and interests are expressly reserved. D. The Customer and Supplier shall reasonably cooperate with each other and any Supplier to which the provision of a product and/or service under the Contract may be transitioned after termination or expiration of the Contract to the extent agreed pursuant to Section 26.4 above. E. Except as otherwise set forth herein, where approval, acceptance, consent, or similar action by a party is required under the Contract, such action shall not be unreasonably delayed or withheld.
General Terms, Miscellaneous, Section 26	<p>Delete Section 26.9, Invalid Term or Condition, in its entirety and replace with the following:</p> <p>To the extent any term or condition in the Contract is finally determined by a court of competent jurisdiction to conflict with a compulsory applicable Oklahoma or United States law or regulation, such Contract term or condition, to the extent in conflict, is void and unenforceable, and to the extent possible and upon mutual agreement by the parties, such term shall be replaced with a term consistent with the purpose and intent of the Contract. By executing any Contract Document which contains a conflicting term or condition, no representation or warranty is made regarding the enforceability of such term or condition. Likewise, any applicable Oklahoma or federal law or regulation which conflicts with the Contract or any non-conflicting applicable State or federal law or regulation is not waived.</p>
General Terms, Miscellaneous, Section 26	<p>Delete the final sentence of Section 26.10, Severability, and replace it with the following:</p> <p>If a court finds that any provision of this contract is invalid or unenforceable, but the parties mutually agree that by limiting such provision it would become valid and enforceable, then such provision shall be deemed to be written, construed, and enforced as so limited.</p>

Term & Section	Language
General Terms, Miscellaneous, Section 26	<p>Delete Section 26.12, Sovereign Immunity, in its entirety and replace with the following:</p> <p>The State does not waive (i) subject to the terms of the Contract, any other right or defense available to the State and (ii) the doctrine of sovereign immunity to the extent authorized by the Constitution and laws of the State of Oklahoma; provided, however, that the parties hereby agree that the doctrine of sovereign immunity does not apply to actions grounded in contract and therefore does not prohibit Supplier from pursuing claims arising under the Contract against the State and Customers.</p>
General Terms, Miscellaneous, Section 26	<p>Section 26.13, Survival, is deleted in its entirety and replaced with the following:</p> <p>As applicable, performance under all license, subscription, service agreements, statements of work, Ordering Documents transition plans and other similar Contract Documents entered into between the parties under the terms of the Contract shall survive Contract expiration. Additionally, rights and obligations under the Contract which by their nature should survive including, without limitation, certain payment obligations invoiced prior to expiration or termination; confidentiality obligations; security incident and data breach obligations and indemnification obligations, remain in effect after expiration or termination of the Contract.</p>
General Terms, Miscellaneous, Section 26	<p>Delete Section 26.14 in its entirety and replace with the following:</p> <p>It is expressly agreed that the terms of the Contract and any Supplier order shall supersede the terms in any purchase order, procurement internet portal or any other similar non-Supplier document that is not mutually executed by Supplier and Customer in connection with the order, and no terms included in any such purchase order, portal or other non-Supplier document shall apply to the Products and/or Service Offerings ordered. The applicable Contract Documents taken together as a whole constitute the entire agreement between the parties. No statement, promise, condition, understanding, inducement or representation, oral or written, expressed or implied, which is not contained in a Contract Document shall be binding or valid.</p>
General Terms, Miscellaneous, Section 26	<p>Delete Section 26.15 in its entirety and replace with the following:</p> <p>The Contract may be immediately terminated by written notice if it is determined that the Supplier, its employee, or its agent or other representative, acting at its direction, violated any federal, State or local law, rule or ordinance by offering or giving a gratuity to any State employee directly involved in the Contract. In addition, Suspension or Debarment of the Supplier may result from such a violation.</p>

Term & Section	Language
General Terms, Miscellaneous, Section 26	<p>Delete Section 26.16 in its entirety and replace with the following:</p> <p>Import/Export Controls</p> <p>Export laws and regulations of the United States and any other relevant local export laws and regulations apply to the Products. Both parties agree that such export laws govern the Customer's use of the Products (including technical data) and any Service Offerings deliverables provided under the Contract, and both parties agree to comply with all such export laws and regulations (including "deemed export" and "deemed re-export" regulations). Both parties agree that no data, information, Product and/or materials resulting from Service Offerings (or direct product thereof) will be exported, directly or indirectly, in violation of these laws, or will be used for any purpose prohibited by these laws including, without limitation, nuclear, chemical, or biological weapons proliferation, or development of missile technology. Customer shall include the following notice on packing lists, commercial invoices, shipping documents and other documents used in the transfer, export or re-export of the Products and any Service Offerings deliverables: 'These commodities, technology, software, or hardware (including any Integrated Software and Operating System(s)) were exported in accordance with U.S. Export Administration Regulations and applicable export laws. Diversion contrary to applicable export laws is prohibited.</p>
General Terms, Segmentation: New Section 26.17	<p>Insert a new Section 26.17 as follows:</p> <p>SEGMENTATION.</p> <p>The purchase of any Products and related Service Offerings or other Service Offerings are all separate offers and separate from any other order for any Products and related Service Offerings or other Service Offerings Customer may receive or have received from Supplier. Customer understands that Customer may purchase any Products and related Service Offerings or other Service Offerings independently of any other Products or Service Offerings. Customer's obligation to pay for (a) any Products and related Service Offerings is not contingent on performance of any other Service Offerings or delivery of any other Products or (b) other Service Offerings is not contingent on delivery of any Products or performance of any additional/other Service Offerings. Customer acknowledges that Customer have entered into the purchase without reliance on any financing or leasing arrangement with Supplier or its affiliate.</p>

Term & Section	Language
General Terms, Other, New Section 26.18	<p>Insert a new Section 26.18 as follows:</p> <p><u>OTHER.</u></p> <p>A Products and Service Offerings deliverables are not designed for or specifically intended for use in nuclear facilities or other hazardous applications. Customer agrees that it is Customer's responsibility to ensure safe use of Products and Service Offerings deliverables in such applications.</p> <p>B If requested by an authorized reseller on Customer's behalf, Customer agrees Supplier may provide a copy of the Contract to the authorized reseller to enable the processing of Customer's order with that authorized reseller.</p> <p>C Customer understands that Supplier's business partners, including any third party firms retained by Customer to provide consulting services, are independent of Supplier and are not Supplier's agents. Supplier is not liable for nor bound by any acts of any such business partner unless (i) the business partner is providing services as a Supplier subcontractor in furtherance of an order placed under the Master Agreement and (ii) only to the same extent as Supplier would be responsible for the performance of Supplier resources under that order.</p> <p>D For software (i) that is part of Programs and (ii) that Customer receive from Supplier in binary form and (iii) that is licensed under an open source license that gives Customer the right to receive the source code for that binary, Customer may obtain a copy of the applicable source code from https://oss.oracle.com/sources/ or http://www.oracle.com/goto/opensourcecode. If the source code for such software was not provided to Customer with the binary, Customer may also receive a copy of the source code on physical media by submitting a written request pursuant to the instructions in the "Written Offer for Source Code" section of the latter website.</p>
General Terms, Ownership, New Section 26.19	<p>Insert a new Section 26.19 as follows:</p> <p>Ownership.</p> <p>Supplier or its licensors retain all ownership and intellectual property rights to the Programs and anything developed or delivered under the Contract. Each Customer retains all ownership and intellectual property rights to its own proprietary information that it provides to Supplier under the Contract.</p>

Term & Section	Language
ATTACHMENT C – Oklahoma Statewide Contract Terms	
Oklahoma Statewide Terms, Statewide Contract Type, Section 1	<p>Section 1.1 is deleted in its entirety and replaced with the following:</p> <p>The Contract is a non-mandatory statewide contract for use by State agencies. Additionally, the Contract may be used by any governmental entity specified as a political subdivision of the State pursuant to the Governmental Tort Claims Act including any associated institution, instrumentality, board, commission, committee, department or other entity designated to act on behalf of the political subdivision; and tribal entities authorized to utilize contracts by the State via a multistate or multigovernmental contract.</p>
Oklahoma Statewide Terms, Statewide Contract Type, Section 1	<p>Section 1.2 is deleted in its entirety and replaced with the following:</p> <p>The Contract is a contract for indefinite delivery and quantity for the Acquisitions available under the Contract.</p>
Oklahoma Statewide Terms, Orders and Addendums, Section 2	<p>Section 2.1 is deleted in its entirety and replaced with the following:</p> <p>Unless mutually agreed in writing otherwise, orders shall be placed directly with the Supplier. Placement of orders shall be in accordance with Section 6.1 of Attachment B, General Terms. All orders placed under the Contract are subject to the Contract terms and any order dated prior to Contract expiration or termination shall be performed in accordance with its terms. Delivery to multiple destinations may be required.</p>
Oklahoma Statewide Terms, Orders and Addendums, Section 2	<p>Section 2.3 is deleted in its entirety and replaced with the following:</p> <p>Additional terms added to a Contract Document by a Customer shall be effective if the additional terms do not conflict with any term that takes precedence over such Contract Document pursuant to Section 2.2 of the General Terms (Order of Priority) and are acceptable to Supplier. However, an Addendum to the Contract shall be signed by the State Purchasing Director or designee. Regarding information technology and telecommunications contracts, pursuant to 62 O.S., §34.11.1, the Chief Information Officer acts as the Information Technology and Telecommunications Purchasing Director.</p>
Oklahoma Statewide Terms, Termination for Funding Insufficiency, Section 3	<p>Section 3 is deleted in its entirety, as termination rights are addressed in the General Terms</p>

Term & Section	Language
Oklahoma Statewide Terms, Termination for Cause, Section 4	Section 4 is deleted in its entirety, as termination rights are addressed in the General Terms.
Oklahoma Statewide Terms, Termination for Convenience, Section 5	Section 5 is deleted in its entirety, as termination rights are addressed in the General Terms.
Oklahoma Statewide Terms, Contract Management Fee and Usage Report, Section 6	<p>Section 6.1 is deleted in its entirety and replaced with the following:</p> <p>Pursuant to 74 O.S. § 85.33A, the State assesses a contract management fee on all transactions under a statewide contract. The payment of such fee will be calculated for all Acquisitions, net of returns and the Supplier has no right of setoff against such fee regardless of the payment status of any Customer or any aggregate accounts receivable percentage. Supplier acknowledges and agrees that all prices quoted under any statewide contract shall include the contract management fee and the contract management fee shall not be reflected as a separate line item in Supplier's billing. The State reserves the right to change this fee upward or downward upon sixty (60) calendar days' written notice to Supplier without further requirement for an Addendum.</p>
Oklahoma Statewide Terms, Contract Management Fee and Usage Report, Section 6	<p>Section 6.2 is deleted in its entirety and replaced with the following:</p> <p>While Supplier is the awardee of the Contract, Acquisitions that occur under the terms of the Contract are subject to a contract management fee in the amount of one percent (1%) of invoiced net sales under the Contract to be paid by Supplier. Supplier shall submit a Contract Usage Report ("Report") on a quarterly basis for the Contract using the template that has been provided by the State and such report shall include applicable information for each Acquisition. Reports shall include usage of the Contract by every Customer during the applicable quarter. A singular report provided late will not be considered a breach of the statewide contract; provided, however, repeated failure to submit accurate quarterly usage reports and submit timely payments may result in suspension or termination, in whole or in part, of the Contract.</p>

Term & Section	Language
Oklahoma Statewide Terms, Contract Management Fee and Usage Report, Section 6	<p>Section 6.3 is deleted in its entirety and replaced with the following: All Contract Usage Reports shall meet the following criteria:</p> <ul style="list-style-type: none"> i. Electronic submission in Microsoft Excel format to strategic.sourcing@omes.ok.gov; ii. Quarterly submission regardless of whether there were Acquisitions under the Contract during the applicable quarterly reporting period; iii. Submission no later than forty-five (45) days following the end of each calendar quarter; iv. Contract quarterly reporting periods shall be as follows: <ul style="list-style-type: none"> a. January 01 through March 31; b. April 01 through June 30; c. July 01 through September 30; and d. October 01 through December 31. v. Reports must include the following information: <ul style="list-style-type: none"> a. Procuring entity; b. Order date; c. Purchase Order number or note that the transaction was paid by Purchase Card; d. City in which products or services were received or specific office or subdivision title; e. Product manufacturer or type of service; f. Manufacturer item number, if applicable; g. Product description; h. General product category, if applicable; i. Quantity; j. Unit list price or MSRP, as applicable; k. Unit price charged to the purchasing entity; and l. Other Contract usage information requested by the State, provided such information (i) is required of all other similarly situated vendors (ii) is not more materially more burdensome for Supplier to provide than the types of information identified above and (iii) is not confidential or otherwise subject to restrictions on disclosure. The parties will work in good faith to address any concerns of Supplier regarding such additional information.

Term & Section	Language
ATTACHMENT D – State of Oklahoma Information Technology Terms	
Information Technology Terms, Introductory Paragraph	<p>The introductory paragraph is deleted in its entirety and replaced with the following:</p> <p>The parties further agree to the following terms (“Information Technology Terms”), as applicable, for any Acquisition of products or services with an information technology or telecommunication component. Pursuant to the Oklahoma Information Technology Consolidation and Coordination Act (the “Act”), OMES-Information Services (“OMES-IS”) is designated to purchase information technology and telecommunication products and services on behalf of the State. The Act directs OMES-IS to acquire necessary hardware, software and services and to authorize the use by other State agencies. OMES, as the holder and/or acquirer of information technology and telecommunication assets and contracts on behalf of the State, allows other State agencies to use the assets while remaining the holder and/or licensee. To the extent provided in Section 13.5 of Attachment B or the Ordering Document, OMES shall have the right to reassign the assets, at no additional cost, upon written notification to Supplier to another State Entity. OMES-IS is the data custodian for State agency data; however, ownership of such data is retained by the respective State agency. For the avoidance of doubt, the foregoing description of OMES-IS’s role pursuant to the Act is a general description only, and does not define or modify any grant of rights in intellectual property made in connection with any Acquisition under the Contract.</p>
Information Technology Terms, Termination of Maintenance and Support Services Section 1	Section 1.1 (COTS definition) is deleted in its entirety.
Information Technology Terms, Definitions Section 1	<p>Section 1.2 is deleted in its entirety and replaced with the following:</p> <p>1.2 Customer Data means all software, data (including Personal Information), text, images, audio, video, photographs, non-Supplier or third party applications, and other content and material, in any format, provided by Customer or any of Customer’s Users that is stored in, or run on or through, the Services (as defined in Schedule C). Services under the Contract, Supplier Software, other Supplier products and services, and Supplier intellectual property, and all derivative works thereof, do not fall within the meaning of the term “Customer Data”. Customer Data includes any Third Party Content (as defined in Schedule C) that is brought by Customer into the Cloud Services, by Customer use of the Services or any Supplier provided tools.</p>

Term & Section	Language
Information Technology Terms, Definitions Section 1	<p>Section 1.3 is deleted in its entirety and replaced with the following:</p> <p>1.3 Data Breach means a breach of security leading to the misappropriation or accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Customer Data transmitted, stored or otherwise processed on Supplier systems or the Services (as defined in Schedule C) environment that compromises the security, confidentiality or integrity of Customer Data.</p>
Information Technology Terms, Definitions Section 1	<p>Section 1.4 shall be revised as follows:</p> <p>1.4 Host includes the terms Hosted or Hosting and shall mean storage on servers and other components that allow the application to be made accessible via the internet.</p>
Information Technology Terms, Definitions Section 1	<p>Section 1.5 (Intellectual Property Rights) is deleted in its entirety.</p>
Information Technology Terms, Definitions Section 1	<p>Section 1.6 (Moral Rights definition) is deleted in its entirety.</p>
Information Technology Terms, Definitions Section 1	<p>Section 1.8 is deleted in its entirety and replaced with the following:</p> <p>1.8 Personal Data means “Personal Information”, as such term is defined in the Data Processing Agreement for Oracle Services.</p>
Information Technology Terms, Definitions Section 1	<p>Section 1.9 is deleted in its entirety and replaced with the following:</p> <p>1.9 Security Incident shall mean a confirmed Information Breach, as defined in the Oracle Data Processing Agreement.</p>
Information Technology Terms, Definitions Section 1	<p>Section 1.11 (Supplier Intellectual Property) is deleted in its entirety.</p>

Term & Section	Language
Information Technology Terms, Definitions Section 1	Section 1.13 (Work Product) is deleted in its entirety.
Information Technology Terms, Termination of Maintenance and Support Services Section 2	<p>Section 2 is deleted in its entirety and replaced with the following:</p> <p>Termination of maintenance or technical support for Supplier software or hardware products, and any repricing of technical support fees as a result of such termination, shall be pursuant to then-current Supplier technical support policies. For avoidance of doubt, the foregoing does not restrict a Customer's right to terminate an Ordering Document for maintenance or technical support pursuant to Sections 17 or 18 of Attachment B, General Terms.</p> <p>2.1 Reserved</p> <p>2.2 If Customer chooses to renew maintenance or support after maintenance has lapsed, Customer may choose to pay the additional fee, if any, associated with renewing a license after such maintenance or support has lapsed, or to purchase a new license. Any amount paid to Supplier in the form of prepaid fees that are unused when services under the Ordering Document are terminated shall be refunded to Customer.</p> <p>2.3 Notwithstanding the foregoing, a Customer shall provide Supplier a thirty (30)-day notice of its intent to terminate maintenance or technical support for Supplier software or hardware products pursuant to this provision. Customer must pay (in accordance with the payment terms detailed in Section 7 (Invoices and Payment) of Attachment B) all amounts that have accrued prior to the effective date termination of the applicable order(s) for such maintenance or technical support for Supplier software or hardware products, as well as all sums remaining unpaid for services rendered and accepted.</p>

Term & Section	Language
Information Technology Terms, Compliance and Electronic and Information Technology Accessibility Section 3	<p>Section 3 is deleted in its entirety and replaced with the following:</p> <p>Compliance and Electronic and Information Technology Accessibility</p> <p>The extent to which a Supplier product is, prior to any customizations, capable of providing comparable access to individuals with disabilities consistent with the applicable provisions of the Architectural and Transportation Barriers Compliance Board standards set out in 36 CFR Part 1194 (known as 'Section 508'), effective as of June, 2001, or the Revised version in Appendix A (known as 'Revised Section 508') effective as of January, 2018 and the Web Content Accessibility Guidelines (WCAG) version 2.0 level AA, or the Web Content Accessibility Guidelines (WCAG) version 2.1 level AA as indicated by the dependencies, comments and exceptions (some of which may be significant, if any) noted on the applicable Accessibility Conformance Report (ACR) based on the Voluntary Product Accessibility Templates (VPAT) available at www.oracle.com/accessibility for each product, when they are used in accordance with Supplier's associated documents and other written information, and provided that any assistive technologies and any other products used with them properly interoperate with them. In the event that no ACR is available for a particular Supplier product, please contact the Supplier Accessibility Program Office at accessible_ww@oracle.com. In some cases, the outcome may be that a product is still being evaluated for accessibility, may be scheduled to meet accessibility standards in a future release, or may not be scheduled to meet accessibility standards at all. Supplier Support customers with disabilities may use the online My Oracle Support or call Supplier Support at 1.800.223.1711. Hearing-impaired customers in the U.S. who wish to speak to a Supplier Support representative may use a telecommunications relay service (TRS). Information about the TRS is available at https://www.fcc.gov/file/15195/download (PDF), and a list of telephone numbers is available at http://www.fcc.gov/cgb/dro/trsphonebk.html. International hearing-impaired customers should use the TRS at +1.605.224.1837. Supplier Support will respond to product accessibility issues according to the current Technical Support Policies. No other terms, conditions, statements or any other such representations regarding or related to accessibility shall apply to the Supplier products provided under the Contract. Supplier cannot make any commitments about future product directions, including plans to address accessibility or the availability of ACRs. Product direction remains at the sole discretion of Supplier.</p>

Term & Section	Language
Information Technology Terms, Media Ownership (Disk Drive and/or Memory Chip Ownership) Section 4	Section 4.1 is deleted in its entirety.
Information Technology Terms, Media Ownership (Disk Drive and/or Memory Chip Ownership) Section 4	Section 4.2 is deleted in its entirety.
Information Technology Terms, Offshore Services, Section 5	<p>Section 5 (Offshore Services) is deleted in its entirety and replaced with the following:</p> <p>Unless an Ordering Document indicates that the data center region applicable to the Cloud Services ordered is customer-selected, the data center region applicable to a Customer's order of Cloud Services shall be as set out in the Ordering Document. Supplier shall not change the applicable data center region without Customer's written authorization during the services period covered by the Ordering Document. Where an order specifies that the data center region is Customer-selected, Customer may have the ability to change the applicable data center region. Supplier and Customer may agree to additional provisions regarding data center region in an ordering document.</p> <p>If a Customer orders Oracle Cloud Platform as a Service and/or Infrastructure as a Service Cloud Services in the Oracle U.S. Government Data Center Region (as indicated in the applicable ordering document), then, for purposes of that order, 1) Hosted Customer Data will be stored in the United States, and 2) personnel that support the Customer Hosting Data on Oracle systems processing/storing Hosted Customer Data will be U.S. Persons.</p>

Term & Section	Language
Information Technology Terms, Compliance with Technology Policies, Section 6	<p>Section 6 is deleted in its entirety and replaced with the following:</p> <p>For Cloud Services, see Data Processing Agreement, Supplier Cloud Hosting & Delivery Policies, and Service Descriptions, and Supplier Corporate Security Practices and the Contract.</p> <p>Supplier acknowledges that the State is subject to the applicable State IT Standards, policies, procedures and architectures as set forth at https://oklahoma.gov/omes/services/information-services.html or as otherwise provided by the State. For the avoidance of doubt, the responsibility for compliance with the aforementioned State IT Standards, policies, procedures and architectures is solely the responsibility of the State except as otherwise provided in an ordering document.</p>
Information Technology Terms, Extension Right, Section 8	Section 8 (Extension Right) is deleted in its entirety.
Information Technology Terms, Source Code Escrow, Section 9	Section 9 is deleted in its entirety. The Contract does not contemplate the development of any “customized computer software” within the meaning of 62 O.S. § 34.31, and any such development or purchase must be pursuant to a separate written agreement.
Information Technology Terms, Ownership Rights, Section 11	<p>Section 11 is deleted in its entirety and replaced with the following:</p> <p>Supplier or its licensors retain all ownership and intellectual property rights to the Programs, Service Offerings, and anything developed or delivered under the Contract. Each Customer retains all ownership and intellectual property rights to its own proprietary information that it provides to Supplier under the Contract.</p> <p>See applicable provisions in the Schedules.</p>
Information Technology Terms, Intellectual Property Ownership, Section 12	<p>Section 12 is retitled “Rights Granted” and is deleted in its entirety and replaced with the following:</p> <p>See applicable provisions in the General Terms and the Schedules.</p>
Information Technology Terms, Hosting Services, Section 13	<p>The heading in Section 13 (Hosting Services) is changed as follows:</p> <p>Hosting Services for Cloud Services</p>

Term & Section	Language
Information Technology Terms, Hosting Services, Section 13	<p>Section 13.2 is deleted in its entirety and replaced with the following:</p> <p>If the Hosting of Customer Data under the Contract contributes to or directly causes a Data Breach or Security Incident, Supplier shall be responsible for the obligations set forth in Appendix 1.</p>
Information Technology Terms, Change Management, Section 14	<p>Section 14 is retitled “Change Management for Cloud Services” and is deleted in its entirety and replaced with the following:</p> <p>Notification shall be in accordance with the Supplier Hosting and Delivery Policies and the Contract.</p>
Information Technology Terms, Service Level Deficiency, Section 15	<p>Section 15 is retitled “Service Level Deficiency for Cloud Services” and is deleted in its entirety and replaced with the following:</p> <p>In addition to other terms of the Contract, in instances of the Supplier’s repeated failure to meet service level agreement metrics, service credits shall be provided by Supplier in accordance with the Supplier Service Level Agreement section of the Hosting and Delivery Policies and the Contract.</p>
Information Technology Terms, Notices, Section 16	<p>Section 16 is deleted in its entirety and replaced with the following:</p> <p>Notification of changes in Cloud Services shall be in accordance with the Supplier Hosting and Delivery Policies and the Contract.</p>
Information Technology Terms, Appendix 1, Introduction	<p>The introduction of Appendix 1 is deleted in its entirety and replaced with the following:</p> <p>For Cloud Services only:</p> <p>The parties agree to the following provisions in connection with any Customer Data accessed, processed or stored by or on behalf of the Supplier and the obligations set forth below shall continue as long as the Supplier has an obligation under the Contract, which shall be in accordance with Service Specifications, as defined in Attachment E-1 (Schedule C) of the Contract, which include but are not limited to Data Processing Agreement and Hosting and Delivery Policies.</p>
Information Technology Terms, Appendix 1, Section A, Customer Data	<p>Section A is retitled “Customer Data for Cloud Services” and is deleted in its entirety and replaced with the following:</p> <p>Customer will be responsible for the accuracy and completeness of all Customer Data provided to Supplier by Customer.</p>

Term & Section	Language
Information Technology Terms, Appendix 1, Section B, Data Security	<p>Section B.1 is deleted in its entirety and replaced with the following:</p> <p>See Section 1 (ORACLE CLOUD SECURITY POLICY) of Hosting and Delivery Policies, including but not limited to section 1.5 (User Encryption for External Connections). With respect to Cloud Services acquired under this Contract which reside on Supplier-managed computing infrastructures: (a) Supplier maintains protections on its computer systems to prevent them from introducing malware (e.g., computer viruses and worms) through administrative access points to those Services, (b) Supplier requires that anti-malware scanning be performed before Supplier software components are deployed by Supplier into those Services, and (c) except for any of those Services that are installed at Customer data center(s), Supplier uses intrusion detection techniques to detect suspicious and malicious traffic on the cloud networks on which those Services are deployed. The data center region for the Cloud Services acquired under the Contract shall be as specified in the applicable ordering document.</p> <p>See Section 4 (Privacy Inquiries and Requests from Individuals) of the Data Processing Agreement.</p>
Information Technology Terms, Appendix 1, Section B, Data Security	<p>Section B.2 is deleted in its entirety and replaced with the following:</p> <p>See the Security and Confidentiality and Incident Management and Breach Notification section of the Data Processing Agreement.</p>
Information Technology Terms, Appendix 1, Section B, Data Security	<p>Section B.3 is deleted in its entirety and replaced with the following:</p> <p>Data Security for Cloud Services.</p> <p>See Section 1 (ORACLE CLOUD SECURITY POLICY) of Hosting and Delivery Policies, including but not limited to section 1.5 (User Encryption for External Connections). With respect to Cloud Services acquired under this Contract which reside on Supplier-managed computing infrastructures: (a) Supplier maintains protections on its computer systems to prevent them from introducing malware (e.g., computer viruses and worms) through administrative access points to those Services, (b) Supplier requires that anti-malware scanning be performed before Supplier software components are deployed by Supplier into those Services, and (c) except for any of those Services that are installed at Customer data center(s), Supplier uses intrusion detection techniques to detect suspicious and malicious traffic on the cloud networks on which those Services are deployed. The data center region for the Cloud Services acquired under the Contract shall be as specified in the applicable ordering document.</p>

Term & Section	Language
Information Technology Terms, Appendix 1, Section B, Data Security	Section B.4 shall be deleted in its entirety.
Information Technology Terms, Appendix 1, Section B, Data Security	Section B.5 is deleted in its entirety and replaced with the following: Supplier shall allow the Customer to audit in conformance to the Contract terms as provided by the General Terms, Attachment B to the Contract and the terms of the applicable Service Specifications (as defined in Schedule C).
Information Technology Terms, Appendix 1, Section B, Data Security	Section B.6 shall be deleted in its entirety.
Information Technology Terms, Appendix 1, Section C, Security Assessment	<p>Section C is deleted in its entirety and replaced with the following:</p> <p>See Section 1 (Supplier Cloud Security Policy) of the Supplier Cloud Hosting & Delivery Policies. The State requires any entity or third-party supplier accessing, processing, storing or transmitting Oklahoma Customer Data to submit to a State Certification and Accreditation Review process to assess initial security risk. Supplier submitted the requested documentation for review and was determined to have met the State's minimum security standards at time the Contract was executed. Supplier acknowledges that the State may request updated or additional documentation as part of its annual supplier review process, and that the outcome of the State's annual supplier review and assessment may be used as a basis for determinations regarding extension of the Contract or termination of the Contract for convenience in accordance with General Terms, Attachment B, Section 19.1.</p> <p>See also Oracle Affiliates and Third Party Subprocessors of the Data Processing Agreement.</p>

Term & Section	Language
Information Technology Terms, Appendix 1, Section D, Security Incident or Data Breach Notification	Section D is deleted in its entirety and replaced with the following: See Incident Management and Breach Notification section of the Data Processing Agreement.
Information Technology Terms, Appendix 1, Section E, Breach Responsibilities	Section E is deleted in its entirety and replaced with the following: See Incident Management and Breach Notification section of the Data Processing Agreement.
Information Technology Terms, Appendix 1, Section F, Notices	Section F is deleted in its entirety and replaced with the following: See section 16 (Notices) of Attachment D.
Information Technology Terms, Appendix 1, Section G, Supplier Representations and Warranties	Section G is deleted in its entirety and replaced with the following: See applicable provisions in Attachments E-1 (Schedule C) and Attachment E-2 (Schedule P).
Information Technology Terms, Appendix 1, Section H, Indemnity	Section H is deleted in its entirety and replaced with the following: See section 16 (Indemnification) of Attachment B (STATE OF OKLAHOMA GENERAL TERMS) to the Contract.

Term & Section	Language
Information Technology Terms, Appendix 1, Section I Termination, Expiration and Suspension of Service	Section I is deleted in its entirety and replaced with the following: See Ordering Document, Attachment E-1 (Schedule C) of the Contract and Hosting and Delivery Policies.
Information Technology Terms, Append. 2	Appendix 2 to State of Oklahoma Information Technology Terms shall be deleted in its entirety.

STATE OF OKLAHOMA CONTRACT WITH ORACLE AMERICA, INC.

RESULTING FROM SOLICITATION NO. 0900000556 (SW1041)

**Template for Contract Modifications for Quotes, Statements of
Work, or other Ordering Documents**

The parties agree to use this template as required by General Terms, Section 2.2 (Contract Effectiveness and Order of Precedence) as the process to formally approve any terms, conditions or clauses that are to supersede the Prevailing Terms itemized in the General Terms, Section 2.2 (Contract Effectiveness and Order of Precedence) for purposes of the applicable quote, statement of work or other ordering document.

Contract Modifications for Quote, Statement of Work, or other Ordering Document

Solely for purposes of this ordering document, the Prevailing Terms of the Contract are hereby amended as set forth below. This amendment is considered an Addendum.

Contract Section	Exception/Conflicting Term

STATE OF OKLAHOMA
by and through the
OFFICE OF MANAGEMENT AND
ENTERPRISE SERVICES

ORACLE AMERICA, INC.

By: _____

By: _____

Name: _____

Name: _____

Title: _____

Title: _____

Date: _____

Date: _____

The [INSERT AGENCY NAME] is additionally executing this document to memorialize its involvement in negotiation of and its agreement with the terms of this document.

By: _____

Name: _____

Title: _____

Date: _____



This addendum is added to and is to be considered part of the subject contract.

Statewide Contract #: SW1041P

PeopleSoft Contract ID: 7150

Contract Title: Software Value Added Reseller

Contract Issuance Date: 10/07/2023

Contract Supplier: Presidio

Addendum # 1

Addendum Date: 03/07/2024

OMES Point of Contact:

Contracting Officer: Marc Brown

Phone Number: 405-521-6669

E-mail address: Marc.brown@omes.ok.gov

Addendum Information: _____

Addendum #1 is issued for term renewal for Presidio per the original T&C's.

Contract Period: 03/14/2024 – 03/13/2025

Agreement Period: 03/14/2024 – 03/13/2028

SW1041 Software**Exhibit 1**

Software Publishers		
Description	Maximum Cost + % Markup	% off List Price
Adobe Systems, Inc	2.10%	n/a
AirMagnet, Inc	2.10%	n/a
AirWatch	2.10%	n/a
Akkadian Labs	2.10%	n/a
AlienVault	2.10%	n/a
Amazon Web Services	n/a	1%
American Well	2.10%	n/a
Anue Systems, Inc.	2.10%	n/a
APC by Schneider Electric IT Corp	2.10%	n/a
APPYDYNAMICS INC	2.10%	n/a
Apple Computer	2.10%	n/a
Arista Networks, Inc.	2.10%	n/a
Avigilon	2.10%	n/a
Barracuda Networks, Inc	2.10%	n/a
BEYOND TRUST, Inc	2.10%	n/a
BitTitan	2.10%	n/a
Black Box Corporation	2.10%	n/a
BlueCat Networks, Inc.	2.10%	n/a
BMC Software, Incl	2.10%	n/a
BRIDGE COMMUNICATIONS, LLC	2.10%	n/a
Calabrio	2.10%	n/a
Calero Software, LLC	2.10%	n/a
Carbon Black	2.10%	n/a
Carbonite	2.10%	n/a
Centrify Corp.	2.10%	n/a
Check Point Software Technologies Ltd.	2.10%	n/a
Citrix Systems Inc	2.10%	n/a
Cloudera	2.10%	n/a
CloudFlare	2.10%	n/a
Cloudgenix	2.10%	n/a
CloudHealth Technologies	2.10%	n/a
Cohesity	2.10%	n/a
CommScope, Inc.	2.10%	n/a
CommVault Systems, Inc.	2.10%	n/a
CompuWare	2.10%	n/a
Cribl	2.10%	n/a
CrowdStrike	2.10%	n/a
CyberArk	2.10%	n/a
Cybereason	2.10%	n/a
CyberX	2.10%	n/a

Cylance	2.10%	n/a
Datrium	2.10%	n/a
Dell	2.10%	n/a
DigiCert	2.10%	n/a
Docker	2.10%	n/a
Dynatrace	2.10%	n/a
Eaton Corporation	2.10%	n/a
Ekahau	2.10%	n/a
EMC Corporation	2.10%	n/a
Enghouse Interactive	2.10%	n/a
Entrust	2.10%	n/a
Equinix	2.10%	n/a
Exabeam	2.10%	n/a
Exagrid	2.10%	n/a
Extrahop	2.10%	n/a
F5 Networks, Inc.	2.10%	n/a
FatPipe Networks, Inc	2.10%	n/a
Firemon	2.10%	n/a
Fluidmesh Networks	2.10%	n/a
Fluke Networks	2.10%	n/a
Forcepoint LLC	2.10%	n/a
ForeScout Technologies	2.10%	n/a
Fortinet, Inc	2.10%	n/a
Gigamon	2.10%	n/a
Google, Inc	n/a	1%
Hewlett-Packard	2.10%	n/a
IBM Corporation	2.10%	n/a
Imperva Inc.	2.10%	n/a
Infoblox Inc	2.10%	n/a
Intel Corporation	2.10%	n/a
Intelisys	2.10%	n/a
IPCELERATE	2.10%	n/a
Ipswitch, Inc	2.10%	n/a
ISI Telemanagement Solutions, Inc.	2.10%	n/a
Ivanti	2.10%	n/a
Ixia	2.10%	n/a
Jamf	2.10%	n/a
Keysight Technologies	2.10%	n/a
LANdesk	2.10%	n/a
Lantronix, Inc	2.10%	n/a
Liebert Corporation	2.10%	n/a
LiveAction Software	2.10%	n/a
LogicMonitor	2.10%	n/a
LogRhythm	2.10%	n/a

Malwarebytes	2.10%	n/a
McAfee, Inc.	2.10%	n/a
Microsoft Azure	n/a	1%
Mimecast	2.10%	n/a
Morpheus Data, LLC	2.10%	n/a
Nasuni	2.10%	n/a
NetBrain Technologies	2.10%	n/a
Netmotion Software	2.10%	n/a
NetScout Systems, Inc	2.10%	n/a
Netskope, Inc	2.10%	n/a
Nexsan Technologies	2.10%	n/a
NICE Systems, Inc.	2.10%	n/a
Novell	2.10%	n/a
Nuance Communications, Inc.	2.10%	n/a
Nutanix	2.10%	n/a
NVIDIA Corporation	2.10%	n/a
OpenText (not Xmedius, Carbonite, or Webr	2.10%	n/a
Oracle Corporation	2.10%	n/a
Proofpoint	2.10%	n/a
Pure Storage, Inc.	2.10%	n/a
Q1 Labs, Inc.	2.10%	n/a
Qualys Inc	2.10%	n/a
Qumulo	2.10%	n/a
Rapid7	2.10%	n/a
Red Hat	2.10%	n/a
Red Sky Technologies -Everbridge	2.10%	n/a
Riverbed Technology, Inc.	2.10%	n/a
RoomReady	2.10%	n/a
RSA Security	2.10%	n/a
Rubrik	2.10%	n/a
SailPoint	2.10%	n/a
SentinelOne	2.10%	n/a
Singlewire Software, LLC	2.10%	n/a
Snowflake	2.10%	n/a
SolarWinds, Inc	2.10%	n/a
Sophos Plc	2.10%	n/a
Spectra Logic Corporation	2.10%	n/a
Spectracom Corp.	2.10%	n/a
Spectrum Industries	2.10%	n/a
SpinSci	2.10%	n/a
Splunk, Inc.	2.10%	n/a
STEALTHbits Technologies	2.10%	n/a
Sumo Logic	2.10%	n/a
Sungard	2.10%	n/a

[illegible]



State of Oklahoma

Office of Management and Enterprise Services

STATE OF OKLAHOMA CONTRACT WITH PRESIDIO NETWORKED SOLUTIONS, LLC

This State of Oklahoma Contract No. 1014 ("Contract") is entered into between the State of Oklahoma by and through the Office of Management and Enterprise Services and **Presidio Networked Solutions, LLC** ("Presidio") ("Supplier") and is effective as of the effective date set forth on a properly issued purchase order or, if no effective date is listed, the date of last signature to this Contract. The initial term of the Contract shall be for one (1) year, with four (4) one-year options to renew.

Purpose

The State is awarding this Contract to Supplier to engineer, design, furnish, install, test, and maintain solutions that will interface with the existing state infrastructure and provide complete telecommunication network and/or services for all State Agencies and other Interlocal entities located in their area of geographic responsibility, as more particularly described in certain Contract Documents. Supplier submitted a proposal which did not contain exceptions to the Solicitation. This Contract memorializes the agreement of the parties with respect to terms of the Contract that is being awarded to Supplier.

Now, therefore, in consideration of the foregoing and the mutual promises set forth herein, the receipt and sufficiency of which are hereby acknowledged the parties agree as follows:

1. The parties agree that Supplier has not yet begun performance of work under this Contract. Upon full execution of this Contract, Supplier may begin work. Issuance of a purchase order is required prior to payment to a Supplier.
2. The following Contract Documents are attached hereto and incorporated herein:
 - 2.1. Solicitation No. 0900000550, Attachment A;
 - 2.2. General Terms, Attachment B;
 - 2.3. Statewide Terms, Attachment C;
 - 2.4. Information Technology terms, Attachment D;
 - 2.5. Sample Statement of Work, Attached E;
 - 2.6. Supplier's Pricing Terms, Attachment E-2; and
 - 2.7. Negotiated Exceptions to Contract, Attachment F.

3. The parties additionally agree:


- 3.1. Information deemed confidential by the State pursuant to applicable law, rule, regulation or policy, the parties agree Contract terms and information are not confidential and are disclosable without further approval of or notice to Supplier.


Attachments referenced in this section are attached hereto and incorporated herein.

4. Any reference to a Contract Document refers to such Contract Document as it may have been amended. If and to the extent any provision is in multiple documents and addresses the same or substantially the same subject matter but does not create an actual conflict, the more recent provision is deemed to supersede earlier versions.

STATE OF OKLAHOMA
by and through the
OFFICE OF MANAGEMENT AND
ENTERPRISE SERVICES

PRESIDIO NETWORKED SOLUTIONS,
LLC

By: 
Joe McIntosh (Sep 7, 2023 12:55 CDT)
Name: Joe McIntosh
Title: Chief Information Officer
Date: Sep 7, 2023

By: 
Name: Jackie Arnett
Title: Contracts Director
Date: Sep 6, 2023

ATTACHMENT A
SOLICITATION NO. 0900000550

This Solicitation is a Contract Document and is a request for proposal in connection with the Contract awarded by the Office of Management and Enterprise Services as more particularly described below. Any defined term used herein but not defined herein shall have the meaning ascribed in the General Terms or other Contract Document.

PURPOSE

The Contract is awarded as a statewide contract on behalf of the Office of Management and Enterprise Services (OMES) for Telecommunication Products and Services for Oklahoma State Agencies and Interlocal Entities.

The Supplier(s) shall be required to engineer, design, furnish, install, test, and maintain solutions that will interface with the existing state infrastructure and provide complete telecommunication network and/or services for all State Agencies and other Interlocal entities located in their area of geographic responsibility.

1. Contract Term and Renewal Options

The initial Contract term, which begins on the effective date of the Contract, is one year and there are [4] one-year options to renew the Contract.

2. Scope of Work

Certain Contract requirements and terms are set forth below as Exhibit 1.

Certain Contract requirements and terms are set forth below as Exhibit 2.

Certain Contract requirements and terms are set forth below as Exhibit 3.

Certain Contract requirements and terms are set forth below as Exhibit 4.

Certain Contract requirements and terms are set as Exhibit 5 – Pricing.

Exhibit 1

The State of Oklahoma requires the highest level of customer service before, during and after the provisioning of services. This optimized service for existing and new telecommunications services will be for strategic alliances with the capabilities to meet Oklahoma's ever growing and changing requirements. Supplier(s) will provide at minimum one of the below services within the below listed KEN's Regions.

1. Carrier Services
2. Equipment-Telecommunications Equipment
3. Telecommunication Services, Ongoing Support and Training
4. Leasing Option

Exhibit 2 – IRS Publication 1075

Safeguarding Contract Language for General Services

I. PERFORMANCE

In performance of this contract, the Contractor agrees to comply with and assume responsibility for compliance by his or her employees with the following requirements:

- (1) All work will be performed under the supervision of the contractor or the contractor's responsible employees.
- (2) The contractor and the contractor's employees with access to or who use FTI must meet the background check requirements defined in IRS Publication 1075.
- (3) Any Federal tax returns or return information (hereafter referred to as returns or return information) made available shall be used only for the purpose of carrying out the provisions of this contract. Information contained in such material shall be treated as confidential and shall not be divulged or made known in any manner to any person except as may be necessary in the performance of this contract. Inspection by or disclosure to anyone other than an officer or employee of the contractor is prohibited.
- (4) All returns and return information will be accounted for upon receipt and properly stored before, during and after processing. In addition, all related output and products will be given the same level of protection as required for the source material.
- (5) No work involving returns and return information furnished under this contract will be subcontracted without prior written approval of the IRS.
- (6) The contractor will maintain a list of employees authorized access. Such list will be provided to the agency and, upon request, to the IRS reviewing office.
- (7) The agency will have the right to void the contract if the contractor fails to provide the safeguards described above.

(Include any additional safeguards that may be appropriate.)

II. CRIMINAL/CIVIL SANCTIONS

Each officer or employee of any person to whom returns or return information is or may be disclosed shall be notified in writing by such person that returns or return information disclosed to such officer or employee can be used only for a purpose and to the extent authorized herein, and that further disclosure of any such returns or return information for a purpose or to an extent unauthorized herein constitutes a felony punishable upon conviction by a fine of as much as \$5,000 or imprisonment for as long as five years, or both, together with the costs of prosecution. Such person shall also notify each such officer and employee that any such unauthorized future

disclosure of returns or return information may also result in an award of civil damages against the officer or employee in an amount not less than \$1,000 with respect to each instance of unauthorized disclosure. These penalties are prescribed by IRCs 7213 and 7431 and set forth at 26 CFR 301.6103(n)-1.

(1) Each officer or employee of any person to whom returns or return information is or may be disclosed shall be notified in writing by such person that any return or return information made available in any format shall be used only for the purpose of carrying out the provisions of this contract. Information contained in such material shall be treated as confidential and shall not be divulged or made known in any manner to any person except as may be necessary in the performance of this contract. Inspection by or disclosure to anyone without an official need-to-know constitutes a criminal misdemeanor punishable upon conviction by a fine of as much as \$1,000.00 or imprisonment for as long as 1 year, or both, together with the costs of prosecution. Such person shall also notify each such officer and employee that any such unauthorized inspection or disclosure of returns or return information may also result in an award of civil damages against the officer or employee [United States for Federal employees] in an amount equal to the sum of the greater of \$1,000.00 for each act of unauthorized inspection or disclosure with respect to which such defendant is found liable or the sum of the actual damages sustained by the plaintiff as a result of such unauthorized inspection or disclosure plus in the case of a willful inspection or disclosure which is the result of gross negligence, punitive damages, plus the costs of the action. The penalties are prescribed by IRCs 7213A and 7431 and set forth at 26 CFR 301.6103(n)-1.

(2) Additionally, it is incumbent upon the contractor to inform its officers and employees of the penalties for improper disclosure imposed by the Privacy Act of 1974, 5 U.S.C. 552a. Specifically, 5 U.S.C. 552a(i)(1), which is made applicable to contractors by 5 U.S.C. 552a(m)(1), provides that any officer or employee of a contractor, who by virtue of his/her employment or official position, has possession of or access to agency records which contain individually identifiable information, the disclosure of which is prohibited by the Privacy Act or regulations established thereunder, and who knowing that disclosure of the specific material is so prohibited, willfully discloses the material in any manner to any person or agency not entitled to receive it, shall be guilty of a misdemeanor and fined not more than \$5,000.

(3) Granting a contractor access to FTI must be preceded by certifying that each individual understands the agency's security policy and procedures for safeguarding IRS information. Contractors must maintain their authorization to access FTI through annual recertification. The initial certification and recertification must be documented and placed in the agency's files for review. As part of the certification and at least annually afterwards, contractors must be advised of the provisions of IRCs [7431](#), [7213](#) and [7213A](#) in [IRS Publication 1075](#). The training provided before the initial certification and annually thereafter must also cover the incident response policy and procedure for reporting unauthorized disclosures and data breaches. (See Section 1.8, Reporting Improper Inspections or Disclosures in [IRS Publication 1045](#).) For both the initial certification and the annual certification, the contractor must sign, either with ink or electronic signature, a confidentiality statement certifying their understanding of the security requirements.

III. DATA INCIDENT RESPONSE

The contractor will:

- (1) Cooperate with and exchange information with agency officials, as determined necessary by the agency, in order to effectively report and manage a suspected or confirmed breach.
- (2) Properly encrypt FTI in accordance with Publication 1075 and other applicable policies and to comply with any agency-specific policies for protecting FTI.
- (3) Complete regular training on how to identify and report a breach;
- (4) Report a suspected or confirmed breach in any medium or form, including paper, oral and electronic, as soon as possible and without unreasonable delay, consistent with the agency's incident management policy;
- (5) Maintain capabilities to determine what FTI was or could have been accessed and by whom, construct a timeline of user activity, determine methods and techniques used to access FTI and identify the initial attack vector; Allow for an inspection, investigation, forensic analysis and any other action necessary to ensure compliance with Publication 1075, the agency's breach response plan and to assist with responding to a breach; Identify roles and responsibilities, in accordance with Publication 1075 and the agency's breach response plan; and, explain that a report of a breach shall not, by itself, be interpreted as evidence that the contractor or its subcontractor failed to provide adequate safeguards for FTI.

IV. INSPECTION

The IRS and the Agency, with 24-hour notice, shall have the right to send its inspectors into the offices and plants of the contractor to inspect facilities and operations performing any work with FTI under this contract for compliance with requirements defined in IRS Publication 1075. The IRS' right of inspection shall include the use of manual and/or automated scanning tools to perform compliance and vulnerability assessments of information technology (IT) assets that access, store, process or transmit FTI. On the basis of such inspection, corrective actions may be required in cases where the contractor is found to be noncompliant with contract safeguards.

Exhibit 3 – IRS Publication 1075

Safeguarding Contract Language for Technology Services

I. PERFORMANCE

In performance of this contract, the contractor agrees to comply with and assume responsibility for compliance by his or her employees with the following requirements:

- (1) All work will be done under the supervision of the contractor or the contractor's employees.
- (2) The contractor and the contractor's employees with access to or who use FTI must meet the background check requirements defined in IRS Publication 1075.
- (3) Any return or return information made available in any format shall be used only for the purpose of carrying out the provisions of this contract. Information contained in such material will be treated as confidential and will not be divulged or made known in any manner to any person except as may be necessary in the performance of this contract. Disclosure to anyone other than an officer or employee of the contractor will be prohibited.
- (4) All returns and return information will be accounted for upon receipt and properly stored before, during and after processing. In addition, all related output will be given the same level of protection as required for the source material.
- (5) The contractor certifies that the data processed during the performance of this contract will be completely purged from all data storage components of his or her computer facility, and no output will be retained by the contractor at the time the work is completed. If immediate purging of all data storage components is not possible, the contractor certifies that any IRS data remaining in any storage component will be safeguarded to prevent unauthorized disclosures.
- (6) Any spoilage or any intermediate hard copy printout that may result during the processing of IRS data will be given to the agency or his or her designee. When this is not possible, the contractor will be responsible for the destruction of the spoilage or any intermediate hard copy printouts, and will provide the agency or his or her designee with a statement containing the date of destruction, description of material destroyed, and the method used.
- (7) All computer systems receiving, processing, storing, accessing, protecting and/or transmitting FTI must meet the requirements defined in IRS Publication 1075. To meet functional and assurance requirements, the security features of the environment must provide for the managerial, operational and technical controls. All security features must be available and activated to protect against unauthorized use of and access to Federal Tax Information.
- (8) No work involving Federal Tax Information furnished under this contract will be subcontracted without prior written approval of the IRS.
- (9) The contractor will maintain a list of employees authorized access. Such list will be provided to the agency and, upon request, to the IRS reviewing office.

(10) The agency will have the right to void the contract if the contractor fails to provide the safeguards described above.

(Include any additional safeguards that may be appropriate.)

II. CRIMINAL/CIVIL SANCTIONS

(1) Each officer or employee of any person to whom returns or return information is or may be disclosed will be notified in writing by such person that returns or return information disclosed to such officer or employee can be used only for a purpose and to the extent authorized herein, and that further disclosure of any such returns or return information for a purpose or to an extent unauthorized herein constitutes a felony punishable upon conviction by a fine of as much as \$5,000 or imprisonment for as long as 5 years, or both, together with the costs of prosecution. Such person shall also notify each such officer and employee that any such unauthorized further disclosure of returns or return information may also result in an award of civil damages against the officer or employee in an amount not less than \$1,000 with respect to each instance of unauthorized disclosure. These penalties are prescribed by IRCs 7213 and 7431 and set forth at 26 CFR 301.6103(n)-1.

(2) Each officer or employee of any person to whom returns or return information is or may be disclosed shall be notified in writing by such person that any return or return information made available in any format shall be used only for the purpose of carrying out the provisions of this contract. Information contained in such material shall be treated as confidential and shall not be divulged or made known in any manner to any person except as may be necessary in the performance of the contract. Inspection by or disclosure to anyone without an official need-to-know constitutes a criminal misdemeanor punishable upon conviction by a fine of as much as \$1,000 or imprisonment for as long as 1 year, or both, together with the costs of prosecution. Such person shall also notify each such officer and employee that any such unauthorized inspection or disclosure of returns or return information may also result in an award of civil damages against the officer or employee [United States for Federal employees] in an amount equal to the sum of the greater of \$1,000 for each act of unauthorized inspection or disclosure with respect to which such defendant is found liable or the sum of the actual damages sustained by the plaintiff as a result of such unauthorized inspection or disclosure plus in the case of a willful inspection or disclosure which is the result of gross negligence, punitive damages, plus the costs of the action. These penalties are prescribed by IRC 7213A and 7431 and set forth at 26 CFR 301.6103(n)-1.

(3) Additionally, it is incumbent upon the contractor to inform its officers and employees of the penalties for improper disclosure imposed by the Privacy Act of 1974, 5 U.S.C. 552a. Specifically, 5 U.S.C. 552a(i)(1), which is made applicable to contractors by 5 U.S.C. 552a(m)(1), provides that any officer or employee of a contractor, who by virtue of his/her employment or official position, has possession of or access to agency records which contain individually identifiable information, the disclosure of which is prohibited by the Privacy Act or regulations established thereunder, and who knowing that disclosure of the specific material is

prohibited, willfully discloses the material in any manner to any person or agency not entitled to receive it, shall be guilty of a misdemeanor and fined not more than \$5,000.

(4) Granting a contractor access to FTI must be preceded by certifying that each individual understands the agency's security policy and procedures for safeguarding IRS information. Contractors must maintain their authorization to access FTI through annual recertification. The initial certification and recertification must be documented and placed in the agency's files for review. As part of the certification and at least annually afterwards, contractors must be advised of the provisions of IRCs [7431](#), [7213](#) and [7213A](#) in [IRS Publication 1075](#). The training provided before the initial certification and annually thereafter must also cover the incident response policy and procedure for reporting unauthorized disclosures and data breaches. (See Section 1.8, Reporting Improper Inspections or Disclosures in [IRS Publication 1045](#).) For both the initial certification and the annual certification, the contractor must sign, either with ink or electronic signature, a confidentiality statement certifying their understanding of the security requirements.

III. DATA INCIDENT RESPONSE

The contractor will:

- (1) Cooperate with and exchange information with agency officials, as determined necessary by the agency, in order to effectively report and manage a suspected or confirmed breach.
- (2) Properly encrypt FTI in accordance with Publication 1075 and other applicable policies and to comply with any agency-specific policies for protecting FTI.
- (3) Complete regular training on how to identify and report a breach;
- (4) Report a suspected or confirmed breach in any medium or form, including paper, oral and electronic, as soon as possible and without unreasonable delay, consistent with the agency's incident management policy;
- (5) Maintain capabilities to determine what FTI was or could have been accessed and by whom, construct a timeline of user activity, determine methods and techniques used to access FTI and identify the initial attack vector; Allow for an inspection, investigation, forensic analysis and any other action necessary to ensure compliance with Publication 1075, the agency's breach response plan and to assist with responding to a breach; Identify roles and responsibilities, in accordance with Publication 1075 and the agency's breach response plan; and, explain that a report of a breach shall not, by itself, be interpreted as evidence that the contractor or its subcontractor failed to provide adequate safeguards for FTI.

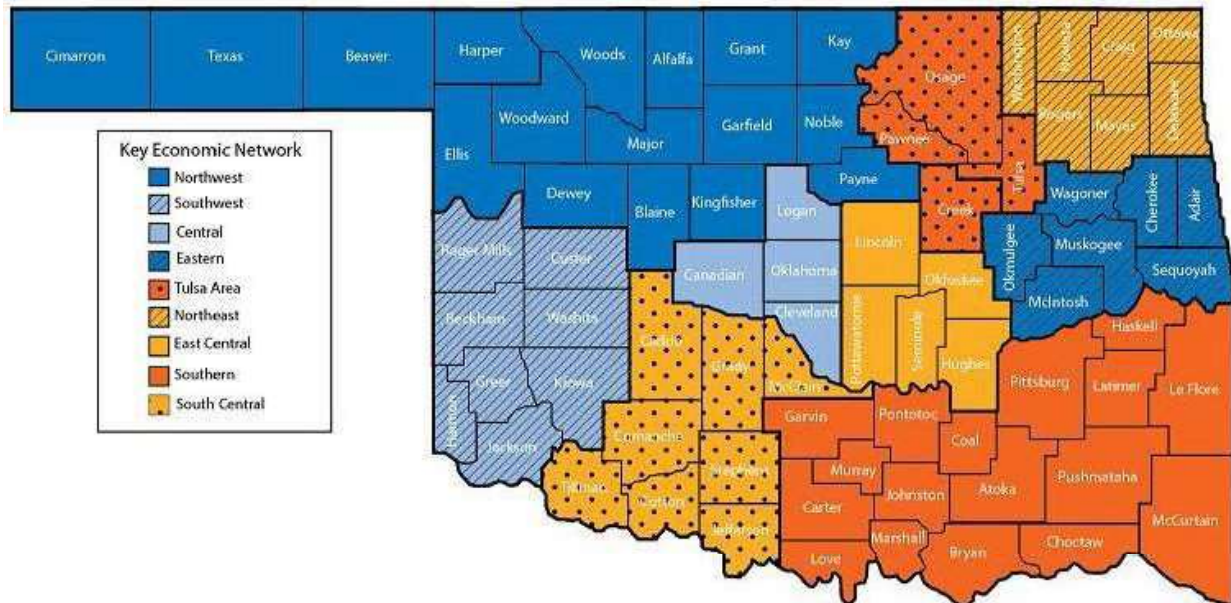
IV. INSPECTION

The IRS and the Agency, with 24 hour notice, shall have the right to send its inspectors into the offices and plants of the contractor to inspect facilities and operations performing any work with FTI under this contract for compliance with requirements defined in IRS Publication 1075. The

IRS' right of inspection shall include the use of manual and/or automated scanning tools to perform compliance and vulnerability assessments of information technology (IT) assets that

access, store, process or transmit FTL. On the basis of such inspection, corrective actions may be required in cases where the contractor is found to be noncompliant with contract safeguards.

Exhibit 4 - Oklahoma Key Economic Networks (KENs) Regions



9 Regions:

Northwest

Southwest

Central

Eastern

Tulsa Area

Northeast

East Central

Southern

South Central

ATTACHMENT B

STATE OF OKLAHOMA GENERAL TERMS

This State of Oklahoma General Terms (“General Terms”) is a Contract Document in connection with a Contract awarded by the Office of Management and Enterprise Services on behalf of the State of Oklahoma.

In addition to other terms contained in an applicable Contract Document, Supplier and State agree to the following General Terms:

1 Scope and Contract Renewal

- 1.1** Supplier may not add products or services to its offerings under the Contract without the State’s prior written approval. Such request may require a competitive bid of the additional products or services. If the need arises for goods or services outside the scope of the Contract, Supplier shall contact the State.
- 1.2** At no time during the performance of the Contract shall the Supplier have the authority to obligate any Customer for payment for any products or services (a) when a corresponding encumbering document is not signed or (b) over and above an awarded Contract amount. Likewise, Supplier is not entitled to compensation for a product or service provided by or on behalf of Supplier that is neither requested nor accepted as satisfactory.
- 1.3** If applicable, prior to any Contract renewal, the State shall subjectively consider the value of the Contract to the State, the Supplier’s performance under the Contract, and shall review certain other factors, including but not limited to the: a) terms and conditions of Contract Documents to determine validity with current State and other applicable statutes and rules; b) current pricing and discounts offered by Supplier; and c) current products, services and support offered by Supplier. If the State determines changes to the Contract are required as a condition precedent to renewal, the State and Supplier will cooperate in good faith to evidence such required changes in an Addendum. Further, any request for a price increase in connection with a renewal or otherwise will be conditioned on the Supplier providing appropriate documentation supporting the request.
- 1.4** The State may extend the Contract for ninety (90) days beyond a final renewal term at the Contract compensation rate for the extended period. If the State

exercises such option to extend ninety (90) days, the State shall notify the Supplier in writing prior to Contract end date. The State, at its sole option and to the extent allowable by law, may choose to exercise subsequent ninety (90) day extensions at the Contract pricing rate, to facilitate the finalization of related terms and conditions of a new award or as needed for transition to a new Supplier.

- 1.5** Supplier understands that supplier registration expires annually and, pursuant to OAC 260:115-3-3, Supplier shall maintain its supplier registration with the State as a precondition to a renewal of the Contract.

2 Contract Effectiveness and Order of Priority

- 2.1** Unless specifically agreed in writing otherwise, the Contract is effective upon the date last signed by the parties. Supplier shall not commence work, commit funds, incur costs, or in any way act to obligate the State until the Contract is effective.

- 2.2** Contract Documents shall be read to be consistent and complementary. Any conflict among the Contract Documents shall be resolved by giving priority to Contract Documents in the following order of precedence:

- A.** any Addendum;
- B.** any applicable Solicitation;
- C.** any Contract-specific State terms contained in a Contract Document including, without limitation, information technology terms and terms specific to a statewide Contract or a State agency Contract;
- D.** the terms contained in this Contract Document;
- E.** any successful Bid as may be amended through negotiation and to the extent the Bid does not otherwise conflict with the Solicitation or applicable law;
- F.** any statement of work, work order, or other similar ordering document as applicable; and
- G.** other mutually agreed Contract Documents.

- 2.3** If there is a conflict between the terms contained in this Contract Document or in Contract-specific terms and an agreement provided by or on behalf of Supplier including but not limited to linked or supplemental documents which alter or diminish the rights of Customer or the State, the conflicting terms

provided by Supplier shall not take priority over this Contract Document or Acquisition-specific terms. In no event will any linked document alter or override such referenced terms except as specifically agreed in an Addendum.

- 2.4 Any Contract Document shall be legibly written in ink or typed. All Contract transactions, and any Contract Document related thereto, may be conducted by electronic means pursuant to the Oklahoma Uniform Electronic Transactions Act.

3 **Modification of Contract Terms and Contract Documents**

- 3.1 The Contract may only be modified, amended, or expanded by an Addendum. Any change to the Contract, including the addition of work or materials, the revision of payment terms, or the substitution of work or materials made unilaterally by the Supplier, is a material breach of the Contract. Unless otherwise specified by applicable law or rules, such changes, including without limitation, any unauthorized written Contract modification, shall be void and without effect and the Supplier shall not be entitled to any claim under the Contract based on those changes. No oral statement of any person shall modify or otherwise affect the terms, conditions, or specifications stated in the Contract.
- 3.2 Any additional terms on an ordering document provided by Supplier are of no effect and are void unless mutually executed. OMES bears no liability for performance, payment or failure thereof by the Supplier or by a Customer other than OMES in connection with an Acquisition.

4 **Definitions**

In addition to any defined terms set forth elsewhere in the Contract, the Oklahoma Central Purchasing Act and the Oklahoma Administrative Code, Title 260, the parties agree that, when used in the Contract, the following terms are defined as set forth below and may be used in the singular or plural form:

- 4.1 **Acquisition** means items, products, materials, supplies, services and equipment acquired by purchase, lease purchase, lease with option to purchase, value provided or rental under the Contract.
- 4.2 **Addendum** means a mutually executed, written modification to a Contract Document.
- 4.3 **Amendment** means a written change, addition, correction or revision to the Solicitation.
- 4.4 **Bid** means an offer a Bidder submits in response to the Solicitation.

- 4.5 Bidder** means an individual or business entity that submits a Bid in response to the Solicitation.
- 4.6 Contract** means the written, mutually agreed and binding legal relationship resulting from the Contract Documents and an appropriate encumbering document as may be amended from time to time, which evidences the final agreement between the parties with respect to the subject matter of the Contract.
- 4.7 Contract Document** means this document; any master or enterprise agreement terms entered into between the parties that are mutually agreed to be applicable to the Contract; any Solicitation; any Contract-specific terms; any Supplier's Bid as may be negotiated; any statement of work, work order, or other similar mutually executed ordering document; other mutually executed documents and any Addendum.
- 4.8 Customer** means the entity receiving goods or services contemplated by the Contract.
- 4.9 Debarment** means action taken by a debarring official under federal or state law or regulations to exclude any business entity from inclusion on the Supplier list; bidding; offering to bid; providing a quote; receiving an award of contract with the State and may also result in cancellation of existing contracts with the State.
- 4.10 Destination** means delivered to the receiving dock or other point specified in the applicable Contract Document.
- 4.11 Indemnified Parties** means the State and Customer and/or its officers, directors, agents, employees, representatives, contractors, assignees and designees thereof.
- 4.12 Inspection** means examining and testing an Acquisition (including, when appropriate, raw materials, components, and intermediate assemblies) to determine whether the Acquisition meets Contract requirements.
- 4.13 Moral Rights** means any and all rights of paternity or integrity of the Work Product and the right to object to any modification, translation or use of the Work Product and any similar rights existing under the judicial or statutory law of any country in the world or under any treaty, regardless of whether or not such right is denominated or referred to as a moral right.
- 4.14 OAC** means the Oklahoma Administrative Code.
- 4.15 OMES** means the Office of Management and Enterprise Services.

- 4.16 Solicitation** means the document inviting Bids for the Acquisition referenced in the Contract and any amendments thereto.
- 4.17 State** means the government of the state of Oklahoma, its employees and authorized representatives, including without limitation any department, agency, or other unit of the government of the state of Oklahoma.
- 4.18 Supplier** means the Bidder with whom the State enters into the Contract awarded pursuant to the Solicitation or the business entity or individual that is a party to the Contract with the State.
- 4.19 Suspension** means action taken by a suspending official under federal or state law or regulations to suspend a Supplier from inclusion on the Supplier list; be eligible to submit Bids to State agencies and be awarded a contract by a State agency subject to the Central Purchasing Act.
- 4.20 Supplier Confidential Information** means certain confidential and proprietary information of Supplier that is clearly marked as confidential and agreed by the State Purchasing Director or Customer, as applicable, but does not include information excluded from confidentiality in provisions of the Contract or the Oklahoma Open Records Act.
- 4.21 Work Product** means any and all deliverables produced by Supplier under a statement of work or similar Contract Document issued pursuant to this Contract, including any and all tangible or intangible items or things that have been or will be prepared, created, developed, invented or conceived at any time following the Contract effective date including but not limited to any (i) works of authorship (such as manuals, instructions, printed material, graphics, artwork, images, illustrations, photographs, computer programs, computer software, scripts, object code, source code or other programming code, HTML code, flow charts, notes, outlines, lists, compilations, manuscripts, writings, pictorial materials, schematics, formulae, processes, algorithms, data, information, multimedia files, text web pages or web sites, other written or machine readable expression of such works fixed in any tangible media, and all other copyrightable works), (ii) trademarks, service marks, trade dress, trade names, logos, or other indicia of source or origin, (iii) ideas, designs, concepts, personality rights, methods, processes, techniques, apparatuses, inventions, formulas, discoveries, or improvements, including any patents, trade secrets and know-how, (iv) domain names, (v) any copies, and similar or derivative works to any of the foregoing, (vi) all documentation and materials related to any of the foregoing, (vii) all other goods, services or deliverables to be provided by or on behalf of Supplier under the Contract and (viii) all Intellectual Property Rights in any of the foregoing, and which are or were created,

prepared, developed, invented or conceived for the use of benefit of Customer in connection with this Contract or with funds appropriated by or for Customer or Customer's benefit (a) by any Supplier personnel or Customer personnel or (b) any Customer personnel who then became personnel to Supplier or any of its affiliates or subcontractors, where, although creation or reduction-to-practice is completed while the person is affiliated with Supplier or its personnel, any portion of same was created, invented or conceived by such person while affiliated with Customer.

5 Pricing

- 5.1** Pursuant to 68 O.S. §§ 1352, 1356, and 1404, State agencies are exempt from the assessment of State sales, use, and excise taxes. Further, State agencies and political subdivisions of the State are exempt from Federal Excise Taxes pursuant to Title 26 of the United States Code. Any taxes of any nature whatsoever payable by the Supplier shall not be reimbursed.
- 5.2** Pursuant to 74 O.S. §85.40, all travel expenses of Supplier must be included in the total Acquisition price.
- 5.3** The price of a product offered under the Contract shall include and Supplier shall prepay all shipping, packaging, delivery and handling fees. All product deliveries will be free on board Customer's Destination. No additional fees shall be charged by Supplier for standard shipping and handling. If Customer requests expedited or special delivery, Customer may be responsible for any charges for expedited or special delivery.

6 Ordering, Inspection, and Acceptance

- 6.1** Any product or service furnished under the Contract shall be ordered by issuance of a valid purchase order or other appropriate payment mechanism, including a pre-encumbrance, or by use of a valid Purchase Card. All orders and transactions are governed by the terms and conditions of the Contract. Any purchase order or other applicable payment mechanism dated prior to termination or expiration of the Contract shall be performed unless mutually agreed in writing otherwise.
- 6.2** Services will be performed in accordance with industry best practices and are subject to acceptance by the Customer. Notwithstanding any other provision in the Contract, deemed acceptance of a service or associated deliverable shall not apply automatically upon receipt of a deliverable or upon provision of a service.

Supplier warrants and represents that a product or deliverable furnished by or through the Supplier shall individually, and where specified by Supplier to perform as a system, be substantially uninterrupted and error-free in operation and guaranteed against faulty material and workmanship for a warranty period of the greater of ninety (90) days from the date of acceptance or the maximum allowed by the manufacturer. A defect in a product or deliverable furnished by or through the Supplier shall be repaired or replaced by Supplier at no additional cost or expense to the Customer if such defect occurs during the warranty period.

Any product to be delivered pursuant to the Contract shall be subject to final inspection and acceptance by the Customer at Destination. The Customer assumes no responsibility for a product until accepted by the Customer. Title and risk of loss or damage to a product shall be the responsibility of the Supplier until accepted. The Supplier shall be responsible for filing, processing, and collecting any and all damage claims accruing prior to acceptance.

Pursuant to OAC 260:115-9-5, payment for an Acquisition does not constitute final acceptance of the Acquisition. If subsequent inspection affirms that the Acquisition does not meet or exceed the specifications of the order or that the Acquisition has a latent defect, the Supplier shall be notified as soon as is reasonably practicable. The Supplier shall retrieve and replace the Acquisition at Supplier's expense or, if unable to replace, shall issue a refund to Customer. Refund under this section shall not be an exclusive remedy.

- 6.3** Supplier shall deliver products and services on or before the required date specified in a Contract Document. Failure to deliver timely may result in liquidated damages as set forth in the applicable Contract Document. Deviations, substitutions, or changes in a product or service, including changes of personnel directly providing services, shall not be made unless expressly authorized in writing by the Customer. Any substitution of personnel directly providing services shall be a person of comparable or greater skills, education and experience for performing the services as the person being replaced. Additionally, Supplier shall provide staff sufficiently experienced and able to perform with respect to any transitional services provided by Supplier in connection with termination or expiration of the Contract.
- 6.4** Product warranty and return policies and terms provided under any Contract Document will not be more restrictive or more costly than warranty and return policies and terms for other similarly situated customers for a like product.

7 Invoices and Payment

- 7.1** Supplier shall be paid upon submission of a proper invoice(s) at the prices stipulated in the Contract in accordance with 74 O.S. §85.44B which requires that payment be made only after products have been provided and accepted or services rendered and accepted.

The following terms additionally apply:

- A.** An invoice shall contain the purchase order number, description of products or services provided and the dates of such provision.
- B.** Failure to provide a timely and proper invoice may result in delay of processing the invoice for payment. Proper invoice is defined at OAC 260:10-1-2.
- C.** Payment of all fees under the Contract shall be due NET 45 days. Payment and interest on late payments are governed by 62 O.S. §34.72. Such interest is the sole and exclusive remedy for late payments by a State agency and no other late fees are authorized to be assessed pursuant to Oklahoma law.
- D.** The date from which an applicable early payment discount time is calculated shall be from the receipt date of a proper invoice. There is no obligation, however, to utilize an early payment discount.
- E.** If an overpayment or underpayment has been made to Supplier any subsequent payments to Supplier under the Contract may be adjusted to correct the account. A written explanation of the adjustment will be issued to Supplier.
- F.** Supplier shall have no right of setoff.
- G.** Because funds are typically dedicated to a particular fiscal year, an invoice will be paid only when timely submitted, which shall in no instance be later than six (6) months after the end of the fiscal year in which the goods are provided or services performed.
- H.** The Supplier shall accept payment by Purchase Card as allowed by Oklahoma law.

8 Maintenance of Insurance, Payment of Taxes, and Workers' Compensation

- 8.1** As a condition of this Contract, Supplier shall procure at its own expense, and provide proof of, insurance coverage with the applicable liability limits set

forth below and any approved subcontractor of Supplier shall procure and provide proof of the same coverage. The required insurance shall be underwritten by an insurance carrier with an A.M. Best rating of A- or better.

Such proof of coverage shall additionally be provided to the Customer if services will be provided by any of Supplier's employees, agents or subcontractors at any Customer premises and/or employer vehicles will be used in connection with performance of Supplier's obligations under the Contract. Supplier may not commence performance hereunder until such proof has been provided. Additionally, Supplier shall ensure each insurance policy includes a thirty (30) day notice of cancellation and name the State and its agencies as certificate holder and shall promptly provide proof to the State of any renewals, additions, or changes to such insurance coverage. Supplier's obligation to maintain insurance coverage under the Contract is a continuing obligation until Supplier has no further obligation under the Contract. Any combination of primary and excess or umbrella insurance may be used to satisfy the limits of coverage for Commercial General Liability, Auto Liability and Employers' Liability. Unless agreed between the parties and approved by the State Purchasing Director, the minimum acceptable insurance limits of liability are as follows:

- A.** Workers' Compensation and Employer's Liability Insurance in accordance with and to the extent required by applicable law;
- B.** Commercial General Liability Insurance covering the risks of personal injury, bodily injury (including death) and property damage, including coverage for contractual liability, with a limit of liability of not less than \$5,000,000 per occurrence;
- C.** Automobile Liability Insurance with limits of liability of not less than \$5,000,000 combined single limit each accident;
- D.** Directors and Officers Insurance which shall include Employment Practices Liability as well as Consultant's Computer Errors and Omissions Coverage, if information technology services are provided under the Contract, with limits not less than \$5,000,000 per occurrence;
- E.** Security and Privacy Liability insurance, including coverage for failure to protect confidential information and failure of the security of Supplier's computer systems that results in unauthorized access to Customer data with limits \$5,000,000 per occurrence; and
- F.** Additional coverage required in writing in connection with a particular Acquisition.

- 8.2** Supplier shall be entirely responsible during the existence of the Contract for the liability and payment of taxes payable by or assessed to Supplier or its employees, agents and subcontractors of whatever kind, in connection with the Contract. Supplier further agrees to comply with all state and federal laws applicable to any such persons, including laws regarding wages, taxes, insurance, and Workers' Compensation. Neither Customer nor the State shall be liable to the Supplier, its employees, agents, or others for the payment of taxes or the provision of unemployment insurance and/or Workers' Compensation or any benefit available to a State or Customer employee.
- 8.3** Supplier agrees to indemnify Customer, the State, and its employees, agents, representatives, contractors, and assignees for any and all liability, actions, claims, demands, or suits, and all related costs and expenses (including without limitation reasonable attorneys' fees and costs required to establish the right to indemnification) relating to tax liability, unemployment insurance and/or Workers' Compensation in connection with its performance under the Contract.

9 Compliance with Applicable Laws

- 9.1** As long as Supplier has an obligation under the terms of the Contract and in connection with performance of its obligations, the Supplier represents its present compliance, and shall have an ongoing obligation to comply, with all applicable federal, State, and local laws, rules, regulations, ordinances, and orders, as amended, including but not limited to the following:
- A.** Drug-Free Workplace Act of 1988 set forth at 41 U.S.C. §81.
 - B.** Section 306 of the Clean Air Act, Section 508 of the Clean Water Act, Executive Order 11738, and Environmental Protection Agency Regulations which prohibit the use of facilities included on the EPA List of Violating Facilities under nonexempt federal contracts, grants or loans;
 - C.** Prospective participant requirements set at 45 C.F.R. part 76 in connection with Debarment, Suspension and other responsibility matters;
 - D.** 1964 Civil Rights Act, Title IX of the Education Amendment of 1972, Section 504 of the Rehabilitation Act of 1973, Americans with Disabilities Act of 1990, and Executive Orders 11246 and 11375;
 - E.** Anti-Lobbying Law set forth at 31 U.S.C. §1325 and as implemented at 45 C.F.R. part 93;

- F.** Requirements of Internal Revenue Service Publication 1075 regarding use, access and disclosure of Federal Tax Information (as defined therein);
 - G.** Obtaining certified independent audits conducted in accordance with Government Auditing Standards and Office of Management and Budget Uniform Guidance, 2 CFR 200 Subpart F §200.500 et seq. with approval and work paper examination rights of the applicable procuring entity;
 - H.** Requirements of the Oklahoma Taxpayer and Citizen Protection Act of 2007, 25 O.S. §1312 and applicable federal immigration laws and regulations and be registered and participate in the Status Verification System. The Status Verification System is defined at 25 O.S. §1312, includes but is not limited to the free Employment Verification Program (E-Verify) through the Department of Homeland Security, and is available at www.dhs.gov/E-Verify;
 - I.** Requirements of the Health Insurance Portability and Accountability Act of 1996; Health Information Technology for Economic and Clinical Health Act; Payment Card Industry Security Standards; Criminal Justice Information System Security Policy and Security Addendum; and Family Educational Rights and Privacy Act; and
 - J.** Be registered as a business entity licensed to do business in the State, have obtained a sales tax permit, and be current on franchise tax payments to the State, as applicable.
- 9.2** The Supplier's employees, agents and subcontractors shall adhere to applicable Customer policies including, but not limited to acceptable use of Internet and electronic mail, facility and data security, press releases, and public relations. As applicable, the Supplier shall adhere to the State Information Security Policy, Procedures, Guidelines set forth at https://omes.ok.gov/sites/g/files/gmc316/f/InfoSecPPG_0.pdf. Supplier is responsible for reviewing and relaying such policies covering the above to the Supplier's employees, agents and subcontractors.
- 9.3** At no additional cost to Customer, the Supplier shall maintain all applicable licenses and permits required in association with its obligations under the Contract.
- 9.4** In addition to compliance under subsection 9.1 above, Supplier shall have a continuing obligation to comply with applicable Customer-specific mandatory

contract provisions required in connection with the receipt of federal funds or other funding source.

- 9.5** The Supplier is responsible to review and inform its employees, agents, and subcontractors who provide a product or perform a service under the Contract of the Supplier's obligations under the Contract and Supplier certifies that its employees and each such subcontractor shall comply with minimum requirements and applicable provisions of the Contract. At the request of the State, Supplier shall promptly provide adequate evidence that such persons are its employees, agents or approved subcontractors and have been informed of their obligations under the Contract.
- 9.6** As applicable, Supplier agrees to comply with the Governor's Executive Orders related to the use of any tobacco product, electronic cigarette or vaping device on any and all properties owned, leased, or contracted for use by the State, including but not limited to all buildings, land and vehicles owned, leased, or contracted for use by agencies or instrumentalities of the State.
- 9.7** The execution, delivery and performance of the Contract and any ancillary documents by Supplier will not, to the best of Supplier's knowledge, violate, conflict with, or result in a breach of any provision of, or constitute a default (or an event which, with notice or lapse of time or both, would constitute a default) under, or result in the termination of, any written contract or other instrument between Supplier and any third party.
- 9.8** Supplier represents that it has the ability to pay its debts when due and it does not anticipate the filing of a voluntary or involuntary bankruptcy petition or appointment of a receiver, liquidator or trustee.
- 9.9** Supplier represents that, to the best of its knowledge, any litigation or claim or any threat thereof involving Supplier has been disclosed in writing to the State and Supplier is not aware of any other litigation, claim or threat thereof.
- 9.10** If services provided by Supplier include delivery of an electronic communication, Supplier shall ensure such communication and any associated support documents are compliant with Section 508 of the Federal Rehabilitation Act and with State standards regarding accessibility. Should any communication or associated support documents be non-compliant, Supplier shall correct and re-deliver such communication immediately upon discovery or notice, at no additional cost to the State. Additionally, as part of compliance with accessibility requirements where documents are only provided in non-electronic format, Supplier shall promptly provide such communication and any associated support documents in an alternate format

usable by individuals with disabilities upon request and at no additional cost, which may originate from an intended recipient or from the State.

10 Audits and Records Clause

- 10.1** As used in this clause and pursuant to 67 O.S. §203, “record” includes a document, book, paper, photograph, microfilm, computer tape, disk, record, sound recording, film recording, video record, accounting procedures and practices, and other data, regardless of type and regardless of whether such items are in written form, in the form of computer data, or in any other form. Supplier agrees any pertinent federal or State agency or governing entity of a Customer shall have the right to examine and audit, at no additional cost to a Customer, all records relevant to the execution and performance of the Contract except, unless otherwise agreed, costs of Supplier that comprise pricing under the Contract.
- 10.2** The Supplier is required to retain records relative to the Contract for the duration of the Contract and for a period of seven (7) years following completion or termination of an Acquisition unless otherwise indicated in the Contract terms. If a claim, audit, litigation or other action involving such records is started before the end of the seven-year period, the records are required to be maintained for two (2) years from the date that all issues arising out of the action are resolved, or until the end of the seven (7) year retention period, whichever is later.
- 10.3** Pursuant to 74 O.S. §85.41, if professional services are provided hereunder, all items of the Supplier that relate to the professional services are subject to examination by the State agency, State Auditor and Inspector and the State Purchasing Director.

11 Confidentiality

- 11.1** The Supplier shall maintain strict security of all State and citizen data and records entrusted to it or to which the Supplier gains access, in accordance with and subject to applicable federal and State laws, rules, regulations, and policies and shall use any such data and records only as necessary for Supplier to perform its obligations under the Contract. The Supplier further agrees to evidence such confidentiality obligation in a separate writing if required under such applicable federal or State laws, rules and regulations. The Supplier warrants and represents that such information shall not be sold, assigned, conveyed, provided, released, disseminated or otherwise disclosed by Supplier, its employees, officers, directors, subsidiaries, affiliates, agents, representatives, assigns, subcontractors, independent contractors, successor or any other persons or entities without Customer’s prior express written

permission. Supplier shall instruct all such persons and entities that the confidential information shall not be disclosed or used without the Customer's prior express written approval except as necessary for Supplier to render services under the Contract. The Supplier further warrants that it has a tested and proven system in effect designed to protect all confidential information.

- 11.2** Supplier shall establish, maintain and enforce agreements with all such persons and entities that have access to State and citizen data and records to fulfill Supplier's duties and obligations under the Contract and to specifically prohibit any sale, assignment, conveyance, provision, release, dissemination or other disclosure of any State or citizen data or records except as required by law or allowed by written prior approval of the Customer.
- 11.3** Supplier shall immediately report to the Customer any and all unauthorized use, appropriation, sale, assignment, conveyance, provision, release, access, acquisition, disclosure or other dissemination of any State or citizen data or records of which it or its parent company, subsidiaries, affiliates, employees, officers, directors, assignees, agents, representatives, independent contractors, and subcontractors is aware or have knowledge or reasonable should have knowledge. The Supplier shall also promptly furnish to Customer full details of the unauthorized use, appropriation, sale, assignment, conveyance, provision, release, access, acquisition, disclosure or other dissemination, or attempt thereof, and use its best efforts to assist the Customer in investigating or preventing the reoccurrence of such event in the future. The Supplier shall cooperate with the Customer in connection with any litigation and investigation deemed necessary by the Customer to protect any State or citizen data and records and shall bear all costs associated with the investigation, response and recovery in connection with any breach of State or citizen data or records including but not limited to credit monitoring services with a term of at least three (3) years, all notice-related costs and toll free telephone call center services.
- 11.4** Supplier further agrees to promptly prevent a reoccurrence of any unauthorized use, appropriation, sale, assignment, conveyance, provision, release, access, acquisition, disclosure or other dissemination of State or citizen data and records.
- 11.5** Supplier acknowledges that any improper use, appropriation, sale, assignment, conveyance, provision, release, access, acquisition, disclosure or other dissemination of any State data or records to others may cause immediate and irreparable harm to the Customer and certain beneficiaries and may violate state or federal laws and regulations. If the Supplier or its affiliates, parent company, subsidiaries, employees, officers, directors, assignees, agents,

representatives, independent contractors, and subcontractors improperly use, appropriate, sell, assign, convey, provide, release, access, acquire, disclose or otherwise disseminate such confidential information to any person or entity in violation of the Contract, the Customer will immediately be entitled to injunctive relief and/or any other rights or remedies available under this Contract, at equity or pursuant to applicable statutory, regulatory, and common law without a cure period.

11.6 The Supplier shall immediately forward to the State Purchasing Director, and any other applicable person listed in the Notices section(s) of the Contract, any request by a third party for data or records in the possession of the Supplier or any subcontractor or to which the Supplier or subcontractor has access and Supplier shall fully cooperate with all efforts to protect the security and confidentiality of such data or records in response to a third party request.

11.7 Customer may be provided access to Supplier Confidential Information. State agencies are subject to the Oklahoma Open Records Act and Supplier acknowledges information marked confidential information will be disclosed to the extent permitted under the Open Records Act and in accordance with this section. Nothing herein is intended to waive the State Purchasing Director's authority under OAC 260:115-3-9 in connection with Bid information requested to be held confidential by a Bidder. Notwithstanding the foregoing, Supplier Confidential Information shall not include information that: (i) is or becomes generally known or available by public disclosure, commercial use or otherwise and is not in contravention of this Contract; (ii) is known and has been reduced to tangible form by the receiving party before the time of disclosure for the first time under this Contract and without other obligations of confidentiality; (iii) is independently developed without the use of any of Supplier Confidential Information; (iv) is lawfully obtained from a third party (without any confidentiality obligation) who has the right to make such disclosure or (v) résumé, pricing or marketing materials provided to the State. In addition, the obligations in this section shall not apply to the extent that the applicable law or regulation requires disclosure of Supplier Confidential Information, provided that the Customer provides reasonable written notice, pursuant to Contract notice provisions, to the Supplier so that the Supplier may promptly seek a protective order or other appropriate remedy.

12 Conflict of Interest

In addition to any requirement of law or of a professional code of ethics or conduct, the Supplier, its employees, agents and subcontractors are required to disclose any outside activity or interest that conflicts or may conflict with the best interest of the State. Prompt disclosure is required under this section if the activity or interest is

related, directly or indirectly, to any person or entity currently under contract with or seeking to do business with the State, its employees or any other third-party individual or entity awarded a contract with the State. Further, as long as the Supplier has an obligation under the Contract, any plan, preparation or engagement in any such activity or interest shall not occur without prior written approval of the State. Any conflict of interest shall, at the sole discretion of the State, be grounds for partial or whole termination of the Contract.

13 Assignment and Permitted Subcontractors

- 13.1** Supplier's obligations under the Contract may not be assigned or transferred to any other person or entity without the prior written consent of the State which may be withheld at the State's sole discretion. Should Supplier assign its rights to payment, in whole or in part, under the Contract, Supplier shall provide the State and all affected Customers with written notice of the assignment. Such written notice shall be delivered timely and contain details sufficient for affected Customers to perform payment obligations without any delay caused by the assignment.
- 13.2** Notwithstanding the foregoing, the Contract may be assigned by Supplier to any corporation or other entity in connection with a merger, consolidation, sale of all equity interests of the Supplier, or a sale of all or substantially all of the assets of the Supplier to which the Contract relates. In any such case, said corporation or other entity shall by operation of law or expressly in writing assume all obligations of the Supplier as fully as if it had been originally made a party to the Contract. Supplier shall give the State and all affected Customers prior written notice of said assignment. Any assignment or delegation in violation of this subsection shall be void.
- 13.3** If the Supplier is permitted to utilize subcontractors in support of the Contract, the Supplier shall remain solely responsible for its obligations under the terms of the Contract, for its actions and omissions and those of its agents, employees and subcontractors and for payments to such persons or entities. Prior to a subcontractor being utilized by the Supplier, the Supplier shall obtain written approval of the State of such subcontractor and each employee, as applicable to a particular Acquisition, of such subcontractor proposed for use by the Supplier. Such approval is within the sole discretion of the State. Any proposed subcontractor shall be identified by entity name, and by employee name, if required by the particular Acquisition, in the applicable proposal and shall include the nature of the services to be performed. As part of the approval request, the Supplier shall provide a copy of a written agreement executed by the Supplier and subcontractor setting forth that such subcontractor is bound by and agrees, as applicable, to perform the same covenants and be subject to

the same conditions and make identical certifications to the same facts and criteria, as the Supplier under the terms of all applicable Contract Documents. Supplier agrees that maintaining such agreement with any subcontractor and obtaining prior written approval by the State of any subcontractor and associated employees shall be a continuing obligation. The State further reserves the right to revoke approval of a subcontractor or an employee thereof in instances of poor performance, misconduct or for other similar reasons.

13.4 All payments under the Contract shall be made directly to the Supplier, except as provided in subsection A above regarding the Supplier's assignment of payment. No payment shall be made to the Supplier for performance by unapproved or disapproved employees of the Supplier or a subcontractor.

13.5 Rights and obligations of the State or a Customer under the terms of this Contract may be assigned or transferred, at no additional cost, to other Customer entities.

14 Background Checks and Criminal History Investigations

Prior to the commencement of any services, background checks and criminal history investigations of the Supplier's employees and subcontractors who will be providing services may be required and, if so, the required information shall be provided to the State in a timely manner. Supplier's access to facilities, data and information may be withheld prior to completion of background verification acceptable to the State. The costs of additional background checks beyond Supplier's normal hiring practices shall be the responsibility of the Customer unless such additional background checks are required solely because Supplier will not provide results of its otherwise acceptable normal background checks; in such an instance, Supplier shall pay for the additional background checks. Supplier will coordinate with the State and its employees to complete the necessary background checks and criminal history investigations. Should any employee or subcontractor of the Supplier who will be providing services under the Contract not be acceptable as a result of the background check or criminal history investigation, the Customer may require replacement of the employee or subcontractor in question and, if no suitable replacement is made within a reasonable time, terminate the purchase order or other payment mechanism associated with the project or services.

15 Patents and Copyrights

Without exception, a product or deliverable price shall include all royalties or costs owed by the Supplier to any third party arising from the use of a patent, intellectual property, copyright or other property right held by such third party. Should any third party threaten or make a claim that any portion of a product or service provided by Supplier under the Contract infringes that party's patent, intellectual property,

copyright or other property right, Supplier shall enable each affected Customer to legally continue to use, or modify for use, the portion of the product or service at issue or replace such potentially infringing product, or re-perform or redeliver in the case of a service, with at least a functional non-infringing equivalent. Supplier's duty under this section shall extend to include any other product or service rendered materially unusable as intended due to replacement or modification of the product or service at issue. If the Supplier determines that none of these alternatives are reasonably available, the State shall return such portion of the product or deliverable at issue to the Supplier, upon written request, in exchange for a refund of the price paid for such returned goods as well as a refund or reimbursement, if applicable, of the cost of any other product or deliverable rendered materially unusable as intended due to removal of the portion of product or deliverable at issue. Any remedy provided under this section is not an exclusive remedy and is not intended to operate as a waiver of legal or equitable remedies because of acceptance of relief provided by Supplier.

16 Indemnification

16.1 Acts or Omissions

- A.** Supplier shall defend and indemnify the Indemnified Parties, as applicable, for any and all liability, claims, damages, losses, costs, expenses, demands, suits and actions of third parties (including without limitation reasonable attorneys' fees and costs required to establish the right to indemnification) arising out of, or resulting from any action or claim for bodily injury, death, or property damage brought against any of the Indemnified parties to the extent arising from any negligent act or omission or willful misconduct of the Supplier or its agents, employees, or subcontractors in the execution or performance of the Contract.
- B.** To the extent Supplier is found liable for loss, damage, or destruction of any property of Customer due to negligence, misconduct, wrongful act, or omission on the part of the Supplier, its employees, agents, representatives, or subcontractors, the Supplier and Customer shall use best efforts to mutually negotiate an equitable settlement amount to repair or replace the property unless such loss, damage or destruction is of such a magnitude that repair or replacement is not a reasonable option. Such amount shall be invoiced to, and is payable by, Supplier sixty (60) calendar days after the date of Supplier's receipt of an invoice for the negotiated settlement amount.

16.2 Infringement

Supplier shall indemnify the Indemnified Parties, as applicable, for all liability, claims, damages, losses, costs, expenses, demands, suits and actions of third parties (including without limitation reasonable attorneys' fees and costs required to establish the right to indemnification) arising from or in connection with Supplier's breach of its representations and warranties in the Contract or alleged infringement of any patent, intellectual property, copyright or other property right in connection with a product or service provided under the Contract. Supplier's duty under this section is reduced to the extent a claimed infringement results from: (a) a Customer's or user's content; (b) modifications by Customer or third party to a product delivered under the Contract or combinations of the product with any non-Supplier-provided services or products unless Supplier recommended or participated in such modification or combination; (c) use of a product or service by Customer in violation of the Contract unless done so at the direction of Supplier, or (d) a non-Supplier product that has not been provided to the State by, through or on behalf of Supplier as opposed to its combination with products Supplier provides to or develops for the State or a Customer as a system.

16.3 Notice and Cooperation

In connection with indemnification obligations under the Contract, the parties agree to furnish prompt written notice to each other of any third-party claim. Any Customer affected by the claim will reasonably cooperate with Supplier and defense of the claim to the extent its interests are aligned with Supplier. Supplier shall use counsel reasonably experienced in the subject matter at issue and will not settle a claim without the written consent of the party being defended, which consent will not be unreasonably withheld or delayed, except that no consent will be required to settle a claim against Indemnified Parties that are not a State agency, where relief against the Indemnified Parties is limited to monetary damages that are paid by the defending party under indemnification provisions of the Contract.

16.4 Coordination of Defense

In connection with indemnification obligations under the Contract, when a State agency is a named defendant in any filed or threatened lawsuit, the defense of the State agency shall be coordinated by the Attorney General of Oklahoma, or the Attorney General may authorize the Supplier to control the defense and any related settlement negotiations; provided, however, Supplier shall not agree to any settlement of claims against the State without obtaining advance written concurrence from the Attorney General. If the Attorney General does not authorize sole control of the defense and settlement negotiations to Supplier, Supplier shall have authorization to equally

participate in any proceeding related to the indemnity obligation under the Contract and shall remain responsible to indemnify the applicable Indemnified Parties.

16.5 Limitation of Liability

- A.** With respect to any claim or cause of action arising under or related to the Contract, neither the State nor any Customer shall be liable to Supplier for lost profits, lost sales or business expenditures, investments, or commitments in connection with any business, loss of any goodwill, or for any other indirect, incidental, punitive, special or consequential damages, even if advised of the possibility of such damages.
- B.** Notwithstanding anything to the contrary in the Contract, no provision shall limit damages, expenses, costs, actions, claims, and liabilities arising from or related to property damage, bodily injury or death caused by Supplier or its employees, agents or subcontractors; indemnity, security or confidentiality obligations under the Contract; the bad faith, negligence, intentional misconduct or other acts for which applicable law does not allow exemption from liability of Supplier or its employees, agents or subcontractors.
- C.** The limitation of liability and disclaimers set forth in the Contract will apply regardless of whether Customer has accepted a product or service. The parties agree that Supplier has set its fees and entered into the Contract in reliance on the disclaimers and limitations set forth herein, that the same reflect an allocation of risk between the parties and form an essential basis of the bargain between the parties. These limitations shall apply notwithstanding any failure of essential purpose of any limited remedy.

17 Termination for Funding Insufficiency

- 17.1** Notwithstanding anything to the contrary in any Contract Document, the State may terminate the Contract in whole or in part if funds sufficient to pay obligations under the Contract are not appropriated or received from an intended third-party funding source. In the event of such insufficiency, Supplier will be provided at least fifteen (15) calendar days' written notice of termination. Any partial termination of the Contract under this section shall not be construed as a waiver of, and shall not affect, the rights and obligations of any party regarding portions of the Contract that are not terminated. The determination by the State of insufficient funding shall be accepted by, and shall be final and binding on, the Supplier.

- 17.2** Upon receipt of notice of a termination, Supplier shall immediately comply with the notice terms and take all necessary steps to minimize the incurrence of costs allocable to the work affected by the notice. If a purchase order or other payment mechanism has been issued and a product or service has been accepted as satisfactory prior to the effective date of termination, the termination does not relieve an obligation to pay for the product or service but there shall not be any liability for further payments ordinarily due under the Contract or for any damages or other amounts caused by or associated with such termination. Any amount paid to Supplier in the form of prepaid fees that are unused when the Contractor certain obligations are terminated shall be refunded.
- 17.3** The State's exercise of its right to terminate the Contract under this section shall not be considered a default or breach under the Contract or relieve the Supplier of any liability for claims arising under the Contract.

18 Termination for Cause

- 18.1** Supplier may terminate the Contract if (i) it has provided the State with written notice of material breach and (ii) the State fails to cure such material breach within thirty (30) days of receipt of written notice. If there is more than one Customer, material breach by a Customer does not give rise to a claim of material breach as grounds for termination by Supplier of the Contract as a whole. The State may terminate the Contract in whole or in part if (i) it has provided Supplier with written notice of material breach, and (ii) Supplier fails to cure such material breach within thirty (30) days of receipt of written notice. Any partial termination of the Contract under this section shall not be construed as a waiver of, and shall not affect, the rights and obligations of any party regarding portions of the Contract that are not terminated.
- 18.2** The State may terminate the Contract in whole or in part immediately without a thirty (30) day written notice to Supplier if (i) Supplier fails to comply with confidentiality, privacy, security, environmental or safety requirements applicable to Supplier's performance or obligations under the Contract; (ii) Supplier's material breach is reasonably determined to be an impediment to the function of the State and detrimental to the State or to cause a condition precluding the thirty (30) day notice or (iii) when the State determines that an administrative error in connection with award of the Contract occurred prior to Contract performance.
- 18.3** Upon receipt of notice of a termination, Supplier shall immediately comply with the notice terms and take all necessary steps to minimize the incurrence

of costs allocable to the work affected by the notice. If a purchase order or other payment mechanism has been issued and a product or service has been accepted as satisfactory prior to the effective date of termination, the termination does not relieve an obligation to pay for the product or service but there shall not be any liability for further payments ordinarily due under the Contract or for any damages or other amounts caused by or associated with such termination. Such termination is not an exclusive remedy but is in addition to any other rights and remedies provided for by law. Any amount paid to Supplier in the form of prepaid fees that are unused when the Contract or certain obligations are terminated shall be refunded. Termination of the Contract under this section, in whole or in part, shall not relieve the Supplier of liability for claims arising under the Contract.

- 18.4** The Supplier's repeated failure to provide an acceptable product or service; Supplier's unilateral revision of linked or supplemental terms that have a materially adverse impact on a Customer's rights or obligations under the Contract (except as required by a governmental authority); actual or anticipated failure of Supplier to perform its obligations under the Contract; Supplier's inability to pay its debts when due; assignment for the benefit of Supplier's creditors; or voluntary or involuntary appointment of a receiver or filing of bankruptcy of Supplier shall constitute a material breach of the Supplier's obligations, which may result in partial or whole termination of the Contract. This subsection is not intended as an exhaustive list of material breach conditions. Termination may also result from other instances of failure to adhere to the Contract provisions and for other reasons provided for by applicable law, rules or regulations; without limitation, OAC 260:115-9-9 is an example.

19 Termination for Convenience

- 19.1** The State may terminate the Contract, in whole or in part, for convenience if it is determined that termination is in the State's best interest. In the event of a termination for convenience, Supplier will be provided at least thirty (30) days' written notice of termination. Any partial termination of the Contract shall not be construed as a waiver of, and shall not affect, the rights and obligations of any party regarding portions of the Contract that remain in effect.
- 19.2** Upon receipt of notice of such termination, Supplier shall immediately comply with the notice terms and take all necessary steps to minimize the incurrence of costs allocable to the work affected by the notice. If a purchase order or other payment mechanism has been issued and a product or service has been accepted as satisfactory prior to the effective date of termination, the termination does not relieve an obligation to pay for the product or service but

there shall not be any liability for further payments ordinarily due under the Contract or for any damages or other amounts caused by or associated with such termination. Such termination shall not be an exclusive remedy but shall be in addition to any other rights and remedies provided for by law. Any amount paid to Supplier in the form of prepaid fees that are unused when the Contract or certain obligations are terminated shall be refunded. Termination of the Contract under this section, in whole or in part, shall not relieve the Supplier of liability for claims arising under the Contract.

20 Suspension of Supplier

- 20.1** Supplier may be subject to Suspension without advance notice and may additionally be suspended from activities under the Contract if Supplier fails to comply with confidentiality, privacy, security, environmental or safety requirements applicable to Supplier's performance or obligations under the Contract.
- 20.2** Upon receipt of a notice pursuant to this section, Supplier shall immediately comply with the notice terms and take all necessary steps to minimize the incurrence of costs allocable to the work affected by the notice. If a purchase order or other payment mechanism has been issued and a product or service has been accepted as satisfactory prior to receipt of notice by Supplier, the Suspension does not relieve an obligation to pay for the product or service but there shall not be any liability for further payments ordinarily due under the Contract during a period of Suspension or suspended activity or for any damages or other amounts caused by or associated with such Suspension or suspended activity. A right exercised under this section shall not be an exclusive remedy but shall be in addition to any other rights and remedies provided for by law. Any amount paid to Supplier in the form of prepaid fees attributable to a period of Suspension or suspended activity shall be refunded.
- 20.3** Such Suspension may be removed, or suspended activity may resume, at the earlier of such time as a formal notice is issued that authorizes the resumption of performance under the Contract or at such time as a purchase order or other appropriate encumbrance document is issued. This subsection is not intended to operate as an affirmative statement that such resumption will occur.

21 Certification Regarding Debarment, Suspension, and Other Responsibility Matters

The certification made by Supplier with respect to Debarment, Suspension, certain indictments, convictions, civil judgments and terminated public contracts is a material representation of fact upon which reliance was placed when entering into the Contract.

A determination that Supplier knowingly rendered an erroneous certification, in addition to other available remedies, may result in whole or partial termination of the Contract for Supplier's default. Additionally, Supplier shall promptly provide written notice to the State Purchasing Director if the certification becomes erroneous due to changed circumstances.

22 Certification Regarding State Employees Prohibition From Fulfilling Services

Pursuant to 74 O.S. § 85.42, the Supplier certifies that no person involved in any manner in development of the Contract employed by the State shall be employed to fulfill any services provided under the Contract.

23 Force Majeure

23.1 Either party shall be temporarily excused from performance to the extent delayed as a result of unforeseen causes beyond its reasonable control including fire or other similar casualty, act of God, strike or labor dispute, war or other violence, or any law, order or requirement of any governmental agency or authority provided the party experiencing the force majeure event has prudently and promptly acted to take any and all steps within the party's control to ensure continued performance and to shorten duration of the event. If a party's performance of its obligations is materially hindered as a result of a force majeure event, such party shall promptly notify the other party of its best reasonable assessment of the nature and duration of the force majeure event and steps it is taking, and plans to take, to mitigate the effects of the force majeure event. The party shall use commercially reasonable best efforts to continue performance to the extent possible during such event and resume full performance as soon as reasonably practicable.

23.2 Subject to the conditions set forth above, non-performance as a result of a force majeure event shall not be deemed a default. However, a purchase order or other payment mechanism may be terminated if Supplier cannot cause delivery of a product or service in a timely manner to meet the business needs of Customer. Supplier is not entitled to payment for products or services not received and, therefore, amounts payable to Supplier during the force majeure event shall be equitably adjusted downward.

23.3 Notwithstanding the foregoing or any other provision in the Contract, (i) the following are not a force majeure event under the Contract: (a) shutdowns, disruptions or malfunctions in Supplier's system or any of Supplier's telecommunication or internet services other than as a result of general and widespread internet or telecommunications failures that are not limited to Supplier's systems or (b) the delay or failure of Supplier or subcontractor personnel to perform any obligation of Supplier hereunder unless such delay

or failure to perform is itself by reason of a force majeure event and (ii) no force majeure event modifies or excuses Supplier's obligations related to confidentiality, indemnification, data security or breach notification obligations set forth herein.

24 Security of Property and Personnel

In connection with Supplier's performance under the Contract, Supplier may have access to Customer personnel, premises, data, records, equipment and other property. Supplier shall use commercially reasonable best efforts to preserve the safety and security of such personnel, premises, data, records, equipment, and other property of Customer. Supplier shall be responsible for damage to such property to the extent such damage is caused by its employees or subcontractors and shall be responsible for loss of Customer property in its possession, regardless of cause. If Supplier fails to comply with Customer's security requirements, Supplier is subject to immediate suspension of work as well as termination of the associated purchase order or other payment mechanism.

25 Notices

All notices, approvals or requests allowed or required by the terms of any Contract Document shall be in writing, reference the Contract with specificity and deemed delivered upon receipt or upon refusal of the intended party to accept receipt of the notice. In addition to other notice requirements in the Contract and the designated Supplier contact provided in a successful Bid, notices shall be sent to the State at the physical address set forth below. Notice information may be updated in writing to the other party as necessary. Notwithstanding any other provision of the Contract, confidentiality, breach and termination-related notices shall not be delivered solely via e-mail.

If sent to the State:

State Purchasing Director
2401 North Lincoln Boulevard, Suite 116
Oklahoma City, Oklahoma 73105

With a copy, which shall not constitute notice, to:

Purchasing Division Deputy General Counsel
2401 North Lincoln Boulevard, Suite 116
Oklahoma City, Oklahoma 73105

26 Miscellaneous

26.1 Choice of Law and Venue

Any claim, dispute, or litigation relating to the Contract Documents, in the singular or in the aggregate, shall be governed by the laws of the State without regard to application of choice of law principles. Pursuant to 74 O.S. §85.14, where federal granted funds are involved, applicable federal laws, rules and regulations shall govern to the extent necessary to insure benefit of such federal funds to the State. Venue for any action, claim, dispute, or litigation relating in any way to the Contract Documents, shall be in Oklahoma County, Oklahoma.

26.2 No Guarantee of Products or Services Required

The State shall not guarantee any minimum or maximum amount of Supplier products or services required under the Contract.

26.3 Employment Relationship

The Contract does not create an employment relationship. Individuals providing products or performing services pursuant to the Contract are not employees of the State or Customer and, accordingly are not eligible for any rights or benefits whatsoever accruing to such employees.

26.4 Transition Services

If transition services are needed at the time of Contract expiration or termination, Supplier shall provide such services on a month-to-month basis, at the contract rate or other mutually agreed rate. Supplier shall provide a proposed transition plan, upon request, and cooperate with any successor supplier and with establishing a mutually agreeable transition plan. Failure to cooperate may be documented as poor performance of Supplier.

26.5 Publicity

The existence of the Contract or any Acquisition is in no way an endorsement of Supplier, the products or services and shall not be so construed by Supplier in any advertising or publicity materials. Supplier agrees to submit to the State all advertising, sales, promotion, and other publicity matters relating to the Contract wherein the name of the State or any Customer is mentioned or language used from which, in the State's judgment, an endorsement may be inferred or implied. Supplier further agrees not to publish or use such advertising, sales promotion, or publicity matter or release any informational pamphlets, notices, press releases, research reports, or similar public notices concerning the Contract or any Acquisition hereunder without obtaining the prior written approval of the State.

26.6 Open Records Act

Supplier acknowledges that all State agencies and certain other Customers are subject to the Oklahoma Open Records Act set forth at 51 O.S. §24A-1 *et seq.* Supplier also acknowledges that compliance with the Oklahoma Open Records Act and all opinions of the Oklahoma Attorney General concerning the Act is required.

26.7 Failure to Enforce

Failure by the State or a Customer at any time to enforce a provision of, or exercise a right under, the Contract shall not be construed as a waiver of any such provision. Such failure to enforce or exercise shall not affect the validity of any Contract Document, or any part thereof, or the right of the State or a Customer to enforce any provision of, or exercise any right under, the Contract at any time in accordance with its terms. Likewise, a waiver of a breach of any provision of a Contract Document shall not affect or waive a subsequent breach of the same provision or a breach of any other provision in the Contract.

26.8 Mutual Responsibilities

- A.** No party to the Contract grants the other the right to use any trademarks, trade names, other designations in any promotion or publication without the express written consent by the other party.
- B.** The Contract is a non-exclusive contract and each party is free to enter into similar agreements with others.
- C.** The Customer and Supplier each grant the other only the licenses and rights specified in the Contract and all other rights and interests are expressly reserved.
- D.** The Customer and Supplier shall reasonably cooperate with each other and any Supplier to which the provision of a product and/or service under the Contract may be transitioned after termination or expiration of the Contract.
- E.** Except as otherwise set forth herein, where approval, acceptance, consent, or similar action by a party is required under the Contract, such action shall not be unreasonably delayed or withheld.

26.9 Invalid Term or Condition

To the extent any term or condition in the Contract conflicts with a compulsory applicable State or United States law or regulation, such Contract term or

condition is void and unenforceable. By executing any Contract Document which contains a conflicting term or condition, no representation or warranty is made regarding the enforceability of such term or condition. Likewise, any applicable State or federal law or regulation which conflicts with the Contract or any non-conflicting applicable State or federal law or regulation is not waived.

26.10 Severability

If any provision of a Contract Document, or the application of any term or condition to any party or circumstances, is held invalid or unenforceable for any reason, the remaining provisions shall continue to be valid and enforceable and the application of such provision to other parties or circumstances shall remain valid and in full force and effect. If a court finds that any provision of this contract is invalid or unenforceable, but that by limiting such provision it would become valid and enforceable, then such provision shall be deemed to be written, construed, and enforced as so limited.

26.11 Section Headings

The headings used in any Contract Document are for convenience only and do not constitute terms of the Contract.

26.12 Sovereign Immunity

Notwithstanding any provision in the Contract, the Contract is entered into subject to the State's Constitution, statutes, common law, regulations, and the doctrine of sovereign immunity, none of which are waived by the State nor any other right or defense available to the State.

26.13 Survival

As applicable, performance under all license, subscription, service agreements, statements of work, transition plans and other similar Contract Documents entered into between the parties under the terms of the Contract shall survive Contract expiration. Additionally, rights and obligations under the Contract which by their nature should survive including, without limitation, certain payment obligations invoiced prior to expiration or termination; confidentiality obligations; security incident and data breach obligations and indemnification obligations, remain in effect after expiration or termination of the Contract.

26.14 Entire Agreement

The Contract Documents taken together as a whole constitute the entire agreement between the parties. No statement, promise, condition,

understanding, inducement or representation, oral or written, expressed or implied, which is not contained in a Contract Document shall be binding or valid. The Supplier's representations and certifications, including any completed electronically, are incorporated by reference into the Contract.

26.15 Gratuities

The Contract may be immediately terminated, in whole or in part, by written notice if it is determined that the Supplier, its employee, agent, or another representative violated any federal, State or local law, rule or ordinance by offering or giving a gratuity to any State employee directly involved in the Contract. In addition, Suspension or Debarment of the Supplier may result from such a violation.

26.16 Import/Export Controls

Neither party will use, distribute, transfer or transmit any equipment, services, software or technical information provided under the Contract (even if incorporated into other products) except in compliance with all applicable import and export laws, conventions and regulations.

ATTACHMENT C
AGENCY TERMS
SOLICITATION NO. 0900000550

1. Statewide Contract Type

- 1.1** The Contract is a non-mandatory statewide contract for use by State agencies. Additionally, the Contract may be used by any governmental entity specified as a political subdivision of the State pursuant to the Governmental Tort Claims Act including any associated institution, instrumentality, board, commission, committee, department or other entity designated to act on behalf of the political subdivision; a state, county or local governmental entity in its state of origin; and entities authorized to utilize contracts by the State via a multistate or multigovernmental contract.
- 1.2** The Contract is a firm, fixed price contract for indefinite delivery and quantity for the Acquisitions available under the Contract.

2. Orders and Addendums

- 2.1** Unless mutually agreed in writing otherwise, orders shall be placed directly with the Supplier by issuance of written purchase orders or by Purchase Card by state agencies and other authorized entities. All orders are subject to the Contract terms and any order dated prior to Contract expiration shall be performed. Delivery to multiple destinations may be required.
- 2.2** Any ordering document shall be effective between Supplier and the Customer only and shall not be an Addendum to the Contract in its entirety or apply to any Acquisition by another Customer.
- 2.3** Additional terms added to a Contract Document by a Customer shall be effective if the additional terms do not conflict with the General Terms and are acceptable to Supplier. However, an Addendum to the Contract shall be signed by the State Purchasing Director or designee. Regarding information technology and telecommunications contracts, pursuant to 62 O.S., §34.11.1, the Chief Information Officer acts as the Information Technology and Telecommunications Purchasing Director.

3. Termination for Funding Insufficiency

In addition to Contract terms relating to termination due to insufficient funding, a Customer may terminate any purchase order or other payment mechanism if funds sufficient to pay obligations under the Contract are not appropriated or received from an intended third-party funding source. The determination by the Customer of insufficient funding shall be accepted by, and shall be final and binding on, the Supplier.

4. Termination for Cause

In addition to Contract terms relating to termination for cause, a customer may terminate its obligations, in whole or in part, to Supplier if it has provided Supplier with written notice of material breach and Supplier fails to cure such material breach within thirty (30) days of receipt of written notice. The Customer may also terminate a purchase order or other payment mechanism or Supplier's activities under the Contract immediately without a thirty (30) day written notice to Supplier, if Supplier fails to comply with confidentiality, privacy, security, environmental or safety requirements if such non-compliance relates or may relate to Supplier provision of products or services to the Customer or if Supplier's material breach is reasonably determined (i) to be an impediment to the function of the Customer and detrimental to the Customer, or (ii) when conditions preclude the thirty (30) day notice.

5. Termination for Convenience

In addition to any termination for convenience provisions in the Contract, a Customer may terminate a purchase order or other payment mechanism for convenience if it is determined that termination is in the Customer's best interest. Supplier will be provided at least thirty (30) days' written notice of termination.

6. Contract Management Fee and Usage Report

6.1 Pursuant to 74 O.S. § 85.33A, the State assesses a contract management fee on all transactions under a statewide contract. The payment of such fee will be calculated for all transactions, net of returns and the Supplier has no right of setoff against such fee regardless of the payment status of any Customer or any aggregate accounts receivable percentage. Supplier acknowledges and agrees that all prices quoted under any statewide contract shall include the contract management fee and the contract management fee shall not be reflected as a separate line item in Supplier's billing. The State reserves the

right to change this fee upward or downward upon sixty (60) calendar days' written notice to Supplier without further requirement for an Addendum.

6.2 While Supplier is the awardee of a statewide contract, transactions that occur under the terms of the statewide contract are subject to a one percent (1%) contract management fee to be paid by Supplier. Supplier shall submit a Contract Usage Report on a quarterly basis for each contract using a form provided by the State and such report shall include applicable information for each transaction. Reports shall include usage of the statewide contract by every Customer during the applicable quarter. A singular report provided late will not be considered a breach of the statewide contract; provided, however, repeated failure to submit accurate quarterly usage reports and submit timely payments may result in suspension or termination, in whole or in part, of the Contract.

6.3 All Contract Usage Reports shall meet the following criteria:

- i.** Electronic submission in Microsoft Excel format to strategic.sourcing@omes.ok.gov;
- ii.** Quarterly submission regardless of whether there were transactions under the Contract during the applicable quarterly reporting period;
- iii.** Submission no later than forty-five (45) days following the end of each calendar quarter;
- iv.** Contract quarterly reporting periods shall be as follows:
 - a.** January 01 through March 31;
 - b.** April 01 through June 30;
 - c.** July 01 through September 30; and
 - d.** October 01 through December 31.
- v.** Reports must include the following information:
 - a.** Procuring entity;
 - b.** Order date;

- c. Purchase Order number or note that the transaction was paid by Purchase Card;
- d. City in which products or services were received or specific office or subdivision title;
- e. Product manufacturer or type of service;
- f. Manufacturer item number, if applicable;
- g. Product description;
- h. General product category, if applicable;
- i. Quantity;
- j. Unit list price or MSRP, as applicable;
- k. Unit price charged to the purchasing entity; and
- l. Other Contract usage information requested by the State.

6.4 Payment of the contract management fee shall be delivered to the following address within forty-five (45) calendar days after the end of each quarterly reporting period:

State of Oklahoma
Office of Management and Enterprise Services, Central Purchasing
2401 North Lincoln Boulevard, Suite 116
Oklahoma City, Oklahoma 73105

To ensure payment is properly accounted for, Supplier shall provide the following information with payment: (i) reference to the applicable Contract Usage Report and quarterly reporting period and (ii) the applicable statewide contract number(s) and the amount of the contract management fee being paid for each contract number.

ATTACHMENT D

STATE OF OKLAHOMA INFORMATION TECHNOLOGY TERMS

The parties further agree to the following terms (“Information Technology Terms”), as applicable, for any Acquisition of products or services with an information technology or telecommunication component. Pursuant to the Oklahoma Information Technology Consolidation and Coordination Act (“The Act” or “Act”), OMES- Information Services (“OMES-IS”) is designated to purchase information technology and telecommunication products and services on behalf of the State. The Act directs OMES-IS to acquire necessary hardware, software and services and to authorize the use by other State agencies. OMES, as the owner of information technology and telecommunication assets and contracts on behalf of the State, allows other State agencies to use the assets while retaining ownership and the right to reassign the assets, at no additional cost, upon written notification to Supplier. OMES-IS is the data custodian for State agency data; however, such data is owned by the respective State agency.

1 DEFINITIONS

- 1.1 **Customer Data** means all data supplied by or on behalf of a Customer in connection with the Contract, excluding any confidential information of Supplier. Customer Data includes both Non-Public Data and Personal Data.
- 1.2 **Data Breach** means the unauthorized access or the reasonable suspicion of unauthorized access, by an unauthorized person that results in the use, destruction, loss, alteration, disclosure, or theft of Customer Data.
- 1.3 **Host** includes the terms Hosted or Hosting and means the accessing, processing or storing of Customer Data.
- 1.4 **Intellectual Property Rights** means the worldwide legal rights or interests evidenced by or embodied in any idea, design, concept, personality right, method, process, technique, apparatus, invention, discovery or improvement including any patents, trade secrets and know-how; any work of authorship including any copyrights, Moral Rights or neighboring rights; any trademark, service mark, trade dress, trade name or other indicia of source or origin; domain name registrations; and any other proprietary or similar rights. Intellectual Property Rights of a party also includes all worldwide legal rights or interests that the party may have acquired by assignment or license with the right to grant sublicenses.
- 1.5 **Non-Public Data** means Customer Data, other than Personal Data, that is not subject to distribution to the public as public information. It is deemed to be sensitive and confidential by Customer because it contains information that is exempt by statute, ordinance or administrative rule from access by the general public as public information. Non-Public Data includes any data deemed confidential pursuant to the Contract, otherwise identified by Customer as Non-Public Data, or that a reasonable person would deem confidential.
- 1.6 **Personal Data** means Customer Data that contains 1) any combination of an individual’s name, social security numbers, driver’s license, state/federal identification number,

account number, credit or debit card number and/or 2) data subject to protection under a federal, state or local law, rule, regulation or ordinance.

- 1.7 Security Incident** means the attempted or successful unauthorized access, use, disclosure, modification, loss, theft, or destruction of information or interference with the Hosted environment used to perform the services.
- 1.8 Supplier** means the Bidder with whom the State enters into the Contract awarded pursuant to the Solicitation or the business entity or individual that is a party to the Contract with the State. A Supplier with whom the State enters into an awarded Contract shall also be known as a Contractor.
- 1.9 Supplier Intellectual Property** means all tangible or intangible items or things, including the Intellectual Property Rights therein, created or developed by Supplier and identified in writing as such (a) prior to providing any services or Work Product to Customer and prior to receiving any documents, materials, information or funding from or on behalf of a Customer relating to the services or Work Product, or (b) after the effective date of the Contract if such tangible or intangible items or things were independently developed by Supplier outside Supplier's provision of services or Work Product for Customer under the Contract and were not created, prepared, developed, invented or conceived by any Customer personnel who then became personnel to Supplier or any of its affiliates or subcontractors, where, although creation or reduction-to-practice is completed while the person is affiliated with Supplier or its personnel, any portion of same was created, invented or conceived by such person while affiliated with Customer.
- 1.10 Third Party Intellectual Property** means the Intellectual Property Rights of any third party that is not a party to the Contract, and that is not directly or indirectly providing any goods or services to a Customer under the Contract.

2 TERMINATION OF MAINTENANCE AND SUPPORT SERVICES

Customer may terminate maintenance or support services without an adjustment charge, provided any of the following circumstances occur:

- 2.1** Customer removes the product for which the services are provided, from productive use; or,
- 2.2** The location at which the services are provided is no longer controlled by Customer (for example, because of statutory or regulatory changes or the sale or closing of a facility).
- 2.3** If Customer chooses to renew maintenance or support after maintenance has lapsed, Customer may choose to pay the additional fee, if any, associated with renewing a license after such maintenance or support has lapsed, or to purchase a new license. Any amount paid to Supplier in the form of prepaid fees that are unused when services under the Contract or purchase order are terminated shall be refunded to Customer.

3 COMPLIANCE AND ELECTRONIC AND INFORMATION TECHNOLOGY ACCESSIBILITY

- 3.1** State procurement of information technology is subject to certain federal and State laws, rules and regulations related to information technology accessibility, including but not limited to Oklahoma Information Technology Accessibility Standards (“Standards”) set forth at <https://oklahoma.gov/omes/services/information-services/is/policies-and-standards/accessibility-standards.html>. Supplier shall provide a Voluntary Product Accessibility Template (“VPAT”) describing accessibility compliance via a URL linking to the VPAT and shall update the VPAT as necessary in order to allow a Customer to obtain current VPAT information as required by State law. If products require development or customization, additional requirements and documentation may be required and compliance shall be necessary by Supplier. Such requirements may be stated in appropriate documents including but not limited to a statement of work, riders, agreement, purchase order or Addendum.

All representations contained in the VPAT provided will be relied upon by the State or a Customer, as applicable, for accessibility compliance purposes.

4 MEDIA OWNERSHIP (Disk Drive and/or Memory Chip Ownership)

- 4.1** Any disk drives and memory cards purchased with or included for use in leased or purchased products under the Contract remain the sole and exclusive property of the Customer.
- 4.2** Personal information may be retained within electronic media devices and components; therefore, electronic media shall not be released either between Customers or for the resale, of refurbished equipment that has been in use by a Customer, by the Supplier to the general public or other entities. This provision applies to replacement devices and components, whether purchased or leased, supplied by Supplier, its agents or subcontractors during the downtime (repair) of products purchased or leased through the Contract. If a device is removed from a location for repairs, the Customer shall have sole discretion, prior to removal, to determine and implement sufficient safeguards (such as a record of hard drive serial numbers) to protect personal information that may be stored within the hard drive or memory of the device.

5 OFFSHORE SERVICES

No offshore services are provided for under the Contract. State data shall not be used or accessed internationally for troubleshooting or any other use not specifically provided for herein without the prior written permission, which may be withheld in the State’s sole discretion, from the appropriate authorized representative of the State. Notwithstanding the above, back office administrative functions of the Supplier may be located offshore and the follow-the-sun support model may be used by the Supplier to the extent allowed by law applicable to any Customer data being accessed or used.

6 COMPLIANCE WITH TECHNOLOGY POLICIES

- 6.1** The Supplier agrees to adhere to the State of Oklahoma “Information Security Policy, Procedures, and Guidelines” available at <https://oklahoma.gov/content/dam/ok/en/omes/documents/InfoSecPPG.pdf>.

Supplier’s employees and subcontractors shall adhere to the applicable State IT

Standards, policies, procedures and architectures as set forth at <https://oklahoma.gov/omes/services/information-services.html> or as otherwise provided by the State.

- 6.2** Supplier shall comply with applicable Federal Information Processing Standards including, without limitation, FIPS 200, FIPS 140-2 or successor standards and all recommendations from the National Institute of Standards and Technology. The confidentiality of Customer Data shall be protected and maintained in accordance with these standards as well as other applicable Customer standards.

7 EMERGING TECHNOLOGIES

The State reserves the right to enter into an Addendum to the Contract at any time to allow for emerging technologies not identified elsewhere in the Contract Documents if there are repeated requests for such emerging technology or the State determines it is warranted to add such technology.

8 EXTENSION RIGHT

In addition to extension rights of the State set forth in the Contract, the State Chief Information Officer reserves the right to extend any Contract at his or her sole option if the State Chief Information Officer determine such extension to be in the best interest of the State.

9 SOURCE CODE ESCROW

Pursuant to 62 O.S. § 34.31, if customized computer software is developed or modified exclusively for a State agency, the Supplier has a continuing obligation to comply with such law and place the source code for such software and any modifications thereto into escrow with an independent third-party escrow agent. Supplier shall pay all fees charged by the escrow agent and enter into an escrow agreement, the terms of which are subject to the prior written approval of the State, including terms that provide the State receives ownership of all escrowed source code upon the occurrence of any of the following:

- 9.1** A bona fide material default of the obligations of the Supplier under the agreement with the applicable Customer;
- 9.2** An assignment by the Supplier for the benefit of its creditors;
- 9.3** A failure by the Supplier to pay, or an admission by the Supplier of its inability to pay, its debts as they mature;
- 9.4** The filing of a petition in bankruptcy by or against the Supplier when such petition is not dismissed within sixty (60) days of the filing date;
- 9.5** The appointment of a receiver, liquidator or trustee appointed for any substantial part of the Supplier's property;
- 9.6** The inability or unwillingness of the Supplier to provide the maintenance and support services in accordance with the agreement with the agency;
- 9.7** Supplier's ceasing of maintenance and support of the software; or

9.8 Such other condition as may be statutorily imposed by the future amendment or enactment of applicable Oklahoma law.

10 COMMERCIAL OFF THE SHELF SOFTWARE OR SUPPLIER TERMS

If Supplier specifies terms and conditions or clauses in an electronic license, subscription, maintenance, support or similar agreement, including via a hyperlink or uniform resource locator address to a site on the internet, that conflict with the terms of this Contract, the additional terms and conditions or conflicting clauses shall not be binding on the State and the provisions of this Contract shall prevail. Further, no such terms and conditions or clauses shall expand the State's or Customer's liability or reduce the rights of Customer or the State.

11 OWNERSHIP RIGHTS

Any software developed, modified, or customized by the Supplier in accordance with a mutually negotiated statement of work pursuant to this Contract is for the sole and exclusive use of the State including but not limited to the right to use, reproduce, re-use, alter, modify, edit, or change the software as it sees fit and for any purpose. The parties mutually agree the State as a licensee of the Supplier does not make a claim of ownership to the existing Intellectual Property of Supplier. Moreover, except with regard to any deliverable based on Supplier Intellectual Property, the State shall be deemed the sole and exclusive owner of all right, title, and interest therein, including but not limited to all source data, information and materials furnished to the State, together with all plans, system analysis, and design specifications and drawings, completed programs and documentation thereof, reports and listing, all data and test procedures and all other items pertaining to the work and services to be performed pursuant to this Contract including all copyright and proprietary rights relating thereto. With respect to Supplier Intellectual Property, the Supplier grants the State, for no additional consideration, a perpetual, irrevocable, royalty-free license, solely for the internal business use of the State, to use, copy, modify, display, perform, transmit and prepare derivative works of Supplier Intellectual Property embodied in or delivered to the State in conjunction with the products.

Except for any Supplier Intellectual Property, all work performed by the Supplier of developing, modifying or customizing software and any related supporting documentation shall be considered as Work for Hire (as defined under the U.S. copyright laws) and, as such, shall be owned by and for the benefit of State.

In the event that it should be determined that any portion of such software or related supporting documentation does not qualify as "Work for Hire", Supplier hereby irrevocably grants to the State, for no additional consideration, a non-exclusive, irrevocable, royalty-free license to use, copy, modify, display, perform, transmit and prepare derivative works of any such software and any Supplier Intellectual Property embodied in or delivered to the State in conjunction with the products.

Supplier shall assist the State and its agents, upon request, in preparing U.S. and foreign copyright, trademark, and/or patent applications covering software developed, modified or customized for the State when made in accordance with a mutually negotiated statement of work pursuant to this Contract. Supplier shall sign any such applications, upon request, and deliver them to the State. The State shall bear all expenses that incurred in connection with such copyright, trademark, and/or patent applications.

If any Acquisition pursuant to this Contract is funded wholly or in part with federal funds, the source code and all associated software and related documentation owned by the State may be shared with other publicly funded agencies at the discretion of the State without permission from or additional compensation to the Supplier.

12 INTELLECTUAL PROPERTY OWNERSHIP TO WORK PRODUCT

The following terms apply to ownership and rights related to Intellectual Property:

- 12.1** As to the Intellectual Property Rights to Work Product between Supplier and Customer, Customer shall be the exclusive owner and not Supplier. Supplier specifically agrees that the Work Product shall be considered “works made for hire” and that the Work Product shall, upon creation, be owned exclusively by Customer. To the extent that the Work Product, under applicable law, may not be considered works made for hire, Supplier agrees that all right, title and interest in and to all ownership rights and all Intellectual Property Rights in the Work Product is effectively transferred, granted, conveyed, assigned, and relinquished exclusively to Customer, without the necessity of any further consideration, and Customer shall be entitled to obtain and hold in its own name all Intellectual Property Rights in and to the Work Product. Supplier acknowledges that Supplier and Customer do not intend Supplier to be a joint author of the Work Product within the meaning of the Copyright Act of 1976. Customer shall have access, during normal business hours (Monday through Friday, 8:00 a.m. to 5:00 p.m.) and upon reasonable prior notice to Supplier, to all Supplier materials, premises and computer files containing the Work Product. Supplier and Customer, as appropriate, will cooperate with one another and execute such other documents as may be reasonably appropriate to achieve the objectives herein. No license or other right is granted under the Contract to any Third-Party Intellectual Property, except as may be incorporated in the Work Product by Supplier.
- 12.2** Supplier, upon request and without further consideration, shall perform any acts that may be deemed reasonably necessary or desirable by Customer to evidence more fully the transfer of ownership and/or registration of all Intellectual Property Rights in all Work Product to Customer to the fullest extent possible including, but not limited to, the execution, acknowledgement and delivery of such further documents in a form determined by Customer. In the event Customer shall be unable to obtain Supplier’s signature due to the dissolution of Supplier or Supplier’s failure to respond to Customer’s repeated requests for such signature on any document reasonably necessary for any purpose set forth in the foregoing sentence, Supplier hereby irrevocably designates and appoints Customer and its duly authorized officers and agents as Supplier’s agent and Supplier’s attorney-in-fact to act for and in Supplier’s behalf and stead to execute and file any such document and to do all other lawfully permitted acts to further any such purpose with the same force and effect as if executed and delivered by Supplier, provided however that no such grant of right to Customer is applicable if Supplier fails to execute any document due to a good faith dispute by Supplier with respect to such document. It is understood that such power is coupled with an interest and is therefore irrevocable. Customer shall have the full and sole power to prosecute such applications and to take all other action concerning the Work Product, and Supplier shall cooperate, at Customer’s sole expense, in the preparation and prosecution of all such applications and in any legal actions and proceedings concerning the Work Product.

- 12.3** Supplier hereby irrevocably and forever waives, and agrees never to assert, any Moral Rights in or to the Work Product which Supplier may now have or which may accrue to Supplier's benefit under U.S. or foreign copyright or other laws and any and all other residual rights and benefits which arise under any other applicable law now in force or hereafter enacted. Supplier acknowledges the receipt of equitable compensation for its assignment and waiver of such Moral Rights.
- 12.4** All documents, information and materials forwarded to Supplier by Customer for use in and preparation of the Work Product shall be deemed the confidential information of Customer, subject to the license granted by Customer to Supplier hereunder. Supplier shall not otherwise use, disclose, or permit any third party to use or obtain the Work Product, or any portion thereof, in any manner without the prior written approval of Customer.
- 12.5** These provisions are intended to protect Customer's proprietary rights pertaining to the Work Product and the Intellectual Property Rights therein and any misuse of such rights would cause substantial and irreparable harm to Customer's business. Therefore, Supplier acknowledges and stipulates that a court of competent jurisdiction may immediately enjoin a material breach of the Supplier's obligations with respect to confidentiality provisions of the Contract and the Work Product and a Customer's Intellectual Property Rights, upon a request by Customer, without requiring proof of irreparable injury, as same is presumed.
- 12.6** Upon the request of Customer, but in any event upon termination or expiration of this Contract or a statement of work, Supplier shall surrender to Customer all documents and things pertaining to the Work Product, generated or developed by Supplier or furnished by Customer to Supplier, including all materials embodying the Work Product, any Customer confidential information and Intellectual Property Rights in such Work Product, regardless of whether complete or incomplete. This section is intended to apply to all Work Product as well as to all documents and things furnished to Supplier by Customer or by anyone else that pertains to the Work Product.
- 12.7** Customer hereby grants to Supplier a non-transferable, non-exclusive, royalty-free, fully paid license to use any Work Product solely as necessary to provide services to Customer. Except as provided in this section, neither Supplier nor any subcontractor shall have the right to use the Work Product in connection with the provision of services to its other customers without the prior written consent of Customer, which consent may be withheld in Customer's sole discretion.
- 12.8** To the extent that any Third Party Intellectual Property is embodied or reflected in the Work Product or is necessary to provide services, Supplier shall obtain from the applicable third party for the Customer's benefit, an irrevocable, perpetual, non-exclusive, worldwide, royalty-free license, solely for Customer's internal business purposes; likewise, with respect to any Supplier Intellectual Property embodied or reflected in the Work Product or necessary to provide services, Supplier grants to Customer an irrevocable, perpetual, non-exclusive, worldwide, royalty-free license, solely for the Customer's internal business purposes. Each such license shall allow the applicable Customer to (i) use, copy, modify, display, perform (by any means), transmit and prepare derivative works of any Third Party Intellectual Property or Supplier Intellectual Property embodied in or delivered to Customer in conjunction with the Work

Product and (ii) authorize others to do any or all of the foregoing. Supplier agrees to notify Customer on delivery of the Work Product or services if such materials include any Third Party Intellectual Property. The foregoing license includes the right to sublicense third parties, solely for the purpose of engaging such third parties to assist or carry out Customer's internal business use of the Work Product. Except for the preceding license, all rights in Supplier Intellectual Property remain in Supplier. On request, Supplier shall provide Customer with documentation indicating a third party's written approval for Supplier to use any Third Party Intellectual Property that may be embodied or reflected in the Work Product.

12.9 Supplier agrees that it shall have written agreement(s) that are consistent with the provisions hereof related to Work Product and Intellectual Property Rights with any employees, agents, consultants, contractors or subcontractors providing services or Work Product pursuant to the Contract, prior to the provision of such services or Work Product and that it shall maintain such written agreements at all times during performance of this Contract which are sufficient to support all performance and grants of rights by Supplier. Copies of such agreements shall be provided to the Customer promptly upon request.

12.10 To the extent not inconsistent with Customer's rights in the Work Product or other provisions, nothing in this Contract shall preclude Supplier from developing for itself, or for others, materials which are competitive with those produced as a result of the services provided under the Contract, provided that no Work Product is utilized, and no Intellectual Property Rights of Customer therein are infringed by such competitive materials. To the extent that Supplier wishes to use the Work Product or acquire licensed rights in certain Intellectual Property Rights of Customer therein in order to offer competitive goods or services to third parties, Supplier and Customer agree to negotiate in good faith regarding an appropriate license and royalty agreement to allow for such.

12.11 If any Acquisition pursuant to the Contract is funded wholly or in part with federal funds, the source code and all associated software and related documentation and materials owned by a Customer may be shared with other publicly funded agencies at the discretion of such Customer without permission from or additional compensation to the Supplier.

13 HOSTING SERVICES

A Supplier shall be responsible for the obligations set forth in in this Contract, including those obligations related to breach reporting and associated costs when a Supplier Hosting Customer Data or providing products or services pursuant to an Acquisition, contributes to, or directly causes a Data Breach or a Security Incident. Likewise, Supplier shall be responsible for the obligations set forth in in this Contract, including those obligations related to breach reporting and associated costs when a Supplier's affiliate or subcontractor contributes to, or directly causes a Data Breach or a Security Incident.

14 CHANGE MANAGEMENT

When a scheduled change is made to products or services provided to a Customer that impacts the Customer's system related to such product or service, Supplier shall provide two (2) weeks' prior written notice of such change. When the change is an emergency change, Supplier shall provide twenty-four (24) hours' prior written notice of the change. Repeated failure to provide such notice may be an evaluation factor (as indicative of Supplier's past performance) upon

renewal or if future bids submitted by Supplier are evaluated by the State.

15 SERVICE LEVEL DEFICIENCY

In addition to other terms of the Contract, in instances of the Supplier's repeated failure to provide an acceptable level of service or meet service level agreement metrics, service credits shall be provided by Supplier and may be used as an offset to payment due.

16 OWNERSHIP OF IT AND TELECOMMUNICATION ASSETS

Notwithstanding any other provision in the Contract and pursuant to the Oklahoma Information Technology Consolidation and Coordination Act, all information technology and telecommunication assets and contracts on behalf of appropriated agencies of the State belong to OMES-IS. OMES-IS allows other State agencies to use the assets while retaining ownership and the right to reassign the assets, at no additional cost, upon written notification to Supplier.

17 CUSTOMER DATA

17.1 The parties agree to the following provisions in connection with any Customer Data accessed, processed transmitted, or stored by or on behalf of the Supplier and the obligations, representations and warranties set forth below shall continue as long as the Supplier has an obligation under the Contract.

17.2 Customer will be responsible for the accuracy and completeness of all Customer Data provided to Supplier by Customer. Customer shall retain exclusive ownership of rights, title, and interest in Customer Data. Non-Public Data and Personal Data shall be deemed to be Customer's confidential information. Supplier shall restrict access to Customer Data to their employees with a need to know (and advise such employees of the confidentiality and non-disclosure obligations assumed herein).

17.3 Supplier shall promptly notify the Customer upon receipt of any requests from unauthorized third parties which in any way might reasonably require access to Customer Data or Customer's use of the Hosted environment. Supplier shall notify the Customer by the fastest means available and also in writing pursuant to Contract notice provisions and the notice provision herein. Except to the extent required by law, Supplier shall not respond to subpoenas, service or process, Freedom of Information Act or other open records requests, and other legal request related to Customer without first notifying the Customer and obtaining the Customer's prior approval, which shall not be unreasonably withheld, of Supplier's proposed responses. Supplier agrees to provide its completed responses to the Customer with adequate time for Customer review, revision and approval.

17.4 Supplier will use commercially reasonable efforts to prevent the loss of or damage to Customer Data in its possession and will maintain commercially reasonable back-up procedures and copies to facilitate the reconstruction of any Customer Data that may be lost or damaged by Supplier. Supplier will promptly notify Customer of any loss, damage to, or unauthorized access of Customer Data. Supplier will use commercially reasonable efforts to reconstruct any Customer Data that has been lost or damaged by Supplier as a result of its negligence or willful misconduct. If Customer Data is lost or damaged for reasons other than as a result of Supplier's negligence or willful misconduct, Supplier, at

the Customer's expense, will, at the request of the State, use commercially reasonable efforts to reconstruct any Customer Data lost or damaged.

18 DATA SECURITY

- 18.1** Supplier will use commercially reasonable efforts, consistent with industry standards, to provide security for the Hosted environment and Customer Data and to protect against both unauthorized access to the Hosting environment, and unauthorized communications between the Hosting environment and the Customer's browser. Supplier shall implement and maintain appropriate administrative, technical and organizational security measures to safeguard against unauthorized access, disclosure or theft of Personal Data and Non-Public Data. Such security measures shall be in accordance with recognized industry practice and not less stringent than the measures the service provider applies to its own personal data and non-public data of similar kind.
- 18.2** All Personal Data and Non-public Data shall be encrypted at rest and in transit with controlled access. Unless otherwise stipulated, the service provider is responsible for encryption of Personal Data. All Personal Data and Non-Public Data shall be subject to controlled access. Any stipulation of responsibilities shall be included in a Statement of Work and will identify specific roles and responsibilities.
- 18.3** Supplier represents and warrants to the Customer that the Hosting equipment and environment will be routinely checked with a commercially available, industry standard software application with up-to-date virus definitions. Supplier will regularly update the virus definitions to ensure that the definitions are as up-to-date as is commercially reasonable. Supplier will promptly purge all viruses discovered during virus checks. If there is a reasonable basis to believe that a virus may have been transmitted to Customer by Supplier, Supplier will promptly notify Customer of such possibility in a writing that states the nature of the virus, the date on which transmission may have occurred, and the means Supplier has used to remediate the virus. Should the virus propagate to Customer's IT infrastructure, Supplier is responsible for costs incurred by Customer for Customer to remediate the virus.
- 18.4** At no time shall any Customer Data or processes – that either belong to or are intended for the use of the State - be copied, disclosed, or retained by Supplier or any party related to Supplier for subsequent use in any transaction that does not include the State unless otherwise agreed to by the State.
- 18.5** Supplier shall provide its services to Customer and its users solely from data centers in the U.S. Storage of Customer Data at rest shall be located solely in data centers in the U.S. Supplier shall not allow its personnel or contractors to store Customer Data on portable devices, including personal computers, except for devices that are used and kept only at its U.S. data centers. Supplier shall permit its personnel and contractors to access Customer Data remotely only as required to fulfill Supplier's obligations under the Contract.
- 18.6** Supplier shall allow the Customer to audit conformance to the Contract terms. The Customer may perform this audit or contract with a third party at its discretion and at Customer's expense.

- 18.7** Supplier shall perform an independent audit of its data centers at least annually at its expense and provide a redacted version of the audit report upon request. Supplier may remove its proprietary information from the redacted version. A Service Organization Control (SOC) 2 audit report or approved equivalent sets the minimum level of a third-party audit.
- 18.8** Any remedies provided are not exclusive and are in addition to other rights and remedies available under the terms of the Contract, at law or in equity.

19 SECURITY ASSESSMENT

- 19.1** The State requires any entity or third-party Supplier Hosting Oklahoma Customer Data to submit to a State Certification and Accreditation Review process to assess initial security risk. Supplier submitted to the review and met the State's minimum security standards at time the Contract was executed. Failure to maintain the State's minimum security standards during the term of the contract, including renewals, constitutes a material breach. Upon request, the Supplier shall provide updated data security information in connection with a potential renewal. If information provided in the security risk assessment changes, Supplier shall promptly notify the State and include in such notification the updated information; provided, however, Supplier shall make no change that results in lessened data protection or increased data security risk. Failure to provide the notice required by this section or maintain the level of security required in the Contract constitutes a material breach by Supplier and may result in a whole or partial termination of the Contract.
- 19.2** Any Hosting entity change must be approved in writing prior to such change. To the extent Supplier requests a different sub-contractor than the third-party Hosting Supplier already approved by the State, the different sub-contractor is subject to the State's approval. Supplier agrees not to migrate State's data or otherwise utilize the different third-party Hosting Supplier in connection with key business functions that are Supplier's obligations under the contract until the State approves the third-party Hosting Supplier's State Certification and Accreditation Review, which approval shall not be unreasonably withheld or delayed. In the event the third-party Hosting Supplier does not meet the State's requirements under the State Certification and Accreditation Review, Supplier acknowledges and agrees it will not utilize the third-party Supplier in connection with key business functions that are Supplier's obligations under the contract, until such third party meets such requirements.

20 SECURITY INCIDENT OR DATA BREACH NOTIFICATION

- 20.1** Supplier shall inform Customer of any Security Incident or Data Breach.
- 20.2** Supplier may need to communicate with outside parties regarding a Security Incident, which may include contacting law enforcement, fielding media inquiries and seeking external expertise as mutually agreed upon, defined by law or contained in the Contract. If a Security Incident involves Customer Data, Supplier will coordinate with Customer prior to any such communication.
- 20.3** Supplier shall report a Security Incident to the Customer identified contact set forth herein within five (5) days of discovery of the Security Incident or within a shorter notice

period required by applicable law or regulation (i.e., HIPAA requires notice to be provided within 24 hours).

20.4 Supplier shall maintain processes and procedures to identify, respond to and analyze Security Incidents; (ii) make summary information regarding such procedures available to Customer at Customer's request, (iii) mitigate, to the extent practicable, harmful effects of Security Incidents that are known to Vendor; and (iv) documents all Security Incidents and their outcomes.

20.5 If Supplier has reasonable belief or actual knowledge of a Data Breach, Supplier shall (1) promptly notify the appropriate Customer identified contact set forth herein within 24 hours or sooner, unless shorter time is required by applicable law, and (2) take commercially reasonable measures to address the Data Breach in a timely manner.

21 DATA BREACH NOTIFICATION AND RESPONSIBILITIES

This section only applies when a Data Breach occurs with respect to Personal Data or Non-Public Data within the possession or control of Supplier.

21.1 Supplier shall (1) cooperate with Customer as reasonably requested by Customer to investigate and resolve the Data Breach, (2) promptly implement necessary remedial measures, if necessary, and (3) document responsive actions taken related to the Data Breach, including any post-incident review of events and actions taken to make changes in business practices in providing the services, if necessary.

21.2 Unless otherwise stipulated, if a Data Breach is a direct result of Supplier's breach of its obligation to encrypt Personal Data and Non-Public Data or otherwise prevent its release, Supplier shall bear the costs associated with (1) the investigation and resolution of the Data Breach; (2) notifications to individuals, regulators or others required by state law; (3) credit monitoring services required by state or federal law; (4) a website or toll-free numbers and call center for affected individuals required by state law – all not to exceed the agency per record per person cost calculated for data breaches in the United States on the most recent Cost of Data breach Study: Global Analysis published by the Ponemon Institute at the time of the data breach; and (5) complete all corrective actions as reasonably determined by Supplier based on root cause.

21.3 If a Data Breach is a direct result of Supplier's breach of its obligations to encrypt Personal Data and Non-Public Data or otherwise prevent its release, Supplier shall indemnify and hold harmless the Customer against all penalties assessed to Indemnified Parties by governmental authorities in connection with the Data Breach.

22 SUPPLIER REPRESENTATIONS AND WARRANTIES

Supplier represents and warrants the following:

22.1 The product and services provided in connection with Hosting services do not infringe a third party's patent or copyright or other intellectual property rights.

22.2 Supplier will protect Customer's Non-Public Data and Personal Data from unauthorized dissemination and use with the same degree of care that each such party uses to protect

its own confidential information and, in any event, will use no less than a reasonable degree of care in protecting such confidential information.

22.3 The execution, delivery and performance of the Contract and any ancillary documents and the consummation of the transactions contemplated by the Contract or any ancillary documents by Supplier will not violate, conflict with, or result in a breach of any provision of, or constitute a default (or an event which, with notice or lapse of time or both, would constitute a default) under, or result in the termination of, any written contract or other instrument between Supplier and any third parties retained or utilized by Supplier to provide goods or services for the benefit of the Customer.

22.4 Supplier shall not knowingly upload, store, post, e-mail or otherwise transmit, distribute, publish or disseminate to or through the Hosting environment any material that contains software viruses, malware or other surreptitious code designed to interrupt, destroy or limit the functionality of any computer software or hardware or telecommunications equipment or circumvent any “copy-protected” devices, or any other harmful or disruptive program.

23 INDEMNITY

Supplier agrees to defend, indemnify and hold the State, its officers, directors, employees, and agents harmless from all liabilities, claims, damages, losses, costs, expenses, demands, suits and actions (including without limitation reasonable attorneys’ fees and costs required to establish the right to indemnification), excluding damages that are the sole fault of Customer, arising from or in connection with Supplier’s breach of its express representations and warranties in these Information Technology Terms and the Contract. If a third party claims that any portion of the products or services provided by Supplier under the terms of another Contract Document or these Information Technology Terms infringes that party’s patent or copyright, Supplier shall defend, indemnify and hold harmless the State and Customer against the claim at Supplier’s expense and pay all related costs, damages, and attorney’s fees incurred by or assessed to, the State and/or Customer. The State and/or Customer shall promptly notify Supplier of any third-party claims and to the extent authorized by the Attorney General of the State, allow Supplier to control the defense and any related settlement negotiations. If the Attorney General of the State does not authorize sole control of the defense and settlement negotiations to Supplier, Supplier shall be granted authorization to equally participate in any proceeding related to this section, but Supplier shall remain responsible to indemnify Customer and the State for all associated costs, damages and fees incurred by or assessed to the State and/or Customer. Should the software become, or in Supplier’s opinion, be likely to become the subject of a claim or an injunction preventing its use as contemplated in connection with Hosting services, Supplier may, at its option (i) procure for the State the right to continue using the software or (ii) replace or modify the software with a like or similar product so that it becomes non-infringing.

24 TERMINATION, EXPIRATION AND SUSPENSION OF SERVICE

24.1 During any period of service suspension, Supplier shall not take any action to intentionally disclose, alter or erase any Customer Data.

24.2 In the event of a termination or expiration of the Contract, the parties further agree:

Supplier shall implement an orderly return of Customer Data in a format specified by the Customer and, as determined by the Customer:

- a. return the Customer Data to Customer at no additional cost, at a time agreed to by the parties and the subsequent secure disposal of State Data;
- b. transitioned to a different Supplier at a mutually agreed cost and in accordance with a mutually agreed data transition plan and the subsequent secure disposal of State Data or
- c. a combination of the two immediately preceding options.

24.3 Supplier shall not take any action to intentionally erase any Customer Data for a period of:

- a. 10 days after the effective date of termination, if the termination is in accordance with the contract period;
- b. 30 days after the effective date of termination, if the termination is for convenience; or
- c. 60 days after the effective date of termination if the termination is for cause.

After such period, Supplier shall, unless legally prohibited or otherwise stipulated, delete all Customer Data in its systems or otherwise in its possession or under its control.

24.4 The State shall be entitled to any post termination or expiration assistance generally made available with respect to the services.

24.5 Disposal by Supplier of Customer Data in all of its forms, such as disk, CD/DVD, backup tape and paper, when requested by the Customer, shall be performed in a secure manner. Data shall be permanently deleted and shall not be recoverable, according to National Institute of Standards and Technology (NIST)-approved methods. Certificates of destruction shall be provided to Customer within thirty (30) calendar day of its request for disposal of data.

25 GENERAL INFORMATION SECURITY REQUIREMENTS

25.1 No employee of Contractor or its subcontractors will be granted access to State of Oklahoma agency information systems without the prior completion and approval of applicable logon authorization and acceptable use requests.

25.2 Contractor or its subcontractors will notify applicable State of Oklahoma agencies when employees who have access to agency information systems are terminated.

25.3 Contractor or its subcontractors will disclose to Client any suspected breach of the security of the information system or the data contained therein in the most expedient time possible and without unreasonable delay and will cooperate with Client during the investigation of any such incident.

- 25.4** Contractor or its subcontractors agree to adhere to the State of Oklahoma “Information Security Policy, Procedures, and Guidelines” available at: <https://oklahoma.gov/content/dam/ok/en/omes/documents/InfoSecPPG.pdf>

26 HIPAA REQUIREMENTS

- 26.1** Contractor shall agree to use and disclose Protected Health Information in its possession or control in compliance with the Standards for Privacy of Individually Identifiable Health Information (Privacy Rule) (45 C.F.R. Parts 160 and 164) under the Health Insurance Portability and Accountability Act (HIPAA) of 1996. The definitions set forth in the Privacy Rule are incorporated by reference into this Contract (45 C.F.R. §§ 160.103 and 164.501).

- 26.2** If applicable, Contractor will sign and adhere to a Business Associate Agreement (BAA). The Business Associate Agreement provides for satisfactory assurances that Contractor will use the information only for the purposes for which it was engaged. Contractor agrees it will safeguard the information from misuse and will comply with HIPAA as it pertains to the duties stated within the contract. Failure to comply with the requirements of this standard may result in funding being withheld from Contractor, and/or full audit and inspection of Contractor’s security compliance as it pertains to this contract.

26.3 Business Associate Terms Definitions:

- a. Unless otherwise defined in this BAA, all capitalized terms used in this BAA have the meanings ascribed in the HIPAA Regulations, provided; however, that “PHI” and “ePHI” shall mean Protected Health Information and Electronic Protected Health Information, respectively, as defined in 45 C.F.R. § 160.103, limited to the information Business Associate received from or created or received on behalf of the applicable State of Oklahoma agency as a Business Associate. “Administrative Safeguards” shall have the same meaning as the term “administrative safeguards in 45 C.F.R. § 164.304, with the exception that it shall apply to the management of the conduct of Business Associate’s workforce, not the State of Oklahoma agency workforce, in relation to the protection of that information.
- b. Business Associate. “Business Associate” shall generally have the same meaning as the term “Business Associate” at 45 C.F.R. 160.103, and in reference to the party to this agreement, shall mean the entity whose name appears below.
- c. Covered Entity. “Covered Entity” shall generally have the same meaning as the term “Covered Entity” at 45 C.F.R. 160.103.
- d. HIPAA Rules. “HIPAA Rules” shall mean the Privacy, Security, Breach Notification, and Enforcement Rules at 45 C.F.R. Part 160 and Part 164, all as may be amended.
- e. The following terms used in this Agreement shall have the same meaning as those terms in the HIPAA Rules: Breach, Data Aggregation, Designated Record Set, Disclosure, Health Care Operations, Individual, Minimum Necessary, Notice of

Privacy Practices, Protected Health Information, required by law, Secretary, Security Incident, Sub-Contractor, Unsecured PHI, and Use.

26.4 Obligations of Business Associate: Business Associate may use Electronic PHI and PHI (collectively, “PHI”) solely to perform its duties and responsibilities under this Agreement and only as provided in this Agreement. Business Associate acknowledges and agrees that PHI is confidential and shall not be used or disclosed, in whole or in part, except as provided in this Agreement or as required by law. Specifically, Business Associate agrees it will, as applicable:

- a. use or further disclose PHI only as permitted in this Agreement or as Required by Law, including, but not limited to the Privacy and Security Rule;
- b. use appropriate safeguards, and comply with Subpart C of 45 C.F.R. Part 164 with respect to Electronic PHI, to prevent use or disclosure of PHI other than as provided for by this Agreement;
- c. implement and document appropriate administrative, physical, and technical safeguards to protect the confidentiality, integrity, and availability of PHI that it creates, receives, maintains, or transmits for or on behalf of Covered Entity in accordance with 45 C.F.R. 164;
- d. implement and document administrative safeguards to prevent, detect, contain, and correct security violations in accordance with 45 C.F.R. 164;
- e. make its applicable policies and procedures required by the Security Rule available to Covered Entity solely for purposes of verifying BA’s compliance and the Secretary of the Department of Health and Human Services (HHS);
- f. not receive remuneration from a third party in exchange for disclosing PHI received from or on behalf of Covered Entity;
- g. in accordance with 45 C.F.R. 164.502(e)(1) and 164.308(b), if applicable, require that any Sub-Contractors that create, receive, maintain or transmit PHI on behalf of the Business Associate agree to the same restrictions, conditions, and requirements that apply to the Business Associate with respect to such information; this shall be in the form of a written HIPAA Business Associate Contract and a fully executed copy will be provided to the Contract Monitor;
- h. report to Covered Entity in writing any use or disclosure of PHI that is not permitted under this Agreement as soon as reasonably practicable but in no event later than five calendar days from becoming aware of it and mitigate, to the extent practicable and in cooperation with Covered Entity, any harmful effects known to it of a use or disclosure made in violation of this Agreement;
- i. promptly report to Covered Entity in writing and without unreasonable delay and in no case later than five calendar days any successful Security Incident, as defined in the Security Rule, with respect to Electronic PHI;
- j. with the exception of law enforcement delays that satisfy the requirements of 45 C.F.R. 164.412, notify Covered Entity promptly, in writing and without

unreasonable delay and in no case later than five calendar days, upon the discovery of a breach of Unsecured PHI. Such notice shall include, to the extent possible, the name of each individual whose Unsecured PHI has been, or is reasonably believed by Business Associate to have been, accessed, acquired, or disclosed during such Breach. Business Associate shall also, to the extent possible, furnish Covered Entity with any other available information that Covered Entity is required to include in its notification to Individuals under 45 C.F.R. § 164.404(c) at the time of Business Associate's notification to Covered Entity or promptly thereafter as such information becomes available. As used in this Section, "breach" shall have the meaning given such term at 45 C.F.R. 164.402;

- k. to the extent allowed by law, indemnify and hold Covered Entity harmless from all claims, liabilities costs, and damages arising out of or in any manner related to the unauthorized disclosure by Business Associate of any PHI resulting from the negligent acts or omissions of Business Associate or to the breach by Business Associate of any applicable obligation related to PHI;
- l. provide access to PHI it maintains in a Designated Record Set to Covered Entity, or if directed by Covered Entity to an Individual in order to meet the requirements of 45 C.F.R. 164.524. In the event that any Individual requests access to PHI directly from Business Associate, Business Associate shall forward such request to Covered Entity within five working days of receiving a request. This shall be in the form of a written HIPAA Business Associate Contract and a fully executed copy will be provided to the Contract Monitor. Any denials of access to the PHI requested shall be the responsibility of Covered Entity;
- m. make PHI it maintains in a Designated Record Set available to Covered Entity for amendment and incorporate any amendments to PHI in accordance with 45 C.F.R. 164.526;
- n. document disclosure of PHI it maintains in a Designated Record Set and information related to such disclosure as would be required for Covered Entity to respond to a request by an Individual for an accounting of disclosures of PHI, in accordance with 45 C.F.R. 164.528, and within five working days of receiving a request from Covered Entity, make such disclosure documentation and information available to Covered Entity. In the event the request for an accounting is delivered directly to Business Associate, Business Associate shall forward within five working days of receiving a request such request to Covered Entity;
- o. make its internal practices, books, and records related to the use and disclosure of PHI received from or created or received by Business Associate on behalf of Covered Entity available to the Secretary of the Department of HHS, authorized governmental officials, and Covered entity for the purpose of determining Business Associate's compliance with the Privacy Rule. Business Associate shall give Covered Entity advance written notice of requests from HHS or government officials and provide Covered Entity with a copy of all documents made available; and

- p. require that all of its Sub-Contractors, vendors, and agents to whom it provides PHI or who create, receive, use, disclose, maintain, or have access to Covered Entity's PHI shall agree in writing to requirements, restrictions, and conditions at least as stringent as those that apply to Business Associate under this Agreement, including but not limited to implementing reasonable and appropriate safeguards to protect PHI, and shall require that its Sub-Contractors, vendors, and agents agree to indemnify and hold harmless Covered Entity for their failure to comply with each of the provisions of this Agreement.

26.5 Permitted Uses and Disclosures of PHI by Business Associate: Except as otherwise provided in this Agreement, Business Associate may use or disclose PHI on behalf of or to provide services to Covered Entity for the purposes specified in this Agreement, if such use or disclosure of PHI would not violate the Privacy Rule if done by Covered Entity. Unless otherwise limited herein, Business Associate may:

- a. use PHI for its proper management and administration or to fulfill any present or future legal responsibilities of Business Associate;
- b. disclose PHI for its proper management and administration or to fulfill any present or future legal responsibilities of Business Associate, provided that; (i) the disclosures required by law; or (ii) Business Associate obtains reasonable assurances from any person to whom the PHI is disclosed that such PHI will be kept confidential and will be used or further disclosed only as Required by Law or for the purpose(s) for which it was disclosed to the person, and the person commits to notifying Business Associate of any instances of which it is aware in which the confidentiality of the PHI has been breached;
- c. disclose PHI to report violations of law to appropriate federal and state authorities; or
- d. aggregate the PHI with other data in its possession for purposes of Covered Entity's Health Care Operations;
- e. make uses and disclosures and requests for protected health information consistent with Covered Entity's minimum necessary policies and procedures;
- f. de-identify any and all PHI obtained by Business Associate under this BAA, and use such de-identified data, all in accordance with the de-identification requirements of the Privacy Rule [45 C.F.R. § 164.514(d)(1)].

26.6 Obligations of Covered Entity

- a. Covered Entity shall notify Business Associate of any changes in, or revocation of, the permission by an individual to use or disclose his or her PHI, to the extent that such changes may affect Business Associate's use or disclosure of PHI.
- b. Covered Entity shall notify Business Associate of any restriction on the use or disclosure of PHI that Covered Entity has agreed to or is required to abide by under 45 C.F.R. 164.522, to the extent that such restriction may affect Business Associate's use or disclosure of protected health information.

- c. Covered Entity shall not request Business Associate use or disclose PHI in any manner that would violate the Privacy Rule if done by Covered Entity.
- d. Covered Entity agrees to timely notify Business Associate, in writing, of any arrangements between Covered Entity and the Individual that is the subject of PHI that may impact in any manner the use and/or disclosure of the PHI by Business Associate under this BAA.
- e. Covered Entity shall provide the minimum necessary PHI to Business Associate.

26.7 Term and Termination:

- a. Obligations of Business Associate upon Termination. Upon termination of this Agreement for any reason, Business Associate, with respect to PHI received from Covered Entity, or created, maintained, or received by Business Associate on behalf of Covered Entity, shall as applicable:
 - i. retain only that PHI that is necessary for Business Associate to continue its proper management and administration or to carry out its legal responsibilities;
 - ii. return to Covered Entity (or, if agreed to by Covered Entity, destroy) the remaining PHI that the Business Associate still maintains in any form;
 - iii. continue to use appropriate safeguards and comply with Subpart C of 45 C.F.R. Part 164 with respect to PHI to prevent use or disclosure of the PHI, other than as provided for in this Section, for as long as Business Associate retains the PHI;
 - iv. not use or disclose the PHI retained by Business Associate other than for the purposes for which such PHI was retained and subject to the same conditions set out at above under “Permitted Uses and Disclosures By Business Associate” that applied prior to termination; and
 - v. return to Covered Entity (or, if agreed to by Covered Entity, destroy) the PHI retained by Business Associate when it is no longer needed by Business Associate for its proper management and administration or to carry out its legal responsibilities.
- b. All other applicable obligations of Business Associate under this Agreement shall survive termination.
- c. Should the applicable State of Oklahoma agency become aware of a pattern of activity or practice that constitutes a material breach of a material term of this BAA by Business Associate, the agency shall provide Business Associate with written notice of such a breach in sufficient detail to enable Contractor to understand the specific nature of the breach. The Client shall be entitled to terminate the Underlying Contract associated with such breach if, after the applicable State of Oklahoma agency provides the notice to Business Associate, Business Associate fails to cure the breach within a reasonable time period not less than thirty (30) days specified in such notice; provided, however, that such

time period specified shall be based on the nature of the breach involved per 45 C.F.R. §§ 164.504(e)(1)(ii)(A),(B) & 164.314 (a)(2)(i)(D).

26.8 Miscellaneous Provisions:

- a. No Third-Party Beneficiaries: Nothing in this Agreement shall confer upon any person other than the parties and their respective successors or assigns, any rights, remedies, obligations, or liabilities whatsoever.
- b. Business Associate recognizes that any material breach of this Business Associate Terms section or breach of confidentiality or misuse of PHI may result in the termination of this Agreement and/or legal action. Said termination may be immediate and need not comply with any termination provision in the parties' underlying agreement, if any.
- c. The parties agree to amend this Agreement from time to time as is necessary for Covered Entity or Business Associate to comply with the requirements of the Privacy Rule and related laws and regulations.
- d. The applicable State of Oklahoma agency shall make available its Notice of Privacy Practices.
- e. Any ambiguity in this Agreement shall be resolved in a manner that causes this Agreement to comply with HIPAA.
- f. If Business Associate maintains a designated record set in an electronic format on behalf of Covered Entity, then Business Associate agrees that within 30 calendar days of expiration or termination of the parties' agreement, Business Associate shall provide to Covered Entity a complete report of all disclosures of and access to the designated record set covering the three years immediately preceding the termination or expiration. The report shall include patient name, date and time of disclosures/access, description of what was disclosed/accessed, purpose of disclosure/access, name of individual who received or accessed the information, and, if available, what action was taken within the designated record set.
- g. Amendment: To the extent that any relevant provision of the HIPAA Regulations is materially amended in a manner that changes the obligations of Business Associates or Covered Entities, the Parties agree to negotiate in good faith appropriate amendment(s) to this Agreement to give effect to these revised obligations. The parties agree to amend this Agreement from time to time as is necessary for Covered Entity or to comply with the requirements of the Privacy Rule and related laws and regulations.

27 **42 C.F.R. PART 2 RELATED PROVISIONS**

- 27.1** Confidentiality of Information. Contractor's employees and agents shall have access to private data to the extent necessary to carry out the responsibilities, limited by the terms of this Agreement. Contractor accepts the responsibilities for providing adequate administrative supervision and training to their employees and agents to ensure

compliance with relevant confidentiality, privacy laws, regulations and contractual provisions. No private or confidential data collected, maintained, or used shall be disseminated except as authorized by statute and by terms of this Agreement, whether during the period of the Agreement or thereafter. Furthermore, Contractor:

- 27.2** Acknowledges that in receiving, transmitting, transporting, storing, processing, or otherwise dealing with any information received pursuant to this agreement that identifies or otherwise relates to the individuals under the care of or in the custody of a State of Oklahoma agency, it is fully bound by the provisions of the federal regulations governing the confidentiality of Alcohol and Drug Abuse Patient Records, 42 C.F.R. Part 2 and the HIPAA, 45 C.F.R. 45 Parts 142, 160, and 164, Title 43 A § 1-109 of Oklahoma Statutes, and may not use or disclose the information except as permitted or required by this Agreement or by law;
- 27.3** Acknowledges that pursuant to 43A O.S. §1-109, all mental health and drug or alcohol treatment information and all communications between physician or psychotherapist and patient are both privileged and confidential and that such information is available only to persons actively engaged in treatment of the client or consumer or in related administrative work. Contractor agrees that such protected information shall not be available or accessible to staff in general and shall not be used for punishment or prosecution of any kind;
- 27.4** Agrees to resist any efforts in judicial proceedings to obtain access to the protected information except as expressly provided for in the regulations governing the Confidentiality of Alcohol and Drug Abuse Patient Records, 42 C.F.R. Part 2;
- 27.5** Agrees to, when applicable and to the extent within Contractor's control, use appropriate administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of the electronic protected health information that it creates, receives, maintains, or transmits on behalf of the State of Oklahoma agency and to use appropriate safeguards to prevent the unauthorized use or disclosure of the protected health information, and agrees that protected information will not be placed in the Child Protective Services (CPS) record of any individual involved with the Oklahoma Department of Human Services (DHS).
- 27.6** Agrees to report to the State of Oklahoma agency any use or disclosure or any security incident involving protected information not provided for by this Agreement. Such a report shall be made immediately when an employee becomes aware of such a disclosure, use, or security incident.
- 27.7** Agrees to provide access to the protected information at the request of the State of Oklahoma agency or to an authorized individual as directed by the State of Oklahoma agency, in order to meet the requirement of 45 C.F.R. §164.524 which provides clients with the right to access and copy their own protected information;
- 27.8** Agrees to make any amendments to the protected information as directed or agreed to by the State of Oklahoma agency, pursuant to 45 C.F.R. §164.526;
- 27.9** Agrees to make available its internal practices, books, and records, including policies and procedures, relating to the use and disclosure of protected information received from the

State of Oklahoma agency or created or received by the Contractor on behalf of the State of Oklahoma agency, to the State of Oklahoma agency and to the Secretary of the Department of Health and Human Services for purpose of the Secretary determining the giving party's compliance with HIPAA;

- 27.10** Agrees to provide the State of Oklahoma agency, or an authorized individual, information to permit the State of Oklahoma agency to respond to a request by an individual for an accounting of disclosures in accordance with 45 C.F.R. §164.528.

28 DATA SECURITY

The Contractor agrees to, when applicable and to the extent within Contractor's control, maintain the data in a secure manner compatible with the content and use. The Contractor will, when applicable to the extent within Contractor's control, control access to the data in Contractor's possession or control compliance with the terms of this Agreement. Only the Contractor's personnel whose duties require the use of such information, will have regular access to the data. The Contractor's employees will be allowed access to the data only for the purpose set forth in this Agreement.

- 28.1** Data Destruction. Contractor agrees to, when applicable and to the extent within Contractor's control, follow State of Oklahoma agency policies regarding secure data destruction.
- 28.2** Use of Information. Contractor agrees that the information received or accessed through this Agreement shall not be used to the detriment of any individual nor for any purpose other than those stated in this Agreement.
- 28.3** Redisclosure of Data. The Contractor agrees not to redisclose any information to a third party not covered by the Agreement unless written permission by the State of Oklahoma agency is received and redisclosure is permitted under applicable law.

29 FEDERAL TAX INFORMATION REQUIREMENTS IRS PUBLICATION 1075

- 29.1** PERFORMANCE: If Contractor takes possession or control of Federal Tax Information in performance of this contract, the Contractor agrees to, when applicable and to the extent within Contractor's control, comply with and assume responsibility for compliance by officers or employees with the following requirements:
- 29.2** All work will be performed under the supervision of the State of Oklahoma.
- 29.3** The contractor and contractor's officers or employees to be authorized access to FTI must meet background check requirements defined in IRS Publication 1075. The contractor will maintain a list of officers or employees authorized access to FTI. Such list will be provided to the agency and, upon request, to the IRS.
- 29.4** FTI in hardcopy or electronic format shall be used only for the purpose of carrying out the provisions of this contract. FTI in any format shall be treated as confidential and shall not be divulged or made known in any manner to any person except as may be necessary in the performance of this contract. Inspection or disclosure of FTI to anyone other than the contractor or the contractor's officers or employees authorized is prohibited.

- 29.5** FTI will be accounted for upon receipt and properly stored before, during, and after processing. In addition, any related output and products require the same level of protection as required for the source material.
- 29.6** The contractor will certify that FTI processed during the performance of this contract will be completely purged from all physical and electronic data storage with no output to be retained by the contractor at the time the work is completed. If immediate purging of physical and electronic data storage is not possible, the contractor will certify that any FTI in physical or electronic storage will remain safeguarded to prevent unauthorized disclosures.
- 29.7** Any spoilage or any intermediate hard copy printout that may result during the processing of FTI will be given to the agency. When this is not possible, the contractor will be responsible for the destruction of the spoilage or any intermediate hard copy printouts and will provide the agency with a statement containing the date of destruction, description of material destroyed, and the destruction method.
- 29.8** All Contractor computer systems receiving, processing, storing, or transmitting FTI must meet the requirements in IRS Publication 1075. To meet functional and assurance requirements, the security features of the environment must provide for the managerial, operational, and technical controls. All security features must be available and activated to protect against unauthorized use of and access to FTI.
- 29.9** No work involving FTI furnished under this contract will be subcontracted without the prior written approval of the IRS.
- 29.10** Contractor will ensure that the terms of FTI safeguards described herein are included, without modification, in any approved subcontract for work involving FTI.
- 29.11** To the extent the terms, provisions, duties, requirements, and obligations of this contract apply to performing services with FTI, the contractor shall assume toward the subcontractor all obligations, duties and responsibilities that the agency under this contract assumes toward the contractor, and the subcontractor shall assume toward the contractor all the same obligations, duties and responsibilities which the contractor assumes toward the agency under this contract.
- 29.12** In addition to the subcontractor's obligations and duties under an approved subcontract, the terms and conditions of this contract apply to the subcontractor, and the subcontractor is bound and obligated to the contractor hereunder by the same terms and conditions by which the contractor is bound and obligated to the agency under this contract.
- 29.13** For purposes of this contract, the term "contractor" includes any officer or employee of the contractor with access to or who uses FTI, and the term "subcontractor" includes any officer or employee of the subcontractor with access to or who uses FTI.
- 29.14** The agency will have the right to void the contract if the contractor fails to meet the terms of FTI safeguards described herein.

30 CRIMINAL/CIVIL SANCTIONS

- 30.1** Each officer or employee of a contractor to whom FTI is or may be disclosed shall be notified in writing that FTI disclosed to such officer or employee can be used only for a purpose and to the extent authorized herein, and that further disclosure of any FTI for a purpose not authorized herein constitutes a felony punishable upon conviction by a fine of as much as \$5,000 or imprisonment for as long as 5 years, or both, together with the costs of prosecution.
- 30.2** Each officer or employee of a contractor to whom FTI is or may be accessible shall be notified in writing that FTI accessible to such officer or employee may be accessed only for a purpose and to the extent authorized herein, and that access/inspection of FTI without an official need-to-know for a purpose not authorized herein constitutes a criminal misdemeanor punishable upon conviction by a fine of as much as \$1,000 or imprisonment for as long as 1 year, or both, together with the costs of prosecution.
- 30.3** Each officer or employee of a contractor to whom FTI is or may be disclosed shall be notified in writing that any such unauthorized access, inspection or disclosure of FTI may also result in an award of civil damages against the officer or employee in an amount equal to the sum of the greater of \$1,000 for each unauthorized access, inspection, or disclosure, or the sum of actual damages sustained as a result of such unauthorized access, inspection, or disclosure, plus in the case of a willful unauthorized access, inspection, or disclosure or an unauthorized access/inspection or disclosure which is the result of gross negligence, punitive damages, plus the cost of the action. These penalties are prescribed by IRC sections 7213, 7213A and 7431 and set forth at 26 CFR 301.6103(n)-1.
- 30.4** Additionally, it is incumbent upon the contractor to inform its officers and employees of the penalties for improper disclosure imposed by the Privacy Act of 1974, 5 U.S.C. 552a. Specifically, 5 U.S.C. 552a(i)(1), which is made applicable to contractors by 5 U.S.C. 552a(m)(1), provides that any officer or employee of a contractor, who by virtue of his/her employment or official position, has possession of or access to agency records which contain individually identifiable information, the disclosure of which is prohibited by the Privacy Act or regulations established thereunder, and who knowing that disclosure of the specific material is so prohibited, willfully discloses the material in any manner to any person or agency not entitled to receive it, shall be guilty of a misdemeanor and fined not more than \$5,000.
- 30.5** Granting a contractor access to FTI must be preceded by certifying that each officer or employee understands the agency's security policy and procedures for safeguarding FTI. A contractor and each officer or employee must maintain their authorization to access FTI through annual recertification of their understanding of the agency's security policy and procedures for safeguarding FTI. The initial certification and recertifications must be documented and placed in the agency's files for review. As part of the certification and at least annually afterwards, a contractor and each officer or employee must be advised of the provisions of IRC sections 7213, 7213A, and 7431 (see IRS Publication 1075, Exhibit 4, Sanctions for Unauthorized Disclosure, and IRS Publication 1075, Exhibit 5, Civil Damages for Unauthorized Disclosure). The training on the agency's security policy and procedures provided before the initial certification and annually thereafter must also cover the incident response policy and procedure for reporting unauthorized disclosures and data breaches. For the initial certification and the annual recertifications, the contractor and each officer or employee must sign, either with ink or

electronic signature, a confidentiality statement certifying their understanding of the security requirements.

31 INSPECTION

The IRS and the Agency, with 24-hour notice, shall have the right to send its inspectors into the offices and plants of the contractor to inspect facilities and operations performing any work with FTI under this contract for compliance with requirements defined in IRS Publication 1075. The IRS' right of inspection shall include the use of manual and/or automated scanning tools to perform compliance and vulnerability assessments of information technology (IT) assets that access, store, process or transmit FTI. Based on the inspection, corrective actions may be required in cases where the contractor is found to be noncompliant with FTI safeguard requirements.

32 SSA REQUIREMENTS

- 32.1** PERFORMANCE: If Contractor takes possession or control of in SSA provided information in the performance of this contract, the contractor agrees to, where applicable and to the extent within Contractor's control comply with and assume responsibility for compliance by his or her employees with the following requirements:
- 32.2** All work will be done under the supervision of the State of Oklahoma.
- 32.3** Any SSA provided information made available shall be used only for carrying out the provisions of this Agreement. Information contained in such material shall be treated as confidential and shall not be divulged or made known in any manner to any person except as may be necessary in the performance of this contract. Inspection by or disclosure to anyone other than an officer or employee of the Contractor is prohibited.
- 32.4** All SSA provided information shall be accounted for upon receipt and properly stored before, during, and after processing. In addition, all related output and products will be given the same level of protection as required for the source material.
- 32.5** No work involving SSA provided information furnished under this contract shall be subcontracted without prior written approval by the applicable State of Oklahoma agency and the SSA.
- 32.6** The Contractor shall maintain a list of employees authorized access. Such list shall be provided upon request to the applicable State of Oklahoma agency or the SSA.
- 32.7** Contractor or agents may not legally process, transmit, or store SSA-provided information in a cloud environment without explicit permission from SSA's Chief Information Officer. Proof of this authorization shall be provided to the Contractor by the applicable State of Oklahoma agency prior to accessing SSA provided information.
- 32.8** Contractor shall provide security awareness training to all employees, contractors, and agents who access SSA-provided information. The training should be annual, mandatory, and certified by the personnel who receive the training. Contractor is also required to certify that each employee, contractor, and agent who views SSA-provided information certify that they understand the potential criminal, civil, and administrative sanctions or penalties for unlawful assess and/or disclosure.

- 32.9** Contractor shall require employees, contractors, and agents to sign a non-disclosure agreement, attest to their receipt of Security Awareness Training, and acknowledge the rules of behavior concerning proper use and security in systems that process SSA-provided information. Contractor shall retain non-disclosure attestations for at least five (5) to seven (7) years for each employee who processes, views, or encounters SSA-provided information as part of their duties.
- 32.10** The applicable State of Oklahoma agency shall provide the Contractor a copy of the SSA exchange agreement and all related attachments before initial disclosure of SSA data. Contractor is required to follow the terms of the applicable State of Oklahoma agency's data exchange agreement with the SSA. Prior to signing this Agreement, and thereafter at SSA's request, the applicable State of Oklahoma agency shall obtain from the Contractor a current list of the employees of such Contractor with access to SSA data and provide such list to the SSA.
- 32.11** Where the Contractor processes, handles, or transmits information provided to the applicable State of Oklahoma agency by SSA or has authority to perform on the agency's behalf, the applicable State of Oklahoma agency shall clearly state the specific roles and functions of the Contractor within the Agreement.
- 32.12** SSA requires all parties subject to this Agreement to exercise due diligence to avoid hindering legal actions, warrants, subpoenas, court actions, court judgments, state or Federal investigations, and SSA special inquiries for matters pertaining to SSA-provided information.
- 32.13** SSA requires all parties subject to this Agreement to agree that any Client-owned or subcontracted facility involved in the receipt, processing, storage, or disposal of SSA-provided information operate as a "de facto" extension of the Client and is subject to onsite inspection and review by the Client or SSA with prior notice.
- 32.14** If the Contractor must send a Contractor computer, hard drive, or other computing or storage device offsite for repair, the Contractor must have a non-disclosure clause in their contract with the vendor. If the Contractor used the item in a business process that involved SSA-provided information and the vendor will retrieve or may view SSA-provided information during servicing, SSA reserves the right to inspect the Contractor's vendor contract. The Contractor must remove SSA-provided information from electronic devices before sending it to an external vendor for service. SSA expects the Contractor to render SSA-provided information unrecoverable or destroy the electronic device if they do not need to recover the information. The same applies to excessed, donated, or sold equipment placed into the custody of another organization.
- 32.15** In the event of a suspected or verified data breach involving SSA provided information, the Contractor shall notify the Client immediately.
- 32.16** The Client shall have the right to void the contract if the contractor fails to provide the safeguards described above.

33 CRIMINAL/CIVIL SANCTIONS

The Act specifically provides civil remedies, 5 U.S.C. Sec. 552a(g), including damages, and criminal penalties, 5 U.S.C. Sec. 552a(i), for violations of the Act. The civil action provisions are premised violations of the Act committed by parties subject to this Agreement or regulations promulgated thereunder. An individual claiming such a violation by parties subject to this Agreement may bring civil action in a federal district court. If the individual substantially prevails, the court may assess reasonable attorney fees and other litigation costs. In addition, the court may direct the parties subject to this Agreement to grant the plaintiff access to his/her records, and when appropriate direct an amendment or correction of records subject to the Act. Actual damages may be awarded to the plaintiff for intentional or willful refusal by parties subject to this Agreement to comply with the Act.

33.1 Civil Remedies

- a. In any suit brought under the provisions of 5 U.S.C. § 552a(g)(1)(C) or (D) in which the court determines that the parties subject to this Agreement acted in a manner which was intentional or willful, shall be liable in an amount equal to the sum of
- b. actual damages sustained by the individual because of the refusal or failure, but in no case, shall a person entitled to recovery receive less than the sum of \$1,000; and
- c. the costs of the action together with reasonable attorney fees as determined by the court.
- d. An action to enforce any liability created under 5 U.S.C. § 552a may be brought in the district court of the United States in the district in which the complainant resides, or has his principal place of business, or in which the records are situated, or in the District of Columbia, without regard to the amount in controversy, within two years from the date on which the cause of action arises, except that where parties subject to this Agreement have materially and willfully misrepresented any information required under this section to be disclosed to an individual and the information so misrepresented is material to establishment of the liability of the agency to the individual under 5 U.S.C. § 552a, the action may be brought at any time within two years after discovery by the individual of the misrepresentation. Nothing in this section shall be construed to authorize any civil action because of any injury sustained as the result of a disclosure of a record prior to September 27, 1975.

33.2 Criminal Penalties

- a. Any officer or employee of an agency, who by virtue of his employment or official position, has possession of, or access to, agency records which contain individually identifiable information the disclosure of which is prohibited by this section or by rules or regulations established thereunder, and who knowing that disclosure of the specific material is so prohibited, willfully discloses the material in any manner to any person or agency not entitled to receive it, shall be guilty of a misdemeanor and fined not more than \$5,000. See 5 U.S.C. § 552a(i)(1).

- b. Any officer or employee of any agency who willfully maintains a system of records without meeting the notice requirements of subsection (e)(4) of this section shall be guilty of a misdemeanor and fined not more than \$5,000. See 5 U.S.C. § 552a(i)(2).
- c. Any person who knowingly and willfully requests or obtains any record concerning an individual from an agency under false pretenses shall be guilty of a misdemeanor and fined not more than \$5,000. See 5 U.S.C. § 552a(i)(3).

34 CHILD SUPPORT FPLS REQUIREMENTS

- 34.1** Contractor, when applicable and to the extent within Contractor's control, and the applicable State of Oklahoma agency must comply with the security requirements established by the Social Security Act, the Privacy Act of 1974, the Federal Information Security Management Act of 2002 (FISMA), 42 United States Code (USC) 654(26), 42 UCS 654a(d)(1)-(5), the U.S. Department of Health and Human Services (HHS), the U.S. Department of Health and Human Services Administration of Children and Families Office of Child Support Enforcement Security Agreement and the Automated Systems for Child Support Enforcement: A Guide for States Section H Security and Privacy. Contractor and applicable State of Oklahoma agency also agree to use Federal Parent Locator Service (FPLS) information and Child Support (CS) program information solely for the authorized purposes in accordance with the terms in this agreement. The information exchanged between state Child Support agencies and all other state program information must be used for authorized purposes and protected against unauthorized access to reduce fraudulent activities and protect the privacy rights of individuals against unauthorized disclosure of confidential information.
- 34.2** This is applicable to the personnel, facilities, documentation, data, electronic and physical records and other machine-readable information systems of the applicable State of Oklahoma agency and Contractor, including, but not limited to, state employees and contractors working with FPLS information and CS program information and state CS agency data centers, statewide centralized data centers, contractor data centers, state Health and Human Services' data centers, comprehensive tribal agencies, data centers serving comprehensive tribes, and any other individual or entity collecting, storing, transmitting or processing FPLS information and CS program information. This is applicable to all FPLS information, which consists of the National Directory of New Hires (NDNH), Debtor File, and the Federal Case Registry (FCR). The NDNH, Debtor File and FCR are components of an automated national information system.
- 34.3** This is also applicable to all CS program information, which includes the state CS program information, other state and tribal program information, and confidential information. Confidential information means any information relating to a specified individual or an individual who can be identified by reference to one or more factors specific to him or her, including but not limited to the individual's Social Security number, residential and mailing addresses, employment information, and financial information. Ref. 45 Code of Federal Regulations (CFR) 303.21(a).

35 FERPA REQUIREMENTS

- 35.1** If Contractor takes possession or control of Information covered by FERPA in performance of this Agreement, Contractor agrees to, when applicable and to the extent within Contractor's control comply with and assume responsibility for compliance by its employees with the Family Educational Rights and Privacy Act; (20 U.S.C. § 1232g; 34 CFR Part 99) ("FERPA") and the Oklahoma Student Data Accessibility, Transparency, and Accountability Act of 2013; (70 O.S. § 3-168), where personally identifiable student education data is exchanged.

36 CJIS REQUIREMENTS

- 36.1** INTRODUCTION - This section shall be applicable to the extent that Contractor takes possession or control of CJIS data. The use and maintenance of all items of software or equipment offered for purchase herein must be in compliance with the most current version of the U.S. Department of Justice, Federal Bureau of Investigation ("FBI"), Criminal Justice Information Services (CJIS) Division's CJIS Security Policy ("CJIS Security Policy" or "Security Policy" herein).
- 36.2** The Entity or Affiliate acquiring the data or system is hereby ultimately responsible for compliance with the CJIS Security Policy and will be subject to an audit by the State of Oklahoma CJIS Systems Officer ("CSO") and the FBI CJIS Division's Audit Staff.
- 36.3** CJIS SECURITY POLICY REQUIREMENTS GENERALLY - The CJIS Security Policy outlines a number of administrative, procedural, and technical controls agencies must have in place to protect Criminal Justice Information ("CJI"). Our experience is that agencies will generally have many of the administrative and procedural controls in place but will need to implement additional technical safeguards in order to be in complete compliance with the mandate. A Criminal Justice Agency ("CJA") and certain other governmental agencies procuring technology equipment and services that could be used in hosting or connecting or transmitting or receiving CJI data may need to use the check list herein to make sure that the software, equipment, location, security, and persons having the ability to access CJI will meet the CJIS requirements per the then current CJIS Security Policy. A completed Appendix H to said Security Policy will need to be signed by Vendor or a 3rd party if it has access to CJI, such as incident to the maintenance or support of the purchased hardware or software within which resides CJI. Per Appendix "A" to said Security Policy, "access to CJI is the physical or logical (electronic) ability, right or privilege to view, modify or make use of CJI."
- 36.4** DIRECTIVE CONCERNING ACCESS TO CRIMINAL JUSTICE INFORMATION AND TO HARDWARE OR SOFTWARE WHICH INTERACTS WITH CJI AND CERTIFICATION- The FBI CJIS Division provides state-of-the-art identification and information services to the local, state, tribal, federal, and international criminal justice communities for criminal justice purposes, as well as the noncriminal justice communities for noncriminal justice purposes.
- 36.5** This Directive primarily concerns access to CJI and access to hardware and software in the use, retention, transmission, reception, and hosting of CJI for criminal justice purposes and not for noncriminal justice purposes. In that regard, this Directive is not only applicable to such data, but also to the hardware and software interacting with such data, their location(s), and persons having the ability to access such data. The CJIS data applicable to the Security Policy is the data described as such in said Policy plus all data

transmitted over the Oklahoma Law Enforcement Telecommunications System (“OLETS”) which is operated by DPS.

36.6 In order to have access to CJI or to the aforesaid hardware or software, the vendor must be familiar with the FBI CJIS Security Policy, including but not limited to the following portions of said Security Policy:

- a. the Definitions and Acronyms in §3 & Appendices “A” & “B”;
- b. the general policies in §4;
- c. the Policies in §5;
- d. the appropriate forms in Appendices “D”, “E”, “F” & “H”; and
- e. the Supplemental Guidance in Appendices “J”.

36.7 This FBI Security Policy is located and may be downloaded at:

- a. <https://www.fbi.gov/services/cjis/cjissecurity-policy-resource-centerhttps://www.fbi.gov/services/cjis/cjissecurity-policy-resource-center>.
- b. By executing the Contract to which this Directive is attached, the vendor hereby CERTIFIES that the foregoing directive has and will be followed, including but not limited to full compliance with the FBI CJIS Security Policy, as amended and as applicable.

37 NOTICES

37.1 In addition to notice requirements under the terms of the Contract otherwise, the following individuals shall also be provided the request, approval or notice, as applicable:

Chief Information Officer
3115 N. Lincoln Blvd
Oklahoma City, OK 73105

With a copy, which shall not constitute notice, to:

OMES Deputy General Counsel
3115 North Lincoln Blvd
Oklahoma City, Oklahoma 73105

Attachment E to
STATE OF OKLAHOMA CONTRACT WITH Presidio Networked Solutions, LLC
RESULTING FROM SOLICITATION NO. 0900000550

The **Statement of Work** is hereby amended as set forth below and supersedes all prior documents submitted by **Presidio Networked Solutions, LLC** or discussed by the parties. The parties agree to use this **Statement of Work** or a document substantially similar in the form of this **Statement of Work**.

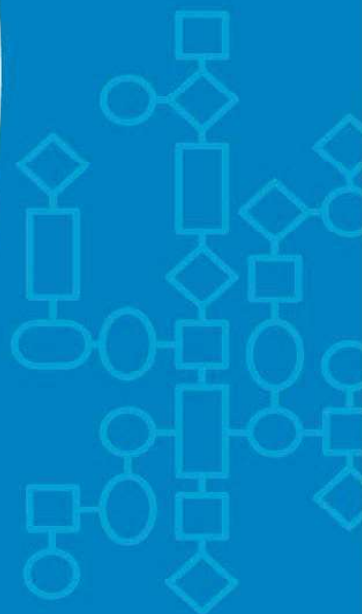
PRESIDIO®

OMES

STATEMENT OF WORK

OKLAHOMA

28-Sep-2022



PROPOSAL TEAM

Name	Company/Function	Phone	Email
	Presidio Account Manager		
	Presidio Solution Architect		

REVISION HISTORY

Revision	Revision Date	Name	Notes
V1.0	28-Sep-2022	Robert Yates	First Client Release

1. EXECUTIVE OVERVIEW

1.1. Introduction

Presidio Networked Solutions, LLC ("Presidio") is pleased to propose the following solution to Oklahoma ("Client"). This Statement of Work ("SOW") defines the tasks to be performed and the responsibilities of Presidio and Client.

1.2. Solution and Approach Overview

State Client's project definition and business need. What is Client trying to accomplish? Provide some critical success factors as seen by Client. This information can be pulled from the "Background" slide in the Vision deck if one has been created.

State Presidio's role in the project. What are we doing (high level)? What is the proposed solution high level? This information can be pulled from the "Proposed Solution" slide in the Vision deck if one has been created.

Limit this to one page of text, lists, etc.

1.3. Locations

Work will be done for the following locations. All work will be performed remotely unless otherwise specified.

Site Name	Address	City, State ZIP	On-Site/Remote Services
OMES	123 Presidio	Tulsa, OK	Remote

2. SCOPE OF WORK

2.1. Project Scope

2.1.1. Planning and Design Phase

2.1.2. Execution Phase

2.2. Training and Knowledge Transfer

Knowledge Transfer provided during the course of the engagement are informal sessions and consist of our engineers sharing their knowledge as they work through various tasks related to the project, and at the time the tasks are performed. The conduct of these sessions will be in a manner that does not slow down the pace of work or distract the engineers. These are not dedicated Knowledge Transfer sessions.

2.3. Deliverables

Documentation may be created by Presidio and provided as part of the Project Deliverables. Some of these deliverables may be delivered as a single document. The specific documentation to be provided depends on your chosen solution(s); several example documentation items are listed below. Additional documentation and/or printed documentation is available upon request for an additional cost.

Deliverable	Format
Dial Plan	Excel
High-Level Design Diagram	Visio

Array layout	Excel
System Manual	URL
Signed Testing Document	PDF
As-Built Documentation	PDF

With the exception of Project Status Reports, each deliverable material will be approved in accordance with the following procedure:

- If a written list of requested changes is received within five business days, the Presidio Project Team will make the agreed upon revisions and will, within five business days, re-submit the updated version to Client.
- Deliverable documentation may be delivered via email, uploaded to a portal, or provided on a physical media and it may be provided in either an encrypted or unencrypted format. If Client requests a specific delivery method and format, Presidio will use that method for all documentation delivery and format otherwise, the sender will choose a delivery method and format that they feel is appropriate given the content of the documentation.

2.4. Resources

Presidio approaches project execution from a skills-based perspective. Our Execution Team is made up of individuals who have specific skillsets that will be utilized at different times during a given project. This allows us to provide a very specialized workforce to Client and utilizes the appropriate resource for the task required.

2.4.1. Presidio Engineering Resources

- **Practice Manager(s)** – the technical manager and regional team lead of the field consulting team. The Practice Manager provides resource and technical oversight assistance to the Project Manager and ensures availability of technical resources and escalation paths for field consultants.
- **Architect/Senior Engineer(s)** – the technical escalation points for Engineer(s) and Project Oversight teams. An Architect or Senior Engineer is a subject matter expert within a certain technology or field. This senior-level resource will be the principal technical resource for the engagement and will have ownership of the final deliverables.

- **Engineer(s)** – one or more individuals assigned to complete technical project tasks. Assignment of these resources depends upon the skillset of the task(s) and the timeline(s) within which the task(s) must be completed. These individuals report directly to the Project Manager for task assignment updates and to the Practice Manager or Architect/Senior Engineer for technical escalation needs.

The following Presidio resources will be engaged on this project:

- Architect
- Principal Engineer

Contact information for the project team personnel will be distributed by the Project Manager.

2.4.2. Client Resources

Throughout the project, Client resources may be required for completion of specific tasks, providing key information or data, oversight, review, and approvals. The responsibilities of Client are outlined in this document.

The following Client resources will be engaged on this project:

- Architect
- Collaboration Engineer
- Collaboration Engineer - Senior
- Data Center Engineer

Contact information for the project team personnel will be distributed by the Project Manager.

2.5. Project Change Request Process

Any items that are determined to be outside of this Scope of Work and deliverables defined must be submitted with a Project Change Request Form. No work outside of this Scope of Work will be undertaken without written approval and processing of a Project Change Request.

In the event that both Presidio and Client agree to a change in this Statement of Work, a written description of the agreed-upon change will be prepared using a Project Change Request (PCR) form, which both parties must sign. The PCR form will be used to describe the change, the rationale for the change, and to specify any change in the scope, schedule, or budget. The terms of a mutually agreed upon Change Authorization will prevail over those of this Statement of Work or any previous Change Authorization.

Modifications in project scope including, but not limited to, the following will require a Project Change Request:

- Client-requested changes in outcome, approach, features, or capabilities.
- Additional required tasks discovered through the planning and design review, but not mentioned in this SOW, or changes to the design after the signoff of the design phase and/or during the implementation phase.
- Upgrade, modification, or repair of equipment or applications to effectively deploy this scope.
- Changes required to existing infrastructure components, not called out in this Statement of Work, including patching and/or reconfiguration.
- Remedial work for the resolution of issues that existed prior to the installation (bad cables, lost passwords, third-party solutions, and so forth).
- Defective equipment provided by Client and integrated into the solution requiring additional diagnostic troubleshooting and/or remediation.
- Troubleshooting issues due to Client changes to configurations made “after” releasing the system or “after” a specific milestone completion in a multi-site phased deployment.
- Delays due to issues relating to site preparation that result in delays to the project.

- Delays in responding to scheduling requests, acceptance requests, and requests for information.
- Insufficient notice of a schedule change. If 24-hour notice is not provided, charges may be applied.

3. ASSUMPTIONS AND RESPONSIBILITIES

Presidio makes the following assumptions and has identified the following Client responsibilities in developing this Statement of Work. These assumptions and responsibilities serve as the foundation to which the project estimate, approach, and timeline were developed. By signing this SOW, Client agrees that these assumptions and responsibilities are correct and valid. Any changes to the following assumptions and responsibilities must be processed using the Presidio Change Management Process and may impact the project duration and labor requirements.

3.1. General Assumptions

The following project assumptions are made and will be verified as part of the engagement:

1. Client has read and agrees with all items contained or omitted within this Statement of Work.
2. This SOW supersedes any previous scope discussion or agreement including "Vision Deck" PowerPoint proposals, emails, or verbal communications, but does not supersede terms and conditions contained in State Wide Contract 1041.
3. All Presidio activities will take place during normal working hours (Monday through Friday, 8:00 a.m. to 5:00 p.m., excluding holidays) unless noted as "Off Hours" in this SOW.
4. Any items or tasks not explicitly listed as in-scope within this SOW are considered to be outside of the scope and not associated with this SOW and price.
5. If integration of the product is performed at a Presidio facility, then transfer of ownership (acceptance) occurs upon the receipt and integration of goods at Presidio, regardless of shipment, as manufacturers will not accept returns of opened products.
6. Presidio will not be held responsible for troubleshooting networks, applications and/or hardware if Client has no formal change management documented processes and policies.
7. Presidio will not make changes to the configuration of any network equipment after it has been installed and tested.
8. Some activities included in this project may be performed on Presidio's premises.
9. Not all features or functions of the installed system are included in the scope of this engagement.
10. Presidio will configure the systems outlined within this Statement of Work, with a unique set of authentication credentials, unless otherwise provided by Client. Upon the completion of the engagement, Presidio will provide Client with all user names, passwords, and additional authentication information that were implemented during the engagement. Presidio strongly recommends that these credentials be changed upon the completion of the engagement.

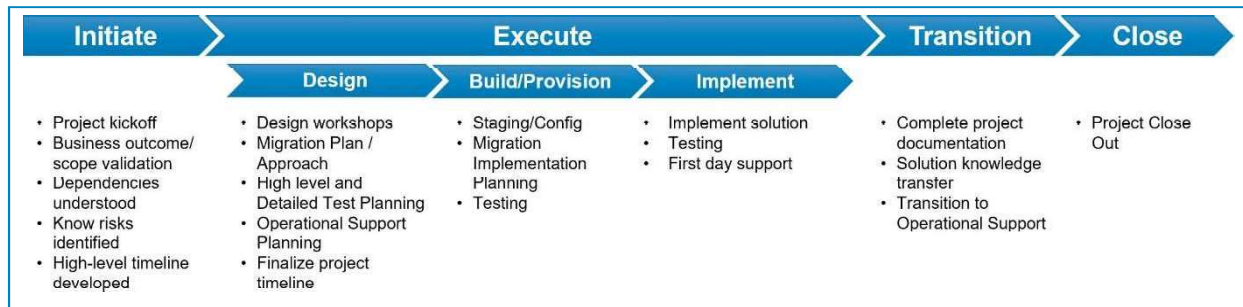
3.2. Client Responsibilities

The following items are listed as responsibilities of Client for this engagement. Client is responsible for performing the items and activities listed in this section or arranging for them to be performed by a third-party if appropriate.

1. Provide a single Client point of contact with the authority and the responsibility of issue resolution and the identification, coordination, and scheduling of Client personnel to participate in the implementation of the SOW. Without a single Client point of contact, a Project Change Request may be required for the additional effort by Presidio.
2. Participate in any required design sessions or workshops.
3. Provide or procure all appropriate hardware, software, licensing, and media required for implementation of the SOW.
4. Supply current equipment configuration for review if applicable.
5. Schedule appropriate maintenance windows for system upgrades or installs and notify user community.
6. Be responsible for having in place, active manufacturer support contracts on all devices that are the subject of this SOW.
7. Dispose of all retired equipment as part of this project.
8. Provide all required physical access to Client's facility (identification badge, escort, parking decal, etc.), as required by Client's policies; and provide all required functional access (passwords, IP address information, etc.), as required for Presidio to complete the tasks.
9. Provide to Presidio all required IP addresses, passwords, system names, and aliases.
10. Validate the site readiness prior to the dispatch of Presidio personnel to perform the services being contracted.
11. Provide adequate facilities for the installation of the hardware. This includes all necessary peripheral hardware (KVM ports or monitors, keyboards, mice, network access, etc.), as well as electrical and spatial needs and required antivirus software.
12. Provide high-speed access to the Internet for verification of device support requirements and for software downloads.
13. Verify operation of the installed/upgraded equipment per the predefined Verification Plan.
14. Provide Presidio administrator access on appropriate devices for the completion of the engagement.
15. Complete all Client installations where required in accordance with Client PC requirements for the new application versions.
16. Provide remote access for troubleshooting and configurations related to the project – preferably VPN access, as necessary.
17. Provide requested documentation or information needed for the project within two business days, unless otherwise agreed to by all parties.
18. Transport of equipment from receiving area(s) to the data center(s) and/or equipment rooms where it will be installed.
19. Ensure all Category 5 (Cat 5) (or higher) and fiber cable infrastructure is in place and tested for all sites.
20. Provide patch cables and complete necessary fiber or Cat 5 cable terminations to patch panels for new switching and routing infrastructure.

4. PRESIDIO PROJECT MANAGEMENT METHOD (PMM)

Presidio's Engagement Delivery Method incorporates best practices from our extensive experience as Digital System Integrators. The method is prescriptive while being flexible and customized for each client's specific needs based on the specific scope of work. This allows Presidio to right size the approach to be flexible and efficient, while maintaining an appropriate structure and governance to effectively deliver the business outcome.



4.1. Escalation Path

Client experience is of the utmost importance to Presidio. If at any time a Client feels the need to escalate an issue or concern, please consider the escalation points and options described below.

Level 1

- **Account Manager** – Client's first point of escalation is always their Account Manager. The AM can facilitate additional escalation if required and coordinate meetings between the required people within Presidio and Client in order to swiftly resolve any issues.
- **Project Manager** – for projects that include Project Management, the Project Manager is an escalation point for any concerns or questions.
- **Practice Manager**– for technical issues, the Service Delivery team will reach out to the manufacturer's support avenues within one hour of identifying an issue. If additional technical escalation is warranted, the Presidio Practice Manager will be contacted after that time.

Level 2

- **Program and Project Management (PPM) Team Lead** – if Client is not satisfied with the response from the Level 1 escalation, the PPM Team Lead would be the next level of escalation for any and all issues associated with the project scope and would own the management of the issue to resolution including technical and non-technical related concerns.
- **Service Delivery Director** – for technical issues specifically, if the issue is not resolved within an hour, the Service Delivery Director will be contacted for additional escalation and action. For technical issues escalated by the Delivery Team, the Service Delivery Director will:
 - Contact and speak with Client via phone to explain the status
 - Develop a plan of action
 - Communicate the plan of action status and completion to Client
 - Contact the Operations team, as required, to request additional resources, as required, in order to execute the plan of action

Level 3

- **Program and Project Management Services (PPM) Director** – for projects that include Project Management, the PPM Director is the third escalation point for any technical or non-technical concerns or questions.

- **Services Vice President** – if the issue or concern cannot be addressed or resolved within Level 1 or Level 2 of the escalation process, the issue will be raised to the executive level for visibility and resolution.

4.2. Technical Support after Completion

For non-critical support, including system expansion options, assessments, audits, and related services, or services that are not covered by a support contract with Presidio or another vendor, Presidio offers a variety of options including Fixed Fee, Hourly Rate, or Daily Rate options. Pricing for these services is not included in this Statement of Work.

Managed Services Clients	Non-Managed Services Clients
Technical support for the solution implemented within the scope of this SOW can be obtained by: <ul style="list-style-type: none">• calling 800-494-0118• sending an email to presidio@service-now.com	Vendor's (such as Cisco or EMC) Support Center or Technical Assistance Center (TAC) is the vehicle for all support. These Vendor Support Centers provides 7x24 support on all hardware and software, including replacement parts, software patches and updates, and configuration assistance.

5. PRICING

Presidio is providing a Fixed Fee Price as part of this Statement of Work. Presidio will invoice Client based on the project milestone(s) listed below:

Milestone Name	Amount
Project Initiation	\$0.00
Design Complete	\$0.00
Execution Complete	\$0.00
Project Closure	\$0.00
Total:	firstrow.totalSell

Presidio will bill Client upon completion of each Milestone. Invoices may contain multiple Milestones.

If Client requires a change in the scope of work, the parties will negotiate in good faith to generate a written change order documenting the additional labor and requirements that will be mutually agreed upon by the parties prior to onset of the additional work.

5.1. Expenses

Reserved.

5.2. Travel Time

Travel to and from the work site(s) by Presidio resources in association with the execution of this Statement of Work is included in the pricing above.

6. TERMS AND CONDITIONS

Terms and conditions are covered under Oklahoma Statewide Contract No. 1014.

7. APPROVAL SIGNOFF

The use of signatures on this Statement of Work is to ensure agreement on project objectives and the work to be performed by Presidio.

Presidio signature signifies our commitment to proceed with the project as described in this document. Please review this document thoroughly, as it will be the basis for all work performed by Presidio on this project.

This Statement of Work is valid for a period of 60 days from the date that this Statement of Work is provided by Presidio to Client unless otherwise agreed to by both parties.

Client

Signature

Date

Printed Name

Presidio

Signature

Date

Printed Name & Title

SW1014 Telecom 2022

Vendor: **Presidio Networked Solutions LLC**

Carrier Services		Monthly Reoccurring Costs	Installation Fees	Total Costs	Upgrade Costs
N/A	Description				

Equipment		Unit of Measure	List Price	% off List Price	Cost per Unit
	Description				
	Cisco	TBD	TBD	38% off product / 16% off Support	N/A
	Juniper	TBD	TBD	45% off product / 15% off support	N/A
	Aruba	TBD	TBD	40% off product / 8% off support	N/A
	Palo Alto	TBD	TBD	30% off product / 10% off support	N/A
	Nimble	TBD	TBD	40% off product / 10% off support	N/A
	APC / Schneider Electric	TBD	TBD	10% off product / 5% off support	N/A
	f5	TBD	TBD	15% off product / 10% off support	N/A
	Infoblox	TBD	TBD	10% off product / 5% off support	N/A
	VMware	TBD	TBD	3% off product / 3% off support	N/A
	Pure	TBD	TBD	25% off product / 10% off support	N/A
	Riverbed	TBD	TBD	25% off product / 10% off support	N/A
	Singewire	TBD	TBD	10% off product / 10% off support	N/A
	Eaton	TBD	TBD	25% off product / 5% off support	N/A
	Veeam	TBD	TBD	5% off product / 2% off support	N/A

Commvault	TBD	TBD	20% off product / 10% off support	N/A
TrendMicro	TBD	TBD	10% off product / 5% off support	N/A
Nutanix	TBD	TBD	5% off product / 5% off support	N/A
Ekahau	TBD	TBD	15% off product / 8% off support	N/A
Firemon	TBD	TBD	10% product / 5% off support	N/A
Gemalto	TBD	TBD	10% product / 5% off support	N/A
LogRhythm	TBD	TBD	10% product / 5% off support	N/A
Exabeam	TBD	TBD	10% product / 5% off support	N/A
NetApp	TBD	TBD	10% product / 5% off support	N/A
Vertiv	TBD	TBD	10% product / 5% off support	N/A
Dell / EMC	TBD	TBD	10% product / 5% off support	N/A
LiveAction	TBD	TBD	5% off list / 3% off support	N/A
Varonis	TBD	TBD	5% off product / 5% off support	N/A
Thales	TBD	TBD	3% off product / 3% off support	N/A
Delinea Inc	TBD	TBD	3% off product / 3% off support	N/A
Cohesity	TBD	TBD	10% off product / 10% off support	N/A
NetBrain	TBD	TBD	3% off product / 3% off support	N/A
OpenText	TBD	TBD	3% off product / 3% off support	N/A
Fortinet	TBD	TBD	10% product / 5% off support	N/A
American Well	TBD	TBD	10% product / 5% off support	N/A
SolarWinds, Inc	TBD	TBD	3% off product / 3% off support	N/A
Ventev	TBD	TBD	10% product / 5% off support	N/A
AudioCodes Inc	TBD	TBD	10% off product / 5% off support	N/A
Zscaler	TBD	TBD	10% off product / 5% off support	N/A
Artic Wolf	TBD	TBD	10% off product / 5% off support	N/A
One Identity	TBD	TBD	5% off product / 5% off support	N/A
Imperva	TBD	TBD	5% off product / 5% off support	N/A
Twilio	TBD	TBD	3% product / 5% off support	N/A
Room Ready	TBD	TBD	3% product / 5% off support	N/A
Calabrio	TBD	TBD	5% off product / 5% off support	N/A

**Attachment F to
STATE OF OKLAHOMA CONTRACT WITH PRESIDIO
NETWORKED SOLUTIONS, LLC
RESULTING FROM 0900000550**

Negotiated Exceptions and Additional Terms to the Contract

The Contract is hereby amended to include the terms as set forth below and supersedes all prior terms and exceptions submitted by **Presidio Networked Solutions, LLC** or discussed by the parties.

Requested Exceptions and Additional Terms not addressed below are declined by the State of Oklahoma.

Term & Section	Language
Attachment B Ordering, Inspection and Acceptance Section 6.2	<p>Section 6.2 shall be modified to add the following:</p> <p>6.2 Services will be performed in accordance with industry best practices and are subject to acceptance by the Customer. Unless stated otherwise in an SOW, Supplier provides an industry standard warranty of 30 days on services. Notwithstanding any other provision in the Contract, deemed acceptance of a service or associated deliverable shall not apply automatically upon receipt of a deliverable or upon provision of a service.</p> <p>Supplier warrants and represents that a product or deliverable furnished by or through the Supplier shall individually, and where specified by Supplier to perform as a system, be substantially uninterrupted and error-free in operation and guaranteed against faulty material and workmanship for <u>the</u> warranty period <u>which is the</u> maximum allowed by the manufacturer. A defect in a product or deliverable furnished by or through the Supplier shall be repaired or replaced by Supplier at no additional cost or expense to the Customer if such defect occurs during the warranty period.</p> <p>Request to add the following language to this Section:</p> <p>EXCEPT AS EXPRESSLY PROVIDED IN THIS AGREEMENT, SUPPLIER MAKES NO WARRANTIES, EXPRESS OR IMPLIED, AND SPECIFICALLY DISCLAIMS ANY WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, TITLE OR NON-INFRINGEMENT OR ANY WARRANTY ARISING BY USAGE OF TRADE, COURSE OF DEALINGS OR COURSE OF PERFORMANCE.</p>

Attachment B

Limitation of Liability

Section 16.5

Section 16.5 shall be modified to add the following:

TO THE EXTENT ALLOWED BY LAW, EXCEPT FOR PROPERTY DAMAGE, BODILY INJURY OR DEATH CAUSED BY SUPPLIER OR ITS EMPLOYEES AGENTS OR SUBCONTRACTOR; INDEMNITY, SECURITY OR CONFIDENTIALITY OBLIGATIONS UNDER THE CONTRACT; THE BAD FAITH NEGLIGENCE, OR INTENTIONAL MISCONDUCT, SUPPLIER'S ENTIRE LIABILITY AND CUSTOMER'S EXCLUSIVE REMEDY FOR DAMAGES FROM ANY CAUSE WHATSOEVER SHALL BE LIMITED TO THE AMOUNTS PAID BY STATE OR CUSTOMER TO SUPPLIER FOR THE PRODUCTS AND/OR SERVICE GIVING RISE TO THE CLAIM IN THE TWELVE (12) MONTHS PRECEDING THE DATE OF THE CLAIM.

Attachment D Commercial off the shelf software Section 10	Section 10 shall be modified to add the following: Supplier specifies terms and conditions or clauses in an electronic license, subscription, maintenance, support or similar agreement that conflict with the terms of this Contract, the additional or conflicting terms and conditions or conflicting clauses shall not be binding on the State and the provisions of this Contract shall prevail.
Attachment D Intellectual Property Ownership Section 12.1	Section 12.1 shall be modified to add the following: As between Supplier and Customer, the Work Product and Intellectual Property Rights therein are and shall be owned exclusively by Customer, excluding Supplier's Background IP, and not Supplier. Supplier specifically agrees that the Work Product shall be considered "works made for hire" and that the Work Product shall, upon creation, be owned exclusively by Customer. To the extent that the Work Product, under applicable law, may not be considered works made for hire, Supplier hereby agrees that all right, title and interest in and to all ownership rights and all Intellectual Property Rights in the Work Product, excluding Supplier's Background IP, is hereby effectively transferred, granted, conveyed, assigned and relinquished exclusively to Customer, without the necessity of any further consideration, and Customer shall be entitled to obtain and hold in its own name all Intellectual Property Rights in and to the Work Product. Supplier acknowledges that Supplier and Customer do not intend Supplier to be a joint author of the Work Product within the meaning of the Copyright Act of 1976. Customer shall have access, during normal business hours (Monday through Friday, 8:00 a.m. to 5:00 p.m.) and upon reasonable prior notice to Supplier, to all Supplier materials, premises and computer files containing the Work Product. Supplier and Customer, as appropriate, will cooperate with one another and execute such other documents as may be reasonably appropriate to achieve the objectives herein. No license or other right is granted under the Contract to any Third Party Intellectual Property, except as may be incorporated in the Work Product by Supplier. Notwithstanding the foregoing Supplier or it's third party manufacturer as applicable, retains all ownership and intellectual property rights in it's Background IP. Background IP" means all object code, Third Party Software, technology, systems, strategies, processes, methods, techniques, ideas, experience, information, know-how, patents, trademarks, copyrights, designs, developments, or other proprietary rights that are used or delivered by Supplier hereunder, whether pre-existing or conceived, created or developed by Supplier outside of the scope of this Agreement, whether embodied or otherwise encompassed in the Work Product and including all improvements or derivatives thereof.



Statewide Contract Summary

Official signed contract documents are on file with OMES Central Purchasing.

Contract title: Software VAR

Contract Number: SW1041PU

Date of Contract issuance: 03/22/2024

Contract period: 03/22/2024 through 03/13/2025

Agreement period: 03/22/2024 through 03/13/2028

Type of contract: Mandatory ☐ Non-Mandatory ☒

OMES Central Purchasing contact: Marc Brown **Title:** Statewide Contracting Officer

Phone: 405 - 521-
6669

Email: Marc.brown@omes.ok.gov

Supplier name: Pulselight Holdings, Inc.

Supplier ID #: 0000549502

Contract ID #: 7315

Supplier Point of Contact: Rita Diamond

Supplier address: 201 W. 5th St. Suite 1575

City: Austin

State: TX

Zip Code: 78701 - 2983

Phone #: 1 - 512 - 682 - 4715

Email team@pulselight.com

Contract Overview:

Software VAR contract for use by all Oklahoma agencies.

Authorized Users: All state departments, boards, commissions, agencies, and institutions, in Addition to counties, school districts and municipalities which may avail themselves of this contract.

How to order:

Request quote from contracted vendor. Please ensure quote references SW1041PU.

Available Brands:

Pulselight Only.

Available Products and Services:

Program Integrity, Incident Detection, Multi-Agency Incident, Case Tracker, Software

Authorized Dealer/Reseller(s):

N/A

Please verify that the software item being purchased is not available on existing mandatory statewide contracts. (i.e. SW1010, SW1079, etc.) This statewide contract is for software, software maintenance, software as a service (SaaS), and software implementation services.

Software Publishers			
Description	Maximum Cost + % Markup	% off List Price	
Pulselight Program Integrity Standard Solution 1st Year License & Implementation	\$ 1,650,000		
Pulselight Program Integrity Standard Solution Annual License Subscription	\$ 540,000		
Pulselight Program Integrity Premier Solution 1st Year License & Implementation	\$ 2,250,000		
Pulselight Program Integrity Premier Solution Annual License Subscription	\$ 540,000		
Pulselight Program Integrity Premier Solution with Expanded Database 1st Year License & Implementation	\$ 2,495,000		
Pulselight Program Integrity Premier Solution with Expanded Database Annual License Subscription	\$ 648,000		
Pulselight Incident Detection Standard Solution 1st Year License & Implementation	\$ 1,650,000		
Pulselight Incident Detection Standard Solution Annual License Subscription	\$ 540,000		
Pulselight Incident Detection Premier Solution 1st Year License & Implementation	\$ 1,900,000		
Pulselight Incident Detection Premier Solution Annual License Subscription	\$ 540,000		
Pulselight Incident Detection Premier Solution with Expanded Database 1st Year License & Implementation	\$ 2,200,000		
Pulselight Incident Detection Premier Solution with Expanded Database Annual License Subscription	\$ 648,000		
Pulselight Multi-Agency Incident Detection Standard Solution 1st Year License & Implementation	\$ 2,200,000		
Pulselight Multi-Agency Incident Detection Standard Solution Annual License Subscription	\$ 600,000		
Pulselight Multi-Agency Incident Detection Premier Solution 1st Year License & Implementation	\$ 2,400,000		
Pulselight Multi-Agency Incident Detection Premier Solution Annual License Subscription	\$ 600,000		
Pulselight Multi-Agency Incident Detection Premier Solution with Expanded Database 1st Year License & Implementation	\$ 2,650,000		
Pulselight Multi-Agency Incident Detection Premier Solution with Expanded Database Annual License Subscription	\$ 675,000		
Pulselight Drug Utilization Solution 1st Year License & Implementation	\$ 750,000		
Pulselight Drug Utilization Solution Annual License Subscription	\$ 360,000		
Pulselight Case Tracker Solution 1st Year License & Implementation	\$ 1,200,000		
Pulselight Case Tracker Solution Annual License Subscription	\$ 420,000		
Pulselight Bundled Discounts - 20% off above pricing for multiple product families		20%	

Other Value Add Products and Services

Description	Maximum Cost + % Markup	% off List Price

Professional Services - Hourly Not-to-Exceed Rates

Description	List Price	Discounted Hourly Rates
Subject Matter Expert - Healthcare	\$ 320.00	\$ 295.00
Subject Matter Expert - Analytics	\$ 320.00	\$ 295.00
Subject Matter Expert - Data	\$ 320.00	\$ 295.00
Project Manager	\$ 200.00	\$ 185.00
Principal Data Scientist	\$ 385.00	\$ 355.00
Security Expert	\$ 300.00	\$ 275.00
Software Architect	\$ 320.00	\$ 295.00
Sr. SW Engineer	\$ 285.00	\$ 260.00
Sr. UI Engineer	\$ 260.00	\$ 240.00
Data Engineer	\$ 250.00	\$ 230.00
Sr. Data Analyst	\$ 225.00	\$ 205.00
Data Analyst	\$ 195.00	\$ 180.00
Investigator	\$ 150.00	\$ 140.00
Analyst	\$ 125.00	\$ 115.00



**STATE OF OKLAHOMA STATEWIDE CONTRACT
WITH PULSELIGHT HOLDINGS, INC.**

This State of Oklahoma Statewide Contract No. 1041 (“Contract”) is entered into between the state of Oklahoma by and through the Office of Management and Enterprise Services and Pulselight Holdings, Inc. (“Supplier”) and is effective as of the date of last signature to this Contract. The initial term of the Contract shall be for 1 year with four (4) one-year options to renew.

Purpose

The State is awarding this Contract to Supplier for software and services to support State agencies and other eligible Oklahoma Interlocal Entities. This Supplier will provide software, training, pre-sales assistance, documentation, installation, maintenance, support, configuration, customization, and license agreement administration, as more particularly described in certain Contract Documents. Supplier submitted a proposal containing exceptions to the Solicitation, Supplier submitted additional terms, Supplier requested confidential matters to be considered, and Supplier submitted a best and final offer. This Contract memorializes the agreement of the parties with respect to the negotiated terms of the Contract that is being awarded to Supplier.

Now, therefore, in consideration of the foregoing and the mutual promises set forth herein, the receipt and sufficiency of which are hereby acknowledged the parties agree as follows:

1. The parties agree that Supplier has not yet begun performance of work under this Contract. Upon full execution of this Contract, Supplier may begin work. Issuance of a purchase order is required prior to payment to a Supplier.
2. The following Contract Documents are attached hereto and incorporated herein:
 - 2.1. Solicitation, Attachment A;
 - 2.2. General Terms, Attachment B;
 - 2.3. Statewide Contract Terms, Attachment C;
 - 2.4. Information Technology Terms, Attachment D;
 - 2.5. Information Security Terms, Attachment D-1
 - 2.6. Portions of the Bid,
 - i. Attachment E-1: Pricing;
 - ii. Attachment E-2: Master Terms;
 - iii. Attachment E-3: User Terms; and

2.7. Negotiated Exceptions to Contract, Attachment F.

3. The parties additionally agree:

3.1. except for trade secret information including method, technique and process and any other information deemed confidential by the State pursuant to applicable law, rule, regulation or policy, the parties agree Contract terms and information are not confidential and are disclosable without further approval of or notice to Supplier.

4. Any reference to a Contract Document refers to such Contract Document as it may have been amended. If and to the extent any provision is in multiple documents and addresses the same or substantially the same subject matter but does not create an actual conflict, the more recent provision is deemed to supersede earlier versions.

STATE OF OKLAHOMA
by and through the
OFFICE OF MANAGEMENT AND
ENTERPRISE SERVICES

PULSELIGHT HOLDINGS, INC.

By: 
Joe McIntosh Dec 22, 2023 11:08 CST

Name: Joe McIntosh

Title: CIO

Date: Dec 22, 2023

By: *Rita Diamond*

Name: Rita Diamond

Title: VP of Finance

Date: Dec 22, 2023

ATTACHMENT A
SOLICITATION NO. 0900000556

This Solicitation is a Contract Document and is a request for proposal in connection with the Contract awarded by the Office of Management and Enterprise Services as more particularly described below. Any defined term used herein but not defined herein shall have the meaning ascribed in the General Terms or other Contract Document.

PURPOSE

The Contract is awarded as a statewide contract on behalf of the Office of Management and Enterprise Services for software and services to support State agencies and other eligible Oklahoma Interlocal Entities. This Supplier will provide software, training, pre-sales assistance, documentation, installation, maintenance, support, configuration, customization, and license agreement administration.

1. Contract Term and Renewal Options

The initial Contract term, which begins on the effective date of the Contract, is one year and there are [4] one-year options to renew the Contract.

ATTACHMENT B

STATE OF OKLAHOMA GENERAL TERMS

This State of Oklahoma General Terms (“General Terms”) is a Contract Document in connection with a Contract awarded by the Office of Management and Enterprise Services on behalf of the State of Oklahoma.

In addition to other terms contained in an applicable Contract Document, Supplier and State agree to the following General Terms:

1 Scope and Contract Renewal

- 1.1** Supplier may not add products or services to its offerings under the Contract without the State’s prior written approval. Such request may require a competitive bid of the additional products or services. If the need arises for goods or services outside the scope of the Contract, Supplier shall contact the State.
- 1.2** At no time during the performance of the Contract shall the Supplier have the authority to obligate any Customer for payment for any products or services (a) when a corresponding encumbering document is not signed or (b) over and above an awarded Contract amount. Likewise, Supplier is not entitled to compensation for a product or service provided by or on behalf of Supplier that is neither requested nor accepted as satisfactory.
- 1.3** If applicable, prior to any Contract renewal, the State shall subjectively consider the value of the Contract to the State, the Supplier’s performance under the Contract, and shall review certain other factors, including but not limited to the: a) terms and conditions of Contract Documents to determine validity with current State and other applicable statutes and rules; b) current pricing and discounts offered by Supplier; and c) current products, services and support offered by Supplier. If the State determines changes to the Contract are required as a condition precedent to renewal, the State and Supplier will cooperate in good faith to evidence such required changes in an Addendum. Further, any request for a price increase in connection with a renewal or otherwise will be conditioned on the Supplier providing appropriate documentation supporting the request.
- 1.4** The State may extend the Contract for ninety (90) days beyond a final renewal term at the Contract compensation rate for the extended period. If the State

exercises such option to extend ninety (90) days, the State shall notify the Supplier in writing prior to Contract end date. The State, at its sole option and to the extent allowable by law, may choose to exercise subsequent ninety (90) day extensions at the Contract pricing rate, to facilitate the finalization of related terms and conditions of a new award or as needed for transition to a new Supplier.

- 1.5** Supplier understands that supplier registration expires annually and, pursuant to OAC 260:115-3-3, Supplier shall maintain its supplier registration with the State as a precondition to a renewal of the Contract.

2 Contract Effectiveness and Order of Priority

- 2.1** Unless specifically agreed in writing otherwise, the Contract is effective upon the date last signed by the parties. Supplier shall not commence work, commit funds, incur costs, or in any way act to obligate the State until the Contract is effective.
- 2.2** Contract Documents shall be read to be consistent and complementary. Any conflict among the Contract Documents shall be resolved by giving priority to Contract Documents in the following order of precedence:
- A.** any Addendum;
 - B.** any applicable Solicitation;
 - C.** any Contract-specific State terms contained in a Contract Document including, without limitation, information technology terms and terms specific to a statewide Contract or a State agency Contract;
 - D.** the terms contained in this Contract Document;
 - E.** any successful Bid as may be amended through negotiation and to the extent the Bid does not otherwise conflict with the Solicitation or applicable law;
 - F.** any statement of work, work order, or other similar ordering document as applicable; and
 - G.** other mutually agreed Contract Documents.
- 2.3** If there is a conflict between the terms contained in this Contract Document or in Contract-specific terms and an agreement provided by or on behalf of Supplier including but not limited to linked or supplemental documents which alter or diminish the rights of Customer or the State, the conflicting terms

provided by Supplier shall not take priority over this Contract Document or Acquisition-specific terms. In no event will any linked document alter or override such referenced terms except as specifically agreed in an Addendum.

- 2.4 Any Contract Document shall be legibly written in ink or typed. All Contract transactions, and any Contract Document related thereto, may be conducted by electronic means pursuant to the Oklahoma Uniform Electronic Transactions Act.

3 **Modification of Contract Terms and Contract Documents**

- 3.1 The Contract may only be modified, amended, or expanded by an Addendum. Any change to the Contract, including the addition of work or materials, the revision of payment terms, or the substitution of work or materials made unilaterally by the Supplier, is a material breach of the Contract. Unless otherwise specified by applicable law or rules, such changes, including without limitation, any unauthorized written Contract modification, shall be void and without effect and the Supplier shall not be entitled to any claim under the Contract based on those changes. No oral statement of any person shall modify or otherwise affect the terms, conditions, or specifications stated in the Contract.
- 3.2 Any additional terms on an ordering document provided by Supplier are of no effect and are void unless mutually executed. OMES bears no liability for performance, payment or failure thereof by the Supplier or by a Customer other than OMES in connection with an Acquisition.

4 **Definitions**

In addition to any defined terms set forth elsewhere in the Contract, the Oklahoma Central Purchasing Act and the Oklahoma Administrative Code, Title 260, the parties agree that, when used in the Contract, the following terms are defined as set forth below and may be used in the singular or plural form:

- 4.1 **Acquisition** means items, products, materials, supplies, services and equipment acquired by purchase, lease purchase, lease with option to purchase, value provided or rental under the Contract.
- 4.2 **Addendum** means a mutually executed, written modification to a Contract Document.
- 4.3 **Amendment** means a written change, addition, correction or revision to the Solicitation.
- 4.4 **Bid** means an offer a Bidder submits in response to the Solicitation.

- 4.5 **Bidder** means an individual or business entity that submits a Bid in response to the Solicitation.
- 4.6 **Contract** means the written, mutually agreed and binding legal relationship resulting from the Contract Documents and an appropriate encumbering document as may be amended from time to time, which evidences the final agreement between the parties with respect to the subject matter of the Contract.
- 4.7 **Contract Document** means this document; any master or enterprise agreement terms entered into between the parties that are mutually agreed to be applicable to the Contract; any Solicitation; any Contract-specific terms; any Supplier's Bid as may be negotiated; any statement of work, work order, or other similar mutually executed ordering document; other mutually executed documents and any Addendum.
- 4.8 **Customer** means the entity receiving goods or services contemplated by the Contract.
- 4.9 **Debarment** means action taken by a debarring official under federal or state law or regulations to exclude any business entity from inclusion on the Supplier list; bidding; offering to bid; providing a quote; receiving an award of contract with the State and may also result in cancellation of existing contracts with the State.
- 4.10 **Destination** means delivered to the receiving dock or other point specified in the applicable Contract Document.
- 4.11 **Indemnified Parties** means the State and Customer and/or its officers, directors, agents, employees, representatives, contractors, assignees and designees thereof.
- 4.12 **Inspection** means examining and testing an Acquisition (including, when appropriate, raw materials, components, and intermediate assemblies) to determine whether the Acquisition meets Contract requirements.
- 4.13 **Moral Rights** means any and all rights of paternity or integrity of the Work Product and the right to object to any modification, translation or use of the Work Product and any similar rights existing under the judicial or statutory law of any country in the world or under any treaty, regardless of whether or not such right is denominated or referred to as a moral right.
- 4.14 **OAC** means the Oklahoma Administrative Code.
- 4.15 **OMES** means the Office of Management and Enterprise Services.

- 4.16 Solicitation** means the document inviting Bids for the Acquisition referenced in the Contract and any amendments thereto.
- 4.17 State** means the government of the state of Oklahoma, its employees and authorized representatives, including without limitation any department, agency, or other unit of the government of the state of Oklahoma.
- 4.18 Supplier** means the Bidder with whom the State enters into the Contract awarded pursuant to the Solicitation or the business entity or individual that is a party to the Contract with the State.
- 4.19 Suspension** means action taken by a suspending official under federal or state law or regulations to suspend a Supplier from inclusion on the Supplier list; be eligible to submit Bids to State agencies and be awarded a contract by a State agency subject to the Central Purchasing Act.
- 4.20 Supplier Confidential Information** means certain confidential and proprietary information of Supplier that is clearly marked as confidential and agreed by the State Purchasing Director or Customer, as applicable, but does not include information excluded from confidentiality in provisions of the Contract or the Oklahoma Open Records Act.
- 4.21 Work Product** means any and all deliverables produced by Supplier under a statement of work or similar Contract Document issued pursuant to this Contract, including any and all tangible or intangible items or things that have been or will be prepared, created, developed, invented or conceived at any time following the Contract effective date including but not limited to any (i) works of authorship (such as manuals, instructions, printed material, graphics, artwork, images, illustrations, photographs, computer programs, computer software, scripts, object code, source code or other programming code, HTML code, flow charts, notes, outlines, lists, compilations, manuscripts, writings, pictorial materials, schematics, formulae, processes, algorithms, data, information, multimedia files, text web pages or web sites, other written or machine readable expression of such works fixed in any tangible media, and all other copyrightable works), (ii) trademarks, service marks, trade dress, trade names, logos, or other indicia of source or origin, (iii) ideas, designs, concepts, personality rights, methods, processes, techniques, apparatuses, inventions, formulas, discoveries, or improvements, including any patents, trade secrets and know-how, (iv) domain names, (v) any copies, and similar or derivative works to any of the foregoing, (vi) all documentation and materials related to any of the foregoing, (vii) all other goods, services or deliverables to be provided by or on behalf of Supplier under the Contract and (viii) all Intellectual Property Rights in any of the foregoing, and which are or were created,

prepared, developed, invented or conceived for the use of benefit of Customer in connection with this Contract or with funds appropriated by or for Customer or Customer's benefit (a) by any Supplier personnel or Customer personnel or (b) any Customer personnel who then became personnel to Supplier or any of its affiliates or subcontractors, where, although creation or reduction-to-practice is completed while the person is affiliated with Supplier or its personnel, any portion of same was created, invented or conceived by such person while affiliated with Customer.

5 Pricing

- 5.1** Pursuant to 68 O.S. §§ 1352, 1356, and 1404, State agencies are exempt from the assessment of State sales, use, and excise taxes. Further, State agencies and political subdivisions of the State are exempt from Federal Excise Taxes pursuant to Title 26 of the United States Code. Any taxes of any nature whatsoever payable by the Supplier shall not be reimbursed.
- 5.2** Pursuant to 74 O.S. §85.40, all travel expenses of Supplier must be included in the total Acquisition price.
- 5.3** The price of a product offered under the Contract shall include and Supplier shall prepay all shipping, packaging, delivery and handling fees. All product deliveries will be free on board Customer's Destination. No additional fees shall be charged by Supplier for standard shipping and handling. If Customer requests expedited or special delivery, Customer may be responsible for any charges for expedited or special delivery.

6 Ordering, Inspection, and Acceptance

- 6.1** Any product or service furnished under the Contract shall be ordered by issuance of a valid purchase order or other appropriate payment mechanism, including a pre-encumbrance, or by use of a valid Purchase Card. All orders and transactions are governed by the terms and conditions of the Contract. Any purchase order or other applicable payment mechanism dated prior to termination or expiration of the Contract shall be performed unless mutually agreed in writing otherwise.
- 6.2** Services will be performed in accordance with industry best practices and are subject to acceptance by the Customer. Notwithstanding any other provision in the Contract, deemed acceptance of a service or associated deliverable shall not apply automatically upon receipt of a deliverable or upon provision of a service.

Supplier warrants and represents that a product or deliverable furnished by or through the Supplier shall individually, and where specified by Supplier to perform as a system, be substantially uninterrupted and error-free in operation and guaranteed against faulty material and workmanship for a warranty period of the greater of ninety (90) days from the date of acceptance or the maximum allowed by the manufacturer. A defect in a product or deliverable furnished by or through the Supplier shall be repaired or replaced by Supplier at no additional cost or expense to the Customer if such defect occurs during the warranty period.

Any product to be delivered pursuant to the Contract shall be subject to final inspection and acceptance by the Customer at Destination. The Customer assumes no responsibility for a product until accepted by the Customer. Title and risk of loss or damage to a product shall be the responsibility of the Supplier until accepted. The Supplier shall be responsible for filing, processing, and collecting any and all damage claims accruing prior to acceptance.

Pursuant to OAC 260:115-9-5, payment for an Acquisition does not constitute final acceptance of the Acquisition. If subsequent inspection affirms that the Acquisition does not meet or exceed the specifications of the order or that the Acquisition has a latent defect, the Supplier shall be notified as soon as is reasonably practicable. The Supplier shall retrieve and replace the Acquisition at Supplier's expense or, if unable to replace, shall issue a refund to Customer. Refund under this section shall not be an exclusive remedy.

- 6.3 Supplier shall deliver products and services on or before the required date specified in a Contract Document. Failure to deliver timely may result in liquidated damages as set forth in the applicable Contract Document. Deviations, substitutions, or changes in a product or service, including changes of personnel directly providing services, shall not be made unless expressly authorized in writing by the Customer. Any substitution of personnel directly providing services shall be a person of comparable or greater skills, education and experience for performing the services as the person being replaced. Additionally, Supplier shall provide staff sufficiently experienced and able to perform with respect to any transitional services provided by Supplier in connection with termination or expiration of the Contract.
- 6.4 Product warranty and return policies and terms provided under any Contract Document will not be more restrictive or more costly than warranty and return policies and terms for other similarly situated customers for a like product.

7 Invoices and Payment

- 7.1** Supplier shall be paid upon submission of a proper invoice(s) at the prices stipulated in the Contract in accordance with 74 O.S. §85.44B which requires that payment be made only after products have been provided and accepted or services rendered and accepted.

The following terms additionally apply:

- A.** An invoice shall contain the purchase order number, description of products or services provided and the dates of such provision.
- B.** Failure to provide a timely and proper invoice may result in delay of processing the invoice for payment. Proper invoice is defined at OAC 260:10-1-2.
- C.** Payment of all fees under the Contract shall be due NET 45 days. Payment and interest on late payments are governed by 62 O.S. §34.72. Such interest is the sole and exclusive remedy for late payments by a State agency and no other late fees are authorized to be assessed pursuant to Oklahoma law.
- D.** The date from which an applicable early payment discount time is calculated shall be from the receipt date of a proper invoice. There is no obligation, however, to utilize an early payment discount.
- E.** If an overpayment or underpayment has been made to Supplier any subsequent payments to Supplier under the Contract may be adjusted to correct the account. A written explanation of the adjustment will be issued to Supplier.
- F.** Supplier shall have no right of setoff.
- G.** Because funds are typically dedicated to a particular fiscal year, an invoice will be paid only when timely submitted, which shall in no instance be later than six (6) months after the end of the fiscal year in which the goods are provided or services performed.
- H.** The Supplier shall accept payment by Purchase Card as allowed by Oklahoma law.

8 Maintenance of Insurance, Payment of Taxes, and Workers' Compensation

- 8.1** As a condition of this Contract, Supplier shall procure at its own expense, and provide proof of, insurance coverage with the applicable liability limits set

forth below and any approved subcontractor of Supplier shall procure and provide proof of the same coverage. The required insurance shall be underwritten by an insurance carrier with an A.M. Best rating of A- or better.

Such proof of coverage shall additionally be provided to the Customer if services will be provided by any of Supplier's employees, agents or subcontractors at any Customer premises and/or employer vehicles will be used in connection with performance of Supplier's obligations under the Contract. Supplier may not commence performance hereunder until such proof has been provided. Additionally, Supplier shall ensure each insurance policy includes a thirty (30) day notice of cancellation and name the State and its agencies as certificate holder and shall promptly provide proof to the State of any renewals, additions, or changes to such insurance coverage. Supplier's obligation to maintain insurance coverage under the Contract is a continuing obligation until Supplier has no further obligation under the Contract. Any combination of primary and excess or umbrella insurance may be used to satisfy the limits of coverage for Commercial General Liability, Auto Liability and Employers' Liability. Unless agreed between the parties and approved by the State Purchasing Director, the minimum acceptable insurance limits of liability are as follows:

- A.** Workers' Compensation and Employer's Liability Insurance in accordance with and to the extent required by applicable law;
- B.** Commercial General Liability Insurance covering the risks of personal injury, bodily injury (including death) and property damage, including coverage for contractual liability, with a limit of liability of not less than \$5,000,000 per occurrence;
- C.** Automobile Liability Insurance with limits of liability of not less than \$5,000,000 combined single limit each accident;
- D.** Directors and Officers Insurance which shall include Employment Practices Liability as well as Consultant's Computer Errors and Omissions Coverage, if information technology services are provided under the Contract, with limits not less than \$5,000,000 per occurrence;
- E.** Security and Privacy Liability insurance, including coverage for failure to protect confidential information and failure of the security of Supplier's computer systems that results in unauthorized access to Customer data with limits \$5,000,000 per occurrence; and
- F.** Additional coverage required in writing in connection with a particular Acquisition.

- 8.2** Supplier shall be entirely responsible during the existence of the Contract for the liability and payment of taxes payable by or assessed to Supplier or its employees, agents and subcontractors of whatever kind, in connection with the Contract. Supplier further agrees to comply with all state and federal laws applicable to any such persons, including laws regarding wages, taxes, insurance, and Workers' Compensation. Neither Customer nor the State shall be liable to the Supplier, its employees, agents, or others for the payment of taxes or the provision of unemployment insurance and/or Workers' Compensation or any benefit available to a State or Customer employee.
- 8.3** Supplier agrees to indemnify Customer, the State, and its employees, agents, representatives, contractors, and assignees for any and all liability, actions, claims, demands, or suits, and all related costs and expenses (including without limitation reasonable attorneys' fees and costs required to establish the right to indemnification) relating to tax liability, unemployment insurance and/or Workers' Compensation in connection with its performance under the Contract.

9 Compliance with Applicable Laws

- 9.1** As long as Supplier has an obligation under the terms of the Contract and in connection with performance of its obligations, the Supplier represents its present compliance, and shall have an ongoing obligation to comply, with all applicable federal, State, and local laws, rules, regulations, ordinances, and orders, as amended, including but not limited to the following:
- A.** Drug-Free Workplace Act of 1988 set forth at 41 U.S.C. §81.
 - B.** Section 306 of the Clean Air Act, Section 508 of the Clean Water Act, Executive Order 11738, and Environmental Protection Agency Regulations which prohibit the use of facilities included on the EPA List of Violating Facilities under nonexempt federal contracts, grants or loans;
 - C.** Prospective participant requirements set at 45 C.F.R. part 76 in connection with Debarment, Suspension and other responsibility matters;
 - D.** 1964 Civil Rights Act, Title IX of the Education Amendment of 1972, Section 504 of the Rehabilitation Act of 1973, Americans with Disabilities Act of 1990, and Executive Orders 11246 and 11375;
 - E.** Anti-Lobbying Law set forth at 31 U.S.C. §1325 and as implemented at 45 C.F.R. part 93;

- F.** Requirements of Internal Revenue Service Publication 1075 regarding use, access and disclosure of Federal Tax Information (as defined therein);
 - G.** Obtaining certified independent audits conducted in accordance with Government Auditing Standards and Office of Management and Budget Uniform Guidance, 2 CFR 200 Subpart F §200.500 et seq. with approval and work paper examination rights of the applicable procuring entity;
 - H.** Requirements of the Oklahoma Taxpayer and Citizen Protection Act of 2007, 25 O.S. §1312 and applicable federal immigration laws and regulations and be registered and participate in the Status Verification System. The Status Verification System is defined at 25 O.S. §1312, includes but is not limited to the free Employment Verification Program (E-Verify) through the Department of Homeland Security, and is available at www.dhs.gov/E-Verify;
 - I.** Requirements of the Health Insurance Portability and Accountability Act of 1996; Health Information Technology for Economic and Clinical Health Act; Payment Card Industry Security Standards; Criminal Justice Information System Security Policy and Security Addendum; and Family Educational Rights and Privacy Act; and
 - J.** Be registered as a business entity licensed to do business in the State, have obtained a sales tax permit, and be current on franchise tax payments to the State, as applicable.
- 9.2** The Supplier's employees, agents and subcontractors shall adhere to applicable Customer policies including, but not limited to acceptable use of Internet and electronic mail, facility and data security, press releases, and public relations. As applicable, the Supplier shall adhere to the State Information Security Policy, Procedures, Guidelines set forth at https://omes.ok.gov/sites/g/files/gmc316/f/InfoSecPPG_0.pdf. Supplier is responsible for reviewing and relaying such policies covering the above to the Supplier's employees, agents and subcontractors.
- 9.3** At no additional cost to Customer, the Supplier shall maintain all applicable licenses and permits required in association with its obligations under the Contract.
- 9.4** In addition to compliance under subsection 9.1 above, Supplier shall have a continuing obligation to comply with applicable Customer-specific mandatory

contract provisions required in connection with the receipt of federal funds or other funding source.

- 9.5** The Supplier is responsible to review and inform its employees, agents, and subcontractors who provide a product or perform a service under the Contract of the Supplier's obligations under the Contract and Supplier certifies that its employees and each such subcontractor shall comply with minimum requirements and applicable provisions of the Contract. At the request of the State, Supplier shall promptly provide adequate evidence that such persons are its employees, agents or approved subcontractors and have been informed of their obligations under the Contract.
- 9.6** As applicable, Supplier agrees to comply with the Governor's Executive Orders related to the use of any tobacco product, electronic cigarette or vaping device on any and all properties owned, leased, or contracted for use by the State, including but not limited to all buildings, land and vehicles owned, leased, or contracted for use by agencies or instrumentalities of the State.
- 9.7** The execution, delivery and performance of the Contract and any ancillary documents by Supplier will not, to the best of Supplier's knowledge, violate, conflict with, or result in a breach of any provision of, or constitute a default (or an event which, with notice or lapse of time or both, would constitute a default) under, or result in the termination of, any written contract or other instrument between Supplier and any third party.
- 9.8** Supplier represents that it has the ability to pay its debts when due and it does not anticipate the filing of a voluntary or involuntary bankruptcy petition or appointment of a receiver, liquidator or trustee.
- 9.9** Supplier represents that, to the best of its knowledge, any litigation or claim or any threat thereof involving Supplier has been disclosed in writing to the State and Supplier is not aware of any other litigation, claim or threat thereof.
- 9.10** If services provided by Supplier include delivery of an electronic communication, Supplier shall ensure such communication and any associated support documents are compliant with Section 508 of the Federal Rehabilitation Act and with State standards regarding accessibility. Should any communication or associated support documents be non-compliant, Supplier shall correct and re-deliver such communication immediately upon discovery or notice, at no additional cost to the State. Additionally, as part of compliance with accessibility requirements where documents are only provided in non-electronic format, Supplier shall promptly provide such communication and any associated support documents in an alternate format

usable by individuals with disabilities upon request and at no additional cost, which may originate from an intended recipient or from the State.

10 Audits and Records Clause

- 10.1** As used in this clause and pursuant to 67 O.S. §203, “record” includes a document, book, paper, photograph, microfilm, computer tape, disk, record, sound recording, film recording, video record, accounting procedures and practices, and other data, regardless of type and regardless of whether such items are in written form, in the form of computer data, or in any other form. Supplier agrees any pertinent federal or State agency or governing entity of a Customer shall have the right to examine and audit, at no additional cost to a Customer, all records relevant to the execution and performance of the Contract except, unless otherwise agreed, costs of Supplier that comprise pricing under the Contract.
- 10.2** The Supplier is required to retain records relative to the Contract for the duration of the Contract and for a period of seven (7) years following completion or termination of an Acquisition unless otherwise indicated in the Contract terms. If a claim, audit, litigation or other action involving such records is started before the end of the seven-year period, the records are required to be maintained for two (2) years from the date that all issues arising out of the action are resolved, or until the end of the seven (7) year retention period, whichever is later.
- 10.3** Pursuant to 74 O.S. §85.41, if professional services are provided hereunder, all items of the Supplier that relate to the professional services are subject to examination by the State agency, State Auditor and Inspector and the State Purchasing Director.

11 Confidentiality

- 11.1** The Supplier shall maintain strict security of all State and citizen data and records entrusted to it or to which the Supplier gains access, in accordance with and subject to applicable federal and State laws, rules, regulations, and policies and shall use any such data and records only as necessary for Supplier to perform its obligations under the Contract. The Supplier further agrees to evidence such confidentiality obligation in a separate writing if required under such applicable federal or State laws, rules and regulations. The Supplier warrants and represents that such information shall not be sold, assigned, conveyed, provided, released, disseminated or otherwise disclosed by Supplier, its employees, officers, directors, subsidiaries, affiliates, agents, representatives, assigns, subcontractors, independent contractors, successor or any other persons or entities without Customer’s prior express written

permission. Supplier shall instruct all such persons and entities that the confidential information shall not be disclosed or used without the Customer's prior express written approval except as necessary for Supplier to render services under the Contract. The Supplier further warrants that it has a tested and proven system in effect designed to protect all confidential information.

- 11.2** Supplier shall establish, maintain and enforce agreements with all such persons and entities that have access to State and citizen data and records to fulfill Supplier's duties and obligations under the Contract and to specifically prohibit any sale, assignment, conveyance, provision, release, dissemination or other disclosure of any State or citizen data or records except as required by law or allowed by written prior approval of the Customer.
- 11.3** Supplier shall immediately report to the Customer any and all unauthorized use, appropriation, sale, assignment, conveyance, provision, release, access, acquisition, disclosure or other dissemination of any State or citizen data or records of which it or its parent company, subsidiaries, affiliates, employees, officers, directors, assignees, agents, representatives, independent contractors, and subcontractors is aware or have knowledge or reasonable should have knowledge. The Supplier shall also promptly furnish to Customer full details of the unauthorized use, appropriation, sale, assignment, conveyance, provision, release, access, acquisition, disclosure or other dissemination, or attempt thereof, and use its best efforts to assist the Customer in investigating or preventing the reoccurrence of such event in the future. The Supplier shall cooperate with the Customer in connection with any litigation and investigation deemed necessary by the Customer to protect any State or citizen data and records and shall bear all costs associated with the investigation, response and recovery in connection with any breach of State or citizen data or records including but not limited to credit monitoring services with a term of at least three (3) years, all notice-related costs and toll free telephone call center services.
- 11.4** Supplier further agrees to promptly prevent a reoccurrence of any unauthorized use, appropriation, sale, assignment, conveyance, provision, release, access, acquisition, disclosure or other dissemination of State or citizen data and records.
- 11.5** Supplier acknowledges that any improper use, appropriation, sale, assignment, conveyance, provision, release, access, acquisition, disclosure or other dissemination of any State data or records to others may cause immediate and irreparable harm to the Customer and certain beneficiaries and may violate state or federal laws and regulations. If the Supplier or its affiliates, parent company, subsidiaries, employees, officers, directors, assignees, agents,

representatives, independent contractors, and subcontractors improperly use, appropriate, sell, assign, convey, provide, release, access, acquire, disclose or otherwise disseminate such confidential information to any person or entity in violation of the Contract, the Customer will immediately be entitled to injunctive relief and/or any other rights or remedies available under this Contract, at equity or pursuant to applicable statutory, regulatory, and common law without a cure period.

11.6 The Supplier shall immediately forward to the State Purchasing Director, and any other applicable person listed in the Notices section(s) of the Contract, any request by a third party for data or records in the possession of the Supplier or any subcontractor or to which the Supplier or subcontractor has access and Supplier shall fully cooperate with all efforts to protect the security and confidentiality of such data or records in response to a third party request.

11.7 Customer may be provided access to Supplier Confidential Information. State agencies are subject to the Oklahoma Open Records Act and Supplier acknowledges information marked confidential information will be disclosed to the extent permitted under the Open Records Act and in accordance with this section. Nothing herein is intended to waive the State Purchasing Director's authority under OAC 260:115-3-9 in connection with Bid information requested to be held confidential by a Bidder. Notwithstanding the foregoing, Supplier Confidential Information shall not include information that: (i) is or becomes generally known or available by public disclosure, commercial use or otherwise and is not in contravention of this Contract; (ii) is known and has been reduced to tangible form by the receiving party before the time of disclosure for the first time under this Contract and without other obligations of confidentiality; (iii) is independently developed without the use of any of Supplier Confidential Information; (iv) is lawfully obtained from a third party (without any confidentiality obligation) who has the right to make such disclosure or (v) résumé, pricing or marketing materials provided to the State. In addition, the obligations in this section shall not apply to the extent that the applicable law or regulation requires disclosure of Supplier Confidential Information, provided that the Customer provides reasonable written notice, pursuant to Contract notice provisions, to the Supplier so that the Supplier may promptly seek a protective order or other appropriate remedy.

12 Conflict of Interest

In addition to any requirement of law or of a professional code of ethics or conduct, the Supplier, its employees, agents and subcontractors are required to disclose any outside activity or interest that conflicts or may conflict with the best interest of the State. Prompt disclosure is required under this section if the activity or interest is

related, directly or indirectly, to any person or entity currently under contract with or seeking to do business with the State, its employees or any other third-party individual or entity awarded a contract with the State. Further, as long as the Supplier has an obligation under the Contract, any plan, preparation or engagement in any such activity or interest shall not occur without prior written approval of the State. Any conflict of interest shall, at the sole discretion of the State, be grounds for partial or whole termination of the Contract.

13 Assignment and Permitted Subcontractors

- 13.1** Supplier's obligations under the Contract may not be assigned or transferred to any other person or entity without the prior written consent of the State which may be withheld at the State's sole discretion. Should Supplier assign its rights to payment, in whole or in part, under the Contract, Supplier shall provide the State and all affected Customers with written notice of the assignment. Such written notice shall be delivered timely and contain details sufficient for affected Customers to perform payment obligations without any delay caused by the assignment.
- 13.2** Notwithstanding the foregoing, the Contract may be assigned by Supplier to any corporation or other entity in connection with a merger, consolidation, sale of all equity interests of the Supplier, or a sale of all or substantially all of the assets of the Supplier to which the Contract relates. In any such case, said corporation or other entity shall by operation of law or expressly in writing assume all obligations of the Supplier as fully as if it had been originally made a party to the Contract. Supplier shall give the State and all affected Customers prior written notice of said assignment. Any assignment or delegation in violation of this subsection shall be void.
- 13.3** If the Supplier is permitted to utilize subcontractors in support of the Contract, the Supplier shall remain solely responsible for its obligations under the terms of the Contract, for its actions and omissions and those of its agents, employees and subcontractors and for payments to such persons or entities. Prior to a subcontractor being utilized by the Supplier, the Supplier shall obtain written approval of the State of such subcontractor and each employee, as applicable to a particular Acquisition, of such subcontractor proposed for use by the Supplier. Such approval is within the sole discretion of the State. Any proposed subcontractor shall be identified by entity name, and by employee name, if required by the particular Acquisition, in the applicable proposal and shall include the nature of the services to be performed. As part of the approval request, the Supplier shall provide a copy of a written agreement executed by the Supplier and subcontractor setting forth that such subcontractor is bound by and agrees, as applicable, to perform the same covenants and be subject to

the same conditions and make identical certifications to the same facts and criteria, as the Supplier under the terms of all applicable Contract Documents. Supplier agrees that maintaining such agreement with any subcontractor and obtaining prior written approval by the State of any subcontractor and associated employees shall be a continuing obligation. The State further reserves the right to revoke approval of a subcontractor or an employee thereof in instances of poor performance, misconduct or for other similar reasons.

13.4 All payments under the Contract shall be made directly to the Supplier, except as provided in subsection A above regarding the Supplier's assignment of payment. No payment shall be made to the Supplier for performance by unapproved or disapproved employees of the Supplier or a subcontractor.

13.5 Rights and obligations of the State or a Customer under the terms of this Contract may be assigned or transferred, at no additional cost, to other Customer entities.

14 Background Checks and Criminal History Investigations

Prior to the commencement of any services, background checks and criminal history investigations of the Supplier's employees and subcontractors who will be providing services may be required and, if so, the required information shall be provided to the State in a timely manner. Supplier's access to facilities, data and information may be withheld prior to completion of background verification acceptable to the State. The costs of additional background checks beyond Supplier's normal hiring practices shall be the responsibility of the Customer unless such additional background checks are required solely because Supplier will not provide results of its otherwise acceptable normal background checks; in such an instance, Supplier shall pay for the additional background checks. Supplier will coordinate with the State and its employees to complete the necessary background checks and criminal history investigations. Should any employee or subcontractor of the Supplier who will be providing services under the Contract not be acceptable as a result of the background check or criminal history investigation, the Customer may require replacement of the employee or subcontractor in question and, if no suitable replacement is made within a reasonable time, terminate the purchase order or other payment mechanism associated with the project or services.

15 Patents and Copyrights

Without exception, a product or deliverable price shall include all royalties or costs owed by the Supplier to any third party arising from the use of a patent, intellectual property, copyright or other property right held by such third party. Should any third party threaten or make a claim that any portion of a product or service provided by Supplier under the Contract infringes that party's patent, intellectual property,

copyright or other property right, Supplier shall enable each affected Customer to legally continue to use, or modify for use, the portion of the product or service at issue or replace such potentially infringing product, or re-perform or redeliver in the case of a service, with at least a functional non-infringing equivalent. Supplier's duty under this section shall extend to include any other product or service rendered materially unusable as intended due to replacement or modification of the product or service at issue. If the Supplier determines that none of these alternatives are reasonably available, the State shall return such portion of the product or deliverable at issue to the Supplier, upon written request, in exchange for a refund of the price paid for such returned goods as well as a refund or reimbursement, if applicable, of the cost of any other product or deliverable rendered materially unusable as intended due to removal of the portion of product or deliverable at issue. Any remedy provided under this section is not an exclusive remedy and is not intended to operate as a waiver of legal or equitable remedies because of acceptance of relief provided by Supplier.

16 Indemnification

16.1 Acts or Omissions

- A.** Supplier shall defend and indemnify the Indemnified Parties, as applicable, for any and all liability, claims, damages, losses, costs, expenses, demands, suits and actions of third parties (including without limitation reasonable attorneys' fees and costs required to establish the right to indemnification) arising out of, or resulting from any action or claim for bodily injury, death, or property damage brought against any of the Indemnified parties to the extent arising from any negligent act or omission or willful misconduct of the Supplier or its agents, employees, or subcontractors in the execution or performance of the Contract.
- B.** To the extent Supplier is found liable for loss, damage, or destruction of any property of Customer due to negligence, misconduct, wrongful act, or omission on the part of the Supplier, its employees, agents, representatives, or subcontractors, the Supplier and Customer shall use best efforts to mutually negotiate an equitable settlement amount to repair or replace the property unless such loss, damage or destruction is of such a magnitude that repair or replacement is not a reasonable option. Such amount shall be invoiced to, and is payable by, Supplier sixty (60) calendar days after the date of Supplier's receipt of an invoice for the negotiated settlement amount.

16.2 Infringement

Supplier shall indemnify the Indemnified Parties, as applicable, for all liability, claims, damages, losses, costs, expenses, demands, suits and actions of third parties (including without limitation reasonable attorneys' fees and costs required to establish the right to indemnification) arising from or in connection with Supplier's breach of its representations and warranties in the Contract or alleged infringement of any patent, intellectual property, copyright or other property right in connection with a product or service provided under the Contract. Supplier's duty under this section is reduced to the extent a claimed infringement results from: (a) a Customer's or user's content; (b) modifications by Customer or third party to a product delivered under the Contract or combinations of the product with any non-Supplier-provided services or products unless Supplier recommended or participated in such modification or combination; (c) use of a product or service by Customer in violation of the Contract unless done so at the direction of Supplier, or (d) a non-Supplier product that has not been provided to the State by, through or on behalf of Supplier as opposed to its combination with products Supplier provides to or develops for the State or a Customer as a system.

16.3 Notice and Cooperation

In connection with indemnification obligations under the Contract, the parties agree to furnish prompt written notice to each other of any third-party claim. Any Customer affected by the claim will reasonably cooperate with Supplier and defense of the claim to the extent its interests are aligned with Supplier. Supplier shall use counsel reasonably experienced in the subject matter at issue and will not settle a claim without the written consent of the party being defended, which consent will not be unreasonably withheld or delayed, except that no consent will be required to settle a claim against Indemnified Parties that are not a State agency, where relief against the Indemnified Parties is limited to monetary damages that are paid by the defending party under indemnification provisions of the Contract.

16.4 Coordination of Defense

In connection with indemnification obligations under the Contract, when a State agency is a named defendant in any filed or threatened lawsuit, the defense of the State agency shall be coordinated by the Attorney General of Oklahoma, or the Attorney General may authorize the Supplier to control the defense and any related settlement negotiations; provided, however, Supplier shall not agree to any settlement of claims against the State without obtaining advance written concurrence from the Attorney General. If the Attorney General does not authorize sole control of the defense and settlement negotiations to Supplier, Supplier shall have authorization to equally

participate in any proceeding related to the indemnity obligation under the Contract and shall remain responsible to indemnify the applicable Indemnified Parties.

16.5 Limitation of Liability

- A.** With respect to any claim or cause of action arising under or related to the Contract, neither the State nor any Customer shall be liable to Supplier for lost profits, lost sales or business expenditures, investments, or commitments in connection with any business, loss of any goodwill, or for any other indirect, incidental, punitive, special or consequential damages, even if advised of the possibility of such damages.
- B.** Notwithstanding anything to the contrary in the Contract, no provision shall limit damages, expenses, costs, actions, claims, and liabilities arising from or related to property damage, bodily injury or death caused by Supplier or its employees, agents or subcontractors; indemnity, security or confidentiality obligations under the Contract; the bad faith, negligence, intentional misconduct or other acts for which applicable law does not allow exemption from liability of Supplier or its employees, agents or subcontractors.
- C.** The limitation of liability and disclaimers set forth in the Contract will apply regardless of whether Customer has accepted a product or service. The parties agree that Supplier has set its fees and entered into the Contract in reliance on the disclaimers and limitations set forth herein, that the same reflect an allocation of risk between the parties and form an essential basis of the bargain between the parties. These limitations shall apply notwithstanding any failure of essential purpose of any limited remedy.

17 Termination for Funding Insufficiency

- 17.1** Notwithstanding anything to the contrary in any Contract Document, the State may terminate the Contract in whole or in part if funds sufficient to pay obligations under the Contract are not appropriated or received from an intended third-party funding source. In the event of such insufficiency, Supplier will be provided at least fifteen (15) calendar days' written notice of termination. Any partial termination of the Contract under this section shall not be construed as a waiver of, and shall not affect, the rights and obligations of any party regarding portions of the Contract that are not terminated. The determination by the State of insufficient funding shall be accepted by, and shall be final and binding on, the Supplier.

- 17.2** Upon receipt of notice of a termination, Supplier shall immediately comply with the notice terms and take all necessary steps to minimize the incurrence of costs allocable to the work affected by the notice. If a purchase order or other payment mechanism has been issued and a product or service has been accepted as satisfactory prior to the effective date of termination, the termination does not relieve an obligation to pay for the product or service but there shall not be any liability for further payments ordinarily due under the Contract or for any damages or other amounts caused by or associated with such termination. Any amount paid to Supplier in the form of prepaid fees that are unused when the Contractor certain obligations are terminated shall be refunded.
- 17.3** The State's exercise of its right to terminate the Contract under this section shall not be considered a default or breach under the Contract or relieve the Supplier of any liability for claims arising under the Contract.

18 Termination for Cause

- 18.1** Supplier may terminate the Contract if (i) it has provided the State with written notice of material breach and (ii) the State fails to cure such material breach within thirty (30) days of receipt of written notice. If there is more than one Customer, material breach by a Customer does not give rise to a claim of material breach as grounds for termination by Supplier of the Contract as a whole. The State may terminate the Contract in whole or in part if (i) it has provided Supplier with written notice of material breach, and (ii) Supplier fails to cure such material breach within thirty (30) days of receipt of written notice. Any partial termination of the Contract under this section shall not be construed as a waiver of, and shall not affect, the rights and obligations of any party regarding portions of the Contract that are not terminated.
- 18.2** The State may terminate the Contract in whole or in part immediately without a thirty (30) day written notice to Supplier if (i) Supplier fails to comply with confidentiality, privacy, security, environmental or safety requirements applicable to Supplier's performance or obligations under the Contract; (ii) Supplier's material breach is reasonably determined to be an impediment to the function of the State and detrimental to the State or to cause a condition precluding the thirty (30) day notice or (iii) when the State determines that an administrative error in connection with award of the Contract occurred prior to Contract performance.
- 18.3** Upon receipt of notice of a termination, Supplier shall immediately comply with the notice terms and take all necessary steps to minimize the incurrence

of costs allocable to the work affected by the notice. If a purchase order or other payment mechanism has been issued and a product or service has been accepted as satisfactory prior to the effective date of termination, the termination does not relieve an obligation to pay for the product or service but there shall not be any liability for further payments ordinarily due under the Contract or for any damages or other amounts caused by or associated with such termination. Such termination is not an exclusive remedy but is in addition to any other rights and remedies provided for by law. Any amount paid to Supplier in the form of prepaid fees that are unused when the Contract or certain obligations are terminated shall be refunded. Termination of the Contract under this section, in whole or in part, shall not relieve the Supplier of liability for claims arising under the Contract.

- 18.4** The Supplier's repeated failure to provide an acceptable product or service; Supplier's unilateral revision of linked or supplemental terms that have a materially adverse impact on a Customer's rights or obligations under the Contract (except as required by a governmental authority); actual or anticipated failure of Supplier to perform its obligations under the Contract; Supplier's inability to pay its debts when due; assignment for the benefit of Supplier's creditors; or voluntary or involuntary appointment of a receiver or filing of bankruptcy of Supplier shall constitute a material breach of the Supplier's obligations, which may result in partial or whole termination of the Contract. This subsection is not intended as an exhaustive list of material breach conditions. Termination may also result from other instances of failure to adhere to the Contract provisions and for other reasons provided for by applicable law, rules or regulations; without limitation, OAC 260:115-9-9 is an example.

19 Termination for Convenience

- 19.1** The State may terminate the Contract, in whole or in part, for convenience if it is determined that termination is in the State's best interest. In the event of a termination for convenience, Supplier will be provided at least thirty (30) days' written notice of termination. Any partial termination of the Contract shall not be construed as a waiver of, and shall not affect, the rights and obligations of any party regarding portions of the Contract that remain in effect.
- 19.2** Upon receipt of notice of such termination, Supplier shall immediately comply with the notice terms and take all necessary steps to minimize the incurrence of costs allocable to the work affected by the notice. If a purchase order or other payment mechanism has been issued and a product or service has been accepted as satisfactory prior to the effective date of termination, the termination does not relieve an obligation to pay for the product or service but

there shall not be any liability for further payments ordinarily due under the Contract or for any damages or other amounts caused by or associated with such termination. Such termination shall not be an exclusive remedy but shall be in addition to any other rights and remedies provided for by law. Any amount paid to Supplier in the form of prepaid fees that are unused when the Contract or certain obligations are terminated shall be refunded. Termination of the Contract under this section, in whole or in part, shall not relieve the Supplier of liability for claims arising under the Contract.

20 Suspension of Supplier

- 20.1** Supplier may be subject to Suspension without advance notice and may additionally be suspended from activities under the Contract if Supplier fails to comply with confidentiality, privacy, security, environmental or safety requirements applicable to Supplier's performance or obligations under the Contract.
- 20.2** Upon receipt of a notice pursuant to this section, Supplier shall immediately comply with the notice terms and take all necessary steps to minimize the incurrence of costs allocable to the work affected by the notice. If a purchase order or other payment mechanism has been issued and a product or service has been accepted as satisfactory prior to receipt of notice by Supplier, the Suspension does not relieve an obligation to pay for the product or service but there shall not be any liability for further payments ordinarily due under the Contract during a period of Suspension or suspended activity or for any damages or other amounts caused by or associated with such Suspension or suspended activity. A right exercised under this section shall not be an exclusive remedy but shall be in addition to any other rights and remedies provided for by law. Any amount paid to Supplier in the form of prepaid fees attributable to a period of Suspension or suspended activity shall be refunded.
- 20.3** Such Suspension may be removed, or suspended activity may resume, at the earlier of such time as a formal notice is issued that authorizes the resumption of performance under the Contract or at such time as a purchase order or other appropriate encumbrance document is issued. This subsection is not intended to operate as an affirmative statement that such resumption will occur.

21 Certification Regarding Debarment, Suspension, and Other Responsibility Matters

The certification made by Supplier with respect to Debarment, Suspension, certain indictments, convictions, civil judgments and terminated public contracts is a material representation of fact upon which reliance was placed when entering into the Contract.

A determination that Supplier knowingly rendered an erroneous certification, in addition to other available remedies, may result in whole or partial termination of the Contract for Supplier's default. Additionally, Supplier shall promptly provide written notice to the State Purchasing Director if the certification becomes erroneous due to changed circumstances.

22 Certification Regarding State Employees Prohibition From Fulfilling Services

Pursuant to 74 O.S. § 85.42, the Supplier certifies that no person involved in any manner in development of the Contract employed by the State shall be employed to fulfill any services provided under the Contract.

23 Force Majeure

23.1 Either party shall be temporarily excused from performance to the extent delayed as a result of unforeseen causes beyond its reasonable control including fire or other similar casualty, act of God, strike or labor dispute, war or other violence, or any law, order or requirement of any governmental agency or authority provided the party experiencing the force majeure event has prudently and promptly acted to take any and all steps within the party's control to ensure continued performance and to shorten duration of the event. If a party's performance of its obligations is materially hindered as a result of a force majeure event, such party shall promptly notify the other party of its best reasonable assessment of the nature and duration of the force majeure event and steps it is taking, and plans to take, to mitigate the effects of the force majeure event. The party shall use commercially reasonable best efforts to continue performance to the extent possible during such event and resume full performance as soon as reasonably practicable.

23.2 Subject to the conditions set forth above, non-performance as a result of a force majeure event shall not be deemed a default. However, a purchase order or other payment mechanism may be terminated if Supplier cannot cause delivery of a product or service in a timely manner to meet the business needs of Customer. Supplier is not entitled to payment for products or services not received and, therefore, amounts payable to Supplier during the force majeure event shall be equitably adjusted downward.

23.3 Notwithstanding the foregoing or any other provision in the Contract, (i) the following are not a force majeure event under the Contract: (a) shutdowns, disruptions or malfunctions in Supplier's system or any of Supplier's telecommunication or internet services other than as a result of general and widespread internet or telecommunications failures that are not limited to Supplier's systems or (b) the delay or failure of Supplier or subcontractor personnel to perform any obligation of Supplier hereunder unless such delay

or failure to perform is itself by reason of a force majeure event and (ii) no force majeure event modifies or excuses Supplier's obligations related to confidentiality, indemnification, data security or breach notification obligations set forth herein.

24 Security of Property and Personnel

In connection with Supplier's performance under the Contract, Supplier may have access to Customer personnel, premises, data, records, equipment and other property. Supplier shall use commercially reasonable best efforts to preserve the safety and security of such personnel, premises, data, records, equipment, and other property of Customer. Supplier shall be responsible for damage to such property to the extent such damage is caused by its employees or subcontractors and shall be responsible for loss of Customer property in its possession, regardless of cause. If Supplier fails to comply with Customer's security requirements, Supplier is subject to immediate suspension of work as well as termination of the associated purchase order or other payment mechanism.

25 Notices

All notices, approvals or requests allowed or required by the terms of any Contract Document shall be in writing, reference the Contract with specificity and deemed delivered upon receipt or upon refusal of the intended party to accept receipt of the notice. In addition to other notice requirements in the Contract and the designated Supplier contact provided in a successful Bid, notices shall be sent to the State at the physical address set forth below. Notice information may be updated in writing to the other party as necessary. Notwithstanding any other provision of the Contract, confidentiality, breach and termination-related notices shall not be delivered solely via e-mail.

If sent to the State:

State Purchasing Director
2401 North Lincoln Boulevard, Suite 116
Oklahoma City, Oklahoma 73105

With a copy, which shall not constitute notice, to:

Purchasing Division Deputy General Counsel
2401 North Lincoln Boulevard, Suite 116
Oklahoma City, Oklahoma 73105

26 Miscellaneous

26.1 Choice of Law and Venue

Any claim, dispute, or litigation relating to the Contract Documents, in the singular or in the aggregate, shall be governed by the laws of the State without regard to application of choice of law principles. Pursuant to 74 O.S. §85.14, where federal granted funds are involved, applicable federal laws, rules and regulations shall govern to the extent necessary to insure benefit of such federal funds to the State. Venue for any action, claim, dispute, or litigation relating in any way to the Contract Documents, shall be in Oklahoma County, Oklahoma.

26.2 No Guarantee of Products or Services Required

The State shall not guarantee any minimum or maximum amount of Supplier products or services required under the Contract.

26.3 Employment Relationship

The Contract does not create an employment relationship. Individuals providing products or performing services pursuant to the Contract are not employees of the State or Customer and, accordingly are not eligible for any rights or benefits whatsoever accruing to such employees.

26.4 Transition Services

If transition services are needed at the time of Contract expiration or termination, Supplier shall provide such services on a month-to-month basis, at the contract rate or other mutually agreed rate. Supplier shall provide a proposed transition plan, upon request, and cooperate with any successor supplier and with establishing a mutually agreeable transition plan. Failure to cooperate may be documented as poor performance of Supplier.

26.5 Publicity

The existence of the Contract or any Acquisition is in no way an endorsement of Supplier, the products or services and shall not be so construed by Supplier in any advertising or publicity materials. Supplier agrees to submit to the State all advertising, sales, promotion, and other publicity matters relating to the Contract wherein the name of the State or any Customer is mentioned or language used from which, in the State's judgment, an endorsement may be inferred or implied. Supplier further agrees not to publish or use such advertising, sales promotion, or publicity matter or release any informational pamphlets, notices, press releases, research reports, or similar public notices concerning the Contract or any Acquisition hereunder without obtaining the prior written approval of the State.

26.6 Open Records Act

Supplier acknowledges that all State agencies and certain other Customers are subject to the Oklahoma Open Records Act set forth at 51 O.S. §24A-1 *et seq.* Supplier also acknowledges that compliance with the Oklahoma Open Records Act and all opinions of the Oklahoma Attorney General concerning the Act is required.

26.7 Failure to Enforce

Failure by the State or a Customer at any time to enforce a provision of, or exercise a right under, the Contract shall not be construed as a waiver of any such provision. Such failure to enforce or exercise shall not affect the validity of any Contract Document, or any part thereof, or the right of the State or a Customer to enforce any provision of, or exercise any right under, the Contract at any time in accordance with its terms. Likewise, a waiver of a breach of any provision of a Contract Document shall not affect or waive a subsequent breach of the same provision or a breach of any other provision in the Contract.

26.8 Mutual Responsibilities

- A.** No party to the Contract grants the other the right to use any trademarks, trade names, other designations in any promotion or publication without the express written consent by the other party.
- B.** The Contract is a non-exclusive contract and each party is free to enter into similar agreements with others.
- C.** The Customer and Supplier each grant the other only the licenses and rights specified in the Contract and all other rights and interests are expressly reserved.
- D.** The Customer and Supplier shall reasonably cooperate with each other and any Supplier to which the provision of a product and/or service under the Contract may be transitioned after termination or expiration of the Contract.
- E.** Except as otherwise set forth herein, where approval, acceptance, consent, or similar action by a party is required under the Contract, such action shall not be unreasonably delayed or withheld.

26.9 Invalid Term or Condition

To the extent any term or condition in the Contract conflicts with a compulsory applicable State or United States law or regulation, such Contract term or

condition is void and unenforceable. By executing any Contract Document which contains a conflicting term or condition, no representation or warranty is made regarding the enforceability of such term or condition. Likewise, any applicable State or federal law or regulation which conflicts with the Contract or any non-conflicting applicable State or federal law or regulation is not waived.

26.10 Severability

If any provision of a Contract Document, or the application of any term or condition to any party or circumstances, is held invalid or unenforceable for any reason, the remaining provisions shall continue to be valid and enforceable and the application of such provision to other parties or circumstances shall remain valid and in full force and effect. If a court finds that any provision of this contract is invalid or unenforceable, but that by limiting such provision it would become valid and enforceable, then such provision shall be deemed to be written, construed, and enforced as so limited.

26.11 Section Headings

The headings used in any Contract Document are for convenience only and do not constitute terms of the Contract.

26.12 Sovereign Immunity

Notwithstanding any provision in the Contract, the Contract is entered into subject to the State's Constitution, statutes, common law, regulations, and the doctrine of sovereign immunity, none of which are waived by the State nor any other right or defense available to the State.

26.13 Survival

As applicable, performance under all license, subscription, service agreements, statements of work, transition plans and other similar Contract Documents entered into between the parties under the terms of the Contract shall survive Contract expiration. Additionally, rights and obligations under the Contract which by their nature should survive including, without limitation, certain payment obligations invoiced prior to expiration or termination; confidentiality obligations; security incident and data breach obligations and indemnification obligations, remain in effect after expiration or termination of the Contract.

26.14 Entire Agreement

The Contract Documents taken together as a whole constitute the entire agreement between the parties. No statement, promise, condition,

understanding, inducement or representation, oral or written, expressed or implied, which is not contained in a Contract Document shall be binding or valid. The Supplier's representations and certifications, including any completed electronically, are incorporated by reference into the Contract.

26.15 Gratuities

The Contract may be immediately terminated, in whole or in part, by written notice if it is determined that the Supplier, its employee, agent, or another representative violated any federal, State or local law, rule or ordinance by offering or giving a gratuity to any State employee directly involved in the Contract. In addition, Suspension or Debarment of the Supplier may result from such a violation.

26.16 Import/Export Controls

Neither party will use, distribute, transfer or transmit any equipment, services, software or technical information provided under the Contract (even if incorporated into other products) except in compliance with all applicable import and export laws, conventions and regulations.

ATTACHMENT C

OKLAHOMA STATEWIDE CONTRACT TERMS

1. Statewide Contract Type

- 1.1** The Contract is a non-mandatory statewide contract for use by State agencies. Additionally, the Contract may be used by any governmental entity specified as a political subdivision of the State pursuant to the Governmental Tort Claims Act including any associated institution, instrumentality, board, commission, committee, department or other entity designated to act on behalf of the political subdivision; a state, county or local governmental entity in its state of origin; and entities authorized to utilize contracts by the State via a multistate or multigovernmental contract.
- 1.2** The Contract is a firm, fixed price contract for indefinite delivery and quantity for the Acquisitions available under the Contract.

2. Orders and Addendums

- 2.1** Unless mutually agreed in writing otherwise, orders shall be placed directly with the Supplier by issuance of written purchase orders or by Purchase Card by state agencies and other authorized entities. All orders are subject to the Contract terms and any order dated prior to Contract expiration shall be performed. Delivery to multiple destinations may be required.
- 2.2** Any ordering document shall be effective between Supplier and the Customer only and shall not be an Addendum to the Contract in its entirety or apply to any Acquisition by another Customer.
- 2.3** Additional terms added to a Contract Document by a Customer shall be effective if the additional terms do not conflict with the General Terms and are acceptable to Supplier. However, an Addendum to the Contract shall be signed by the State Purchasing Director or designee. Regarding information technology and telecommunications contracts, pursuant to 62 O.S., §34.11.1, the Chief Information Officer acts as the Information Technology and Telecommunications Purchasing Director.

3. Termination for Funding Insufficiency

In addition to Contract terms relating to termination due to insufficient funding, a Customer may terminate any purchase order or other payment mechanism if funds sufficient to pay obligations under the Contract are not appropriated or received from an intended third-party funding source. The determination by the Customer of insufficient funding shall be accepted by, and shall be final and binding on, the Supplier.

4. Termination for Cause

In addition to Contract terms relating to termination for cause, a customer may terminate its obligations, in whole or in part, to Supplier if it has provided Supplier with written notice of material breach and Supplier fails to cure such material breach within thirty (30) days of receipt of written notice. The Customer may also terminate a purchase order or other payment mechanism or Supplier's activities under the Contract immediately without a thirty (30) day written notice to Supplier, if Supplier fails to comply with confidentiality, privacy, security, environmental or safety requirements if such non-compliance relates or may relate to Supplier provision of products or services to the Customer or if Supplier's material breach is reasonably determined (i) to be an impediment to the function of the Customer and detrimental to the Customer, or (ii) when conditions preclude the thirty (30) day notice.

5. Termination for Convenience

In addition to any termination for convenience provisions in the Contract, a Customer may terminate a purchase order or other payment mechanism for convenience if it is determined that termination is in the Customer's best interest. Supplier will be provided at least thirty (30) days' written notice of termination.

6. Contract Management Fee and Usage Report

6.1 Pursuant to 74 O.S. § 85.33A, the State assesses a contract management fee on all transactions under a statewide contract. The payment of such fee will be calculated for all transactions, net of returns and the Supplier has no right of setoff against such fee regardless of the payment status of any Customer or any aggregate accounts receivable percentage. Supplier acknowledges and agrees that all prices quoted under any statewide contract shall include the contract management fee and the contract management fee shall not be reflected as a separate line item in Supplier's billing. The State reserves the

right to change this fee upward or downward upon sixty (60) calendar days' written notice to Supplier without further requirement for an Addendum.

6.2 While Supplier is the awardee of a statewide contract, transactions that occur under the terms of the statewide contract are subject to a one percent (1%) contract management fee to be paid by Supplier. Supplier shall submit a Contract Usage Report on a quarterly basis for each contract using a form provided by the State and such report shall include applicable information for each transaction. Reports shall include usage of the statewide contract by every Customer during the applicable quarter. A singular report provided late will not be considered a breach of the statewide contract; provided, however, repeated failure to submit accurate quarterly usage reports and submit timely payments may result in suspension or termination, in whole or in part, of the Contract.

6.3 All Contract Usage Reports shall meet the following criteria:

- i. Electronic submission in Microsoft Excel format to strategic.sourcing@omes.ok.gov;
- ii. Quarterly submission regardless of whether there were transactions under the Contract during the applicable quarterly reporting period;
- iii. Submission no later than forty-five (45) days following the end of each calendar quarter;
- iv. Contract quarterly reporting periods shall be as follows:
 - a. January 01 through March 31;
 - b. April 01 through June 30;
 - c. July 01 through September 30; and
 - d. October 01 through December 31.
- v. Reports must include the following information:
 - a. Procuring entity;
 - b. Order date;

- c. Purchase Order number or note that the transaction was paid by Purchase Card;
- d. City in which products or services were received or specific office or subdivision title;
- e. Product manufacturer or type of service;
- f. Manufacturer item number, if applicable;
- g. Product description;
- h. General product category, if applicable;
- i. Quantity;
- j. Unit list price or MSRP, as applicable;
- k. Unit price charged to the purchasing entity; and
- l. Other Contract usage information requested by the State.

6.4 Payment of the contract management fee shall be delivered to the following address within forty-five (45) calendar days after the end of each quarterly reporting period:

State of Oklahoma
Office of Management and Enterprise Services, Central Purchasing
2401 North Lincoln Boulevard, Suite 116
Oklahoma City, Oklahoma 73105

To ensure payment is properly accounted for, Supplier shall provide the following information with payment: (i) reference to the applicable Contract Usage Report and quarterly reporting period and (ii) the applicable statewide contract number(s) and the amount of the contract management fee being paid for each contract number.

ATTACHMENT D

STATE OF OKLAHOMA INFORMATION TECHNOLOGY TERMS

The parties further agree to the following terms (“Information Technology Terms”), as applicable, for any Acquisition of products or services with an information technology or telecommunication component. Pursuant to the Oklahoma Information Technology Consolidation and Coordination Act, OMES-Information Services (“OMES-IS”) is designated to purchase information technology and telecommunication products and services on behalf of the State. The Act directs OMES-IS to acquire necessary hardware, software and services and to authorize the use by other State agencies. OMES, as the owner of information technology and telecommunication assets and contracts on behalf of the State, allows other State agencies to use the assets while retaining ownership and the right to reassign the assets, at no additional cost, upon written notification to Supplier. OMES-IS is the data custodian for State agency data; however, such data is owned by the respective State agency.

1 Definitions

- 1.1 **COTS** means software that is commercial off the shelf.
- 1.2 **Customer Data** means all data supplied by or on behalf of a Customer in connection with the Contract, excluding any confidential information of Supplier.
- 1.3 **Data Breach** means the unauthorized access by an unauthorized person that results in the use, disclosure or theft of Customer Data.
- 1.4 **Host** includes the terms **Hosted** or **Hosting** and means the accessing, processing or storing of Customer Data.
- 1.5 **Intellectual Property Rights** means the worldwide legal rights or interests evidenced by or embodied in any idea, design, concept, personality right, method, process, technique, apparatus, invention, discovery or improvement including any patents, trade secrets and know-how; any work of authorship including any copyrights, Moral Rights or neighboring rights; any trademark, service mark, trade dress, trade name or other indicia of source or origin; domain name registrations; and any other proprietary or similar rights. Intellectual Property Rights of a party also includes all worldwide legal rights or interests that the party may have acquired by assignment or license with the right to grant sublicenses.
- 1.6 **Moral Rights** means any and all rights of paternity or integrity of the Work Product and the right to object to any modification, translation or use of the Work Product and any similar rights existing under the judicial or statutory law of any country in the world or under any treaty, regardless of whether or not such right is denominated or referred to as a moral right.
- 1.7 **Non-Public Data** means Customer Data, other than Personal Data, that is not subject to distribution to the public as public information. It is deemed to be sensitive and confidential

by Customer because it contains information that is exempt by statute, ordinance or administrative rule from access by the general public as public information. Non-Public Data includes any data deemed confidential pursuant to the Contract, otherwise identified by Customer as Non-Public Data, or that a reasonable person would deem confidential.

- 1.8 Personal Data** means Customer Data that contains 1) any combination of an individual's name, social security numbers, driver's license, state/federal identification number, account number, credit or debit card number and/or 2) data subject to protection under a federal, state or local law, rule, regulation or ordinance.
- 1.9 Security Incident** means the attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with the Hosted environment used to perform the services.
- 1.10 State CIO** means the State Chief Information Officer or authorized designee.
- 1.11 Supplier Intellectual Property** means all tangible or intangible items or things, including the Intellectual Property Rights therein, created or developed by Supplier and identified in writing as such (a) prior to providing any services or Work Product to Customer and prior to receiving any documents, materials, information or funding from or on behalf of a Customer relating to the services or Work Product, or (b) after the effective date of the Contract if such tangible or intangible items or things were independently developed by Supplier outside Supplier's provision of services or Work Product for Customer under the Contract and were not created, prepared, developed, invented or conceived by any Customer personnel who then became personnel to Supplier or any of its affiliates or subcontractors, where, although creation or reduction-to-practice is completed while the person is affiliated with Supplier or its personnel, any portion of same was created, invented or conceived by such person while affiliated with Customer.
- 1.12 Third Party Intellectual Property** means the Intellectual Property Rights of any third party that is not a party to the Contract, and that is not directly or indirectly providing any goods or services to a Customer under the Contract.
- 1.13 Work Product** means any and all deliverables produced by Supplier for Customer under a statement of work issued pursuant to the Contract, including any and all tangible or intangible items or things that have been or will be prepared, created, developed, invented or conceived at any time following the effective date of the Contract, including but not limited to any (i) works of authorship (such as manuals, instructions, printed material, graphics, artwork, images, illustrations, photographs, computer programs, computer software, scripts, object code, source code or other programming code, HTML code, flow charts, notes, outlines, lists, compilations, manuscripts, writings, pictorial materials, schematics, formulae, processes, algorithms, data, information, multimedia files, text web pages or web sites, other written or machine readable expression of such works fixed in any tangible media, and all other copyrightable works), (i) trademarks, service marks, trade dress, trade names, logos, or other indicia of source or origin, (iii) ideas, designs, concepts,

personality rights, methods, processes, techniques, apparatuses, inventions, formulas, discoveries, or improvements, including any patents, trade secrets and know-how, (iv) domain names, (v) any copies, and similar or derivative works to any of the foregoing, (vi) all documentation and materials related to any of the foregoing, (vii) all other goods, services or deliverables to be provided to Customer under the Contract or statement of work, and (viii) all Intellectual Property Rights in any of the foregoing, and which are or were created, prepared, developed, invented or conceived for the use of benefit of Customer in connection with this Contract or a statement of work, or with funds appropriated by or for Customer or Customer's benefit: (a) by any Supplier personnel or Customer personnel, or (b) any Customer personnel who then became personnel to Supplier or any of its affiliates or subcontractors, where, although creation or reduction-to-practice is completed while the person is affiliated with Supplier or its personnel, any portion of same was created, invented or conceived by such person while affiliated with Customer.

2 Termination of Maintenance and Support Services

Customer may terminate maintenance or support services without an adjustment charge, provided any of the following circumstances occur:

- 2.1** Customer removes the product for which the services are provided, from productive use or;
- 2.2** The location at which the services are provided is no longer controlled by Customer (for example, because of statutory or regulatory changes or the sale or closing of a facility).

If Customer chooses to renew maintenance or support after maintenance has lapsed, Customer may choose to pay the additional fee, if any, associated with renewing a license after such maintenance or support has lapsed, or to purchase a new license. Any amount paid to Supplier in the form of prepaid fees that are unused when services under the Contract or purchase order are terminated shall be refunded to Customer.

3 Compliance and Electronic and Information Technology Accessibility

State procurement of information technology is subject to certain federal and State laws, rules and regulations related to information technology accessibility, including but not limited to Oklahoma Information Technology Accessibility Standards ("Standards") set forth at <https://omes.ok.gov/services/information-services/accessibility-standards>. Supplier shall provide a Voluntary Product Accessibility Template ("VPAT") describing accessibility compliance via a URL linking to the VPAT and shall update the VPAT as necessary in order to allow a Customer to obtain current VPAT information as required by State law. If products require development or customization, additional requirements and documentation may be required and compliance shall be necessary by Supplier. Such requirements may be stated in appropriate documents including but not limited to a statement of work, riders, agreement, purchase order or Addendum.

All representations contained in the VPAT provided will be relied upon by the State or a Customer, as applicable, for accessibility compliance purposes.

4 Media Ownership (Disk Drive and/or Memory Chip Ownership)

- 4.1** Any disk drives and memory cards purchased with or included for use in leased or purchased products under the Contract remain the property of the Customer.
- 4.2** Personal information may be retained within electronic media devices and components; therefore, electronic media shall not be released either between Customers or for the resale, of refurbished equipment that has been in use by a Customer, by the Supplier to the general public or other entities. This provision applies to replacement devices and components, whether purchased or leased, supplied by Supplier, its agents or subcontractors during the downtime (repair) of products purchased or leased through the Contract. If a device is removed from a location for repairs, the Customer shall have sole discretion, prior to removal, to determine and implement sufficient safeguards (such as a record of hard drive serial numbers) to protect personal information that may be stored within the hard drive or memory of the device.

5 Offshore Services

No offshore services are provided for under the Contract. State data shall not be used or accessed internationally for troubleshooting or any other use not specifically provided for herein without the prior written permission, which may be withheld in the State's sole discretion, from the appropriate authorized representative of the State. Notwithstanding the above, back office administrative functions of the Supplier may be located offshore and the follow-the-sun support model may be used by the Supplier to the extent allowed by law applicable to any Customer data being accessed or used.

6 Compliance with Technology Policies

- 6.1** The Supplier agrees to adhere to the State of Oklahoma "Information Security Policy, Procedures, and Guidelines" available at https://omes.ok.gov/s/g/files/gmc316/f/InfoSecPPG_0.pdf.

Supplier's employees and subcontractors shall adhere to the applicable State IT Standard Methodologies and Templates including but not limited to Project Management, Business Analysis, System Analysis, Enterprise and IT Architecture, Quality, Application and Security Methodologies and Templates as set forth at <http://eclipse.omes.ok.gov>.

- 6.2** Supplier shall comply with applicable Federal Information Processing Standards including, without limitation, FIPS 200, FIPS 140-2 or successor standards and all recommendations from the National Institute of Standards and Technology. The confidentiality of Customer Data shall be protected and maintained in accordance with these standards as well as other applicable Customer standards.

6.3 Supplier shall comply with the CJIS Security Policy as more particularly described at Appendix 2 attached hereto and incorporated herein.

7 Emerging Technologies

The State of Oklahoma reserves the right to enter into an Addendum to the Contract at any time to allow for emerging technologies not identified elsewhere in the Contract Documents if there are repeated requests for such emerging technology or the State determines it is warranted to add such technology.

8 Extension Right

In addition to extension rights of the State set forth in the Contract, the State CIO reserves the right to extend any Contract if the State CIO determines such extension to be in the best interest of the State.

9 Source Code Escrow

Pursuant to 62 O.S. § 34.31, if customized computer software is developed or modified exclusively for a State agency, the Supplier has a continuing obligation to comply with such law and place the source code for such software and any modifications thereto into escrow with an independent third party escrow agent. Supplier shall pay all fees charged by the escrow agent and enter into an escrow agreement, the terms of which are subject to the prior written approval of the State, including terms that provide the State receives ownership of all escrowed source code upon the occurrence of any of the following:

- 9.1** A bona fide material default of the obligations of the Supplier under the agreement with the applicable Customer;
- 9.2** An assignment by the Supplier for the benefit of its creditors;
- 9.3** A failure by the Supplier to pay, or an admission by the Supplier of its inability to pay, its debts as they mature;
- 9.4** The filing of a petition in bankruptcy by or against the Supplier when such petition is not dismissed within sixty (60) days of the filing date;
- 9.5** The appointment of a receiver, liquidator or trustee appointed for any substantial part of the Supplier's property;
- 9.6** The inability or unwillingness of the Supplier to provide the maintenance and support services in accordance with the agreement with the agency;
- 9.7** Supplier's ceasing of maintenance and support of the software; or
- 9.8** Such other condition as may be statutorily imposed by the future amendment or enactment of applicable Oklahoma law.

10 Commercial Off The Shelf Software

If Supplier specifies terms and conditions or clauses in an electronic license, subscription, maintenance, support or similar agreement that conflict with the terms of this Contract, the additional terms and conditions or conflicting clauses shall not be binding on the State and the provisions of this Contract shall prevail.

11 Ownership Rights

Any software developed by the Supplier under the terms of the Contract is for the sole and exclusive use of the State including but not limited to the right to use, reproduce, re-use, alter, modify, edit, or change the software as it sees fit and for any purpose. Moreover, except with regard to any deliverable based on Supplier Intellectual Property, the State shall be deemed the sole and exclusive owner of all right, title, and interest therein, including but not limited to all source data, information and materials furnished to the State, together with all plans, system analysis, and design specifications and drawings, completed programs and documentation thereof, reports and listing, all data and test procedures and all other items pertaining to the work and services to be performed pursuant to this Contract including all copyright and proprietary rights relating thereto. With respect to Supplier Intellectual Property, the Supplier grants the State, for no additional consideration, a perpetual, irrevocable, royalty-free license, solely for the internal business use of the State, to use, copy, modify, display, perform, transmit and prepare derivative works of Supplier Intellectual Property embodied in or delivered to the State in conjunction with the products.

Except for any Supplier Intellectual Property, all work performed by the Supplier of developing, modifying or customizing software and any related supporting documentation shall be considered as Work for Hire (as defined under the U.S. copyright laws) and, as such, shall be owned by and for the benefit of State.

In the event that it should be determined that any portion of such software or related supporting documentation does not qualify as “Work for Hire”, Supplier hereby irrevocably grants to the State, for no additional consideration, a non-exclusive, irrevocable, royalty-free license to use, copy, modify, display, perform, transmit and prepare derivative works of any such software and any Supplier Intellectual Property embodied in or delivered to the State in conjunction with the products.

Supplier shall assist the State and its agents, upon request, in preparing U.S. and foreign copyright, trademark, and/or patent applications covering software developed, modified or customized for the State. Supplier shall sign any such applications, upon request, and deliver them to the State. The State shall bear all expenses that incurred in connection with such copyright, trademark, and/or patent applications.

If any Acquisition pursuant to this Contract is funded wholly or in part with federal funds, the source code and all associated software and related documentation owned by the State may be

shared with other publicly funded agencies at the discretion of the State without permission from or additional compensation to the Supplier.

12 Intellectual Property Ownership

The following terms apply to ownership and rights related to Intellectual Property:

- 12.1** As between Supplier and Customer, the Work Product and Intellectual Property Rights therein are and shall be owned exclusively by Customer, and not Supplier. Supplier specifically agrees that the Work Product shall be considered “works made for hire” and that the Work Product shall, upon creation, be owned exclusively by Customer. To the extent that the Work Product, under applicable law, may not be considered works made for hire, Supplier hereby agrees that all right, title and interest in and to all ownership rights and all Intellectual Property Rights in the Work Product is hereby effectively transferred, granted, conveyed, assigned and relinquished exclusively to Customer, without the necessity of any further consideration, and Customer shall be entitled to obtain and hold in its own name all Intellectual Property Rights in and to the Work Product. Supplier acknowledges that Supplier and Customer do not intend Supplier to be a joint author of the Work Product within the meaning of the Copyright Act of 1976. Customer shall have access, during normal business hours (Monday through Friday, 8:00 a.m. to 5:00 p.m.) and upon reasonable prior notice to Supplier, to all Supplier materials, premises and computer files containing the Work Product. Supplier and Customer, as appropriate, will cooperate with one another and execute such other documents as may be reasonably appropriate to achieve the objectives herein. No license or other right is granted under the Contract to any Third Party Intellectual Property, except as may be incorporated in the Work Product by Supplier.
- 12.2** Supplier, upon request and without further consideration, shall perform any acts that may be deemed reasonably necessary or desirable by Customer to evidence more fully the transfer of ownership and/or registration of all Intellectual Property Rights in all Work Product to Customer to the fullest extent possible including, but not limited to, the execution, acknowledgement and delivery of such further documents in a form determined by Customer. In the event Customer shall be unable to obtain Supplier’s signature due to the dissolution of Supplier or Supplier’s failure to respond to Customer’s repeated requests for such signature on any document reasonably necessary for any purpose set forth in the foregoing sentence, Supplier hereby irrevocably designates and appoints Customer and its duly authorized officers and agents as Supplier’s agent and Supplier’s attorney-in-fact to act for and in Supplier’s behalf and stead to execute and file any such document and to do all other lawfully permitted acts to further any such purpose with the same force and effect as if executed and delivered by Supplier, provided however that no such grant of right to Customer is applicable if Supplier fails to execute any document due to a good faith dispute by Supplier with respect to such document. It is understood that such power is coupled with an interest and is therefore irrevocable. Customer shall have the full and sole power to prosecute such applications and to take all other action concerning the Work Product, and Supplier shall cooperate, at Customer’s sole expense, in the preparation and

prosecution of all such applications and in any legal actions and proceedings concerning the Work Product.

- 12.3** Supplier hereby irrevocably and forever waives, and agrees never to assert, any Moral Rights in or to the Work Product which Supplier may now have or which may accrue to Supplier's benefit under U.S. or foreign copyright or other laws and any and all other residual rights and benefits which arise under any other applicable law now in force or hereafter enacted. Supplier acknowledges the receipt of equitable compensation for its assignment and waiver of such Moral Rights.
- 12.4** All documents, information and materials forwarded to Supplier by Customer for use in and preparation of the Work Product shall be deemed the confidential information of Customer, subject to the license granted by Customer to Supplier hereunder. Supplier shall not otherwise use, disclose, or permit any third party to use or obtain the Work Product, or any portion thereof, in any manner without the prior written approval of Customer.
- 12.5** These provisions are intended to protect Customer's proprietary rights pertaining to the Work Product and the Intellectual Property Rights therein and any misuse of such rights would cause substantial and irreparable harm to Customer's business. Therefore, Supplier acknowledges and stipulates that a court of competent jurisdiction may immediately enjoin a material breach of the Supplier's obligations with respect to confidentiality provisions of the Contract and the Work Product and a Customer's Intellectual Property Rights, upon a request by Customer, without requiring proof of irreparable injury, as same is presumed.
- 12.6** Upon the request of Customer, but in any event upon termination or expiration of this Contract or a statement of work, Supplier shall surrender to Customer all documents and things pertaining to the Work Product, generated or developed by Supplier or furnished by Customer to Supplier, including all materials embodying the Work Product, any Customer confidential information and Intellectual Property Rights in such Work Product, regardless of whether complete or incomplete. This section is intended to apply to all Work Product as well as to all documents and things furnished to Supplier by Customer or by anyone else that pertains to the Work Product.
- 12.7** Customer hereby grants to Supplier a non-transferable, non-exclusive, royalty-free, fully paid license to use any Work Product solely as necessary to provide services to Customer. Except as provided in this section, neither Supplier nor any subcontractor shall have the right to use the Work Product in connection with the provision of services to its other customers without the prior written consent of Customer, which consent may be withheld in Customer's sole discretion.
- 12.8** To the extent that any Third Party Intellectual Property is embodied or reflected in the Work Product or is necessary to provide services, Supplier shall obtain from the applicable third party for the Customer's benefit, an irrevocable, perpetual, non-exclusive, worldwide, royalty-free license, solely for Customer's internal business purposes; likewise, with respect to any Supplier Intellectual Property embodied or reflected in the Work Product or

necessary to provide services, Supplier grants to Customer an irrevocable, perpetual, non-exclusive, worldwide, royalty-free license, solely for the Customer's internal business purposes. Each such license shall allow the applicable Customer to (i) use, copy, modify, display, perform (by any means), transmit and prepare derivative works of any Third Party Intellectual Property or Supplier Intellectual Property embodied in or delivered to Customer in conjunction with the Work Product and (ii) authorize others to do any or all of the foregoing. Supplier agrees to notify Customer on delivery of the Work Product or services if such materials include any Third Party Intellectual Property. The foregoing license includes the right to sublicense third parties, solely for the purpose of engaging such third parties to assist or carry out Customer's internal business use of the Work Product. Except for the preceding license, all rights in Supplier Intellectual Property remain in Supplier. On request, Supplier shall provide Customer with documentation indicating a third party's written approval for Supplier to use any Third Party Intellectual Property that may be embodied or reflected in the Work Product.

- 12.9** Supplier agrees that it shall have written agreement(s) that are consistent with the provisions hereof related to Work Product and Intellectual Property Rights with any employees, agents, consultants, contractors or subcontractors providing services or Work Product pursuant to the Contract, prior to the provision of such services or Work Product and that it shall maintain such written agreements at all times during performance of this Contract which are sufficient to support all performance and grants of rights by Supplier. Copies of such agreements shall be provided to the Customer promptly upon request.
- 12.10** To the extent not inconsistent with Customer's rights in the Work Product or other provisions, nothing in this Contract shall preclude Supplier from developing for itself, or for others, materials which are competitive with those produced as a result of the services provided under the Contract, provided that no Work Product is utilized, and no Intellectual Property Rights of Customer therein are infringed by such competitive materials. To the extent that Supplier wishes to use the Work Product or acquire licensed rights in certain Intellectual Property Rights of Customer therein in order to offer competitive goods or services to third parties, Supplier and Customer agree to negotiate in good faith regarding an appropriate license and royalty agreement to allow for such.
- 12.11** If any Acquisition pursuant to the Contract is funded wholly or in part with federal funds, the source code and all associated software and related documentation and materials owned by a Customer may be shared with other publicly funded agencies at the discretion of such Customer without permission from or additional compensation to the Supplier.

13 Hosting Services

- 13.1** If Supplier or its subcontractor, affiliate or any other person or entity providing products or services under the Contract Hosts Customer Data in connection with an Acquisition, the provisions of Appendix 1, attached hereto and incorporated herein, apply to such Acquisition.

13.2 If the Hosting of Customer Data by Supplier or its subcontractor, affiliate or any other person or entity providing products or services under the Contract contributes to or directly causes a Data Breach, Supplier shall be responsible for the obligations set forth in Appendix 1 related to breach reporting requirements and associated costs. Likewise if such Hosting contributes to or directly causes a Security Incident, Supplier shall be responsible for the obligations set forth in Appendix 1, as applicable.

14 Change Management

When a scheduled change is made to products or services provided to a Customer that impacts the Customer's system related to such product or service, Supplier shall provide two (2) weeks' prior written notice of such change. When the change is an emergency change, Supplier shall provide twenty-four (24) hours' prior written notice of the change. Repeated failure to provide such notice may be an evaluation factor (as indicative of Supplier's past performance) upon renewal or if future bids submitted by Supplier are evaluated by the State.

15 Service Level Deficiency

In addition to other terms of the Contract, in instances of the Supplier's repeated failure to provide an acceptable level of service or meet service level agreement metrics, service credits shall be provided by Supplier and may be used as an offset to payment due.

16 Notices

In addition to notice requirements under the terms of the Contract otherwise, the following individuals shall also be provided the request, approval or notice, as applicable:

Chief Information Officer
3115 N. Lincoln Blvd
Oklahoma City, OK 73105

With a copy, which shall not constitute notice, to:

Information Services Deputy Counsel
3115 North Lincoln Boulevard
Oklahoma City, Oklahoma 73105

Appendix 1 to State of Oklahoma Information Technology Terms

The parties agree to the following provisions in connection with any Customer Data accessed, processed or stored by or on behalf of the Supplier and the obligations, representations and warranties set forth below shall continue as long as the Supplier has an obligation under the Contract

A. Customer Data

1. Customer will be responsible for the accuracy and completeness of all Customer Data provided to Supplier by Customer. Customer shall retain exclusive ownership of all Customer Data. Non-Public Data and Personal Data shall be deemed to be Customer's confidential information. Supplier shall restrict access to Customer Data to their employees with a need to know (and advise such employees of the confidentiality and non-disclosure obligations assumed herein).
2. Supplier shall promptly notify the Customer upon receipt of any requests from unauthorized third parties which in any way might reasonably require access to Customer Data or Customer's use of the Hosted environment. Supplier shall notify the Customer by the fastest means available and also in writing pursuant to Contract notice provisions and the notice provision herein. Except to the extent required by law, Supplier shall not respond to subpoenas, service or process, Freedom of Information Act or other open records requests, and other legal request related to Customer without first notifying the Customer and obtaining the Customer's prior approval, which shall not be unreasonably withheld, of Supplier's proposed responses. Supplier agrees to provide its completed responses to the Customer with adequate time for Customer review, revision and approval.
3. Supplier will use commercially reasonable efforts to prevent the loss of or damage to Customer Data in its possession and will maintain commercially reasonable back-up procedures and copies to facilitate the reconstruction of any Customer Data that may be lost or damaged by Supplier. Supplier will promptly notify Customer of any loss, damage to, or unauthorized access of Customer Data. Supplier will use commercially reasonable efforts to reconstruct any Customer Data that has been lost or damaged by Supplier as a result of its negligence or willful misconduct. If Customer Data is lost or damaged for reasons other than as a result of Supplier's negligence or willful misconduct, Supplier, at the Customer's expense, will, at the request of the State, use commercially reasonable efforts to reconstruct any Customer Data lost or damaged.

B. Data Security

1. Supplier will use commercially reasonable efforts, consistent with industry standards, to provide security for the Hosted environment and Customer Data and to protect against both unauthorized access to the Hosting environment, and unauthorized communications between the Hosting environment and the Customer's browser. Supplier shall implement and maintain appropriate administrative, technical and organizational security measures to safeguard against unauthorized access, disclosure or theft of Personal Data and Non-Public

Data. Such security measures shall be in accordance with recognized industry practice and not less stringent than the measures the service provider applies to its own personal data and non-public data of similar kind.

2. All Personal Data and Non-public Data shall be encrypted at rest and in transit with controlled access. Unless otherwise stipulated, the service provider is responsible for encryption of Personal Data.
3. Supplier represents and warrants to the Customer that the Hosting equipment and environment will be routinely checked with a commercially available, industry standard software application with up-to-date virus definitions. Supplier will regularly update the virus definitions to ensure that the definitions are as up-to-date as is commercially reasonable. Supplier will promptly purge all viruses discovered during virus checks. If there is a reasonable basis to believe that a virus may have been transmitted to Customer by Supplier, Supplier will promptly notify Customer of such possibility in a writing that states the nature of the virus, the date on which transmission may have occurred, and the means Supplier has used to remediate the virus. Should the virus propagate to Customer's IT infrastructure, Supplier is responsible for costs incurred by Customer for Customer to remediate the virus.
4. Supplier shall provide its services to Customer and its users solely from data centers in the U.S. Storage of Customer Data at rest shall be located solely in data centers in the U.S. Supplier shall not allow its personnel or contractors to store Customer Data on portable devices, including personal computers, except for devices that are used and kept only at its U.S. data centers. Supplier shall permit its personnel and contractors to access Customer Data remotely only as required to fulfill Supplier's obligations under the Contract.
5. Supplier shall allow the Customer to audit conformance to the Contract terms. The Customer may perform this audit or contract with a third party at its discretion and at Customer's expense.
6. Supplier shall perform an independent audit of its data centers at least annually at its expense and provide a redacted version of the audit report upon request. Supplier may remove its proprietary information from the redacted version. A Service Organization Control (SOC) 2 audit report or approved equivalent sets the minimum level of a third-party audit.
7. Any remedies provided in this Appendix are not exclusive and are in addition to other rights and remedies available under the terms of the Contract, at law or in equity.

C. Security Assessment

1. The State requires any entity or third-party Supplier Hosting Oklahoma Customer Data to submit to a State Certification and Accreditation Review process to assess initial security risk. Supplier submitted to the review and met the State's minimum security standards at time the Contract was executed. Failure to maintain the State's minimum security standards

during the term of the contract, including renewals, constitutes a material breach. Upon request, the Supplier shall provide updated data security information in connection with a potential renewal. If information provided in the security risk assessment changes, Supplier shall promptly notify the State and include in such notification the updated information; provided, however, Supplier shall make no change that results in lessened data protection or increased data security risk. Failure to provide the notice required by this section or maintain the level of security required in the Contract constitutes a material breach by Supplier and may result in a whole or partial termination of the Contract.

2. Any Hosting entity change must be approved in writing prior to such change. To the extent Supplier requests a different sub-contractor than the third-party Hosting Supplier already approved by the State, the different sub-contractor is subject to the State's approval. Supplier agrees not to migrate State's data or otherwise utilize the different third-party Hosting Supplier in connection with key business functions that are Supplier's obligations under the contract until the State approves the third-party Hosting Supplier's State Certification and Accreditation Review, which approval shall not be unreasonably withheld or delayed. In the event the third-party Hosting Supplier does not meet the State's requirements under the State Certification and Accreditation Review, Supplier acknowledges and agrees it will not utilize the third-party Supplier in connection with key business functions that are Supplier's obligations under the contract, until such third party meets such requirements.

D. Security Incident or Data Breach Notification: Supplier shall inform Customer of any Security Incident or Data Breach.

1. Supplier may need to communicate with outside parties regarding a Security Incident, which may include contacting law enforcement, fielding media inquiries and seeking external expertise as mutually agreed upon, defined by law or contained in the Contract. If a Security Incident involves Customer Data, Supplier will coordinate with Customer prior to any such communication.
2. Supplier shall report a Security Incident to the Customer identified contact set forth herein within five (5) days of discovery of the Security Incident or within a shorter notice period required by applicable law or regulation (i.e. HIPAA requires notice to be provided within 24 hours).
3. Supplier shall:
 - a. Maintain processes and procedures to identify, respond to and analyze Security Incidents;
 - b. Make summary information regarding such procedures available to Customer at Customer's request;
 - c. Mitigate, to the extent practicable, harmful effects of Security Incidents that are known to Supplier; and

d. Document all Security Incidents and their outcomes.

4. If Supplier has reasonable belief or actual knowledge of a Data Breach, Supplier shall (1) promptly notify the appropriate Customer identified contact set forth herein within 24 hours or sooner, unless shorter time is required by applicable law, and (2) take commercially reasonable measures to address the Data Breach in a timely manner.

E. **Breach Responsibilities:** This section only applies when a Data Breach occurs with respect to Personal Data or Non-Public Data within the possession or control of Supplier.

1. Supplier shall (1) cooperate with Customer as reasonably requested by Customer to investigate and resolve the Data Breach, (2) promptly implement necessary remedial measures, if necessary, and (3) document responsive actions taken related to the Data Breach, including any post-incident review of events and actions taken to make changes in business practices in providing the services, if necessary.
2. Unless otherwise stipulated, if a Data Breach is a direct result of Supplier's breach of its obligation to encrypt Personal Data and Non-Public Data or otherwise prevent its release, Supplier shall bear the costs associated with (1) the investigation and resolution of the Data Breach; (2) notifications to individuals, regulators or others required by state law; (3) credit monitoring services required by state or federal law; (4) a website or toll-free numbers and call center for affected individuals required by state law – all not to exceed the agency per record per person cost calculated for data breaches in the United States on the most recent Cost of Data breach Study: Global Analysis published by the Ponemon Institute at the time of the data breach; and (5) complete all corrective actions as reasonably determined by Supplier based on root cause.
3. If a Data Breach is a direct result of Supplier's breach of its obligations to encrypt Personal Data and Non-Public Data or otherwise prevent its release, Supplier shall indemnify and hold harmless the Customer against all penalties assessed to Indemnified Parties by governmental authorities in connection with the Data Breach.

F. **Notices**

In addition to notice requirements under the terms of the Contract and those set forth above, a request, an approval or a notice in connection with this Appendix provided by Supplier shall be provided to:

Chief Information Security Officer

3115 N. Lincoln Blvd

Oklahoma City, OK 73105

and

servicedesk@omes.ok.gov.

G. Supplier Representations and Warranties

Supplier represents and warrants the following:

1. The product and services provided in connection with Hosting services do not infringe a third party's patent or copyright or other intellectual property rights.
2. Supplier will protect Customer's Non-Public Data and Personal Data from unauthorized dissemination and use with the same degree of care that each such party uses to protect its own confidential information and, in any event, will use no less than a reasonable degree of care in protecting such confidential information.
3. The execution, delivery and performance of the Contract and any ancillary documents and the consummation of the transactions contemplated by the Contract or any ancillary documents by Supplier will not violate, conflict with, or result in a breach of any provision of, or constitute a default (or an event which, with notice or lapse of time or both, would constitute a default) under, or result in the termination of, any written contract or other instrument between Supplier and any third parties retained or utilized by Supplier to provide goods or services for the benefit of the Customer.
4. Supplier shall not knowingly upload, store, post, e-mail or otherwise transmit, distribute, publish or disseminate to or through the Hosting environment any material that contains software viruses, malware or other surreptitious code designed to interrupt, destroy or limit the functionality of any computer software or hardware or telecommunications equipment or circumvent any "copy-protected" devices, or any other harmful or disruptive program.

H. Indemnity

Supplier agrees to defend, indemnify and hold the State, its officers, directors, employees, and agents harmless from all liabilities, claims, damages, losses, costs, expenses, demands, suits and actions (including without limitation reasonable attorneys' fees and costs required to establish the right to indemnification), excluding damages that are the sole fault of Customer, arising from or in connection with Supplier's breach of its express representations and warranties in these Information Technology Terms and the Contract. If a third party claims that any portion of the products or services provided by Supplier under the terms of another Contract Document or these Information Technology Terms infringes that party's patent or copyright, Supplier shall defend, indemnify and hold harmless the State and Customer against the claim at Supplier's expense and pay all related costs, damages, and attorney's fees incurred by or assessed to, the State and/or Customer. The State and/or Customer shall promptly notify Supplier of any third party claims and to the extent authorized by the Attorney General of the State, allow Supplier to control the defense and any related settlement negotiations. If the Attorney General of the State does not authorize sole control of the defense and settlement negotiations to Supplier, Supplier shall be granted authorization to equally participate in any proceeding related to this section but Supplier shall remain responsible to indemnify Customer and the State for all associated costs, damages and fees incurred by or assessed to the State and/or Customer. Should the software become, or in Supplier's

opinion, be likely to become the subject of a claim or an injunction preventing its use as contemplated in connection with Hosting services, Supplier may, at its option (i) procure for the State the right to continue using the software or (ii) replace or modify the software with a like or similar product so that it becomes non-infringing.

I. Termination, Expiration and Suspension of Service

1. During any period of service suspension, Supplier shall not take any action to intentionally disclose, alter or erase any Customer Data.

2. In the event of a termination or expiration of the Contract, the parties further agree:

Supplier shall implement an orderly return of Customer Data in a format specified by the Customer and, as determined by the Customer:

a. return the Customer Data to Customer at no additional cost, at a time agreed to by the parties and the subsequent secure disposal of State Data;

b. transitioned to a different Supplier at a mutually agreed cost and in accordance with a mutually agreed data transition plan and the subsequent secure disposal of State Data or

c. a combination of the two immediately preceding options.

3. Supplier shall not take any action to intentionally erase any Customer Data for a period of:

a. 10 days after the effective date of termination, if the termination is in accordance with the contract period;

b. 30 days after the effective date of termination, if the termination is for convenience; or

c. 60 days after the effective date of termination, if the termination is for cause.

After such period, Supplier shall, unless legally prohibited or otherwise stipulated, delete all Customer Data in its systems or otherwise in its possession or under its control.

4. The State shall be entitled to any post termination or expiration assistance generally made available with respect to the services.

5. Disposal by Supplier of Customer Data in all of its forms, such as disk, CD/DVD, backup tape and paper, when requested by the Customer, shall be performed in a secure manner. Data shall be permanently deleted and shall not be recoverable, according to National Institute of Standards and Technology (NIST)-approved methods. Certificates of destruction shall be provided to Customer within thirty (30) calendar day of its request for disposal of data.

Appendix 2 to State of Oklahoma Information Technology Terms

INTRODUCTION

The use and maintenance of all items of software or equipment offered for purchase herein must be in compliance with the most current version of the U.S. Department of Justice, Federal Bureau of Investigation (“FBI”), Criminal Justice Information Services (CJIS) Division’s CJIS Security Policy (“CJIS Security Policy” or “Security Policy” herein).

The Entity or Affiliate acquiring the data or system is hereby ultimately responsible for compliance with the CJIS Security Policy and will be subject to an audit by the State of Oklahoma CJIS Systems Officer (“CSO”) and the FBI CJIS Division’s Audit Staff.

CJIS SECURITY POLICY REQUIREMENTS GENERALLY

The CJIS Security Policy outlines a number of administrative, procedural, and technical controls agencies must have in place to protect Criminal Justice Information (“CJI”). Our experience is that agencies will generally have many of the administrative and procedural controls in place but will need to implement additional technical safeguards in order to be in complete compliance with the mandate. A Criminal Justice Agency (“CJA”) and certain other governmental agencies procuring technology equipment and services that could be used in hosting or connecting or transmitting or receiving CJI data may need to use the check list herein to make sure that the software, equipment, location, security, and persons having the ability to access CJI will meet the CJIS requirements per the then current CJIS Security Policy. A completed Appendix H to said Security Policy will need to be signed by Vendor or a 3rd party if it has access to CJI, such as incident to the maintenance or support of the purchased hardware or software within which resides CJI. **Per Appendix “A” to said Security Policy, “access to CJI is the physical or logical (electronic) ability, right or privilege to view, modify or make use of CJI.”**

DIRECTIVE CONCERNING ACCESS TO CRIMINAL JUSTICE INFORMATION AND TO HARDWARE OR SOFTWARE WHICH INTERACTS WITH CJI and CERTIFICATION

The FBI CJIS Division provides state-of-the-art identification and information services to the local, state, tribal, federal, and international criminal justice communities for criminal justice purposes, as well as the noncriminal justice communities for noncriminal justice purposes.

This Directive primarily concerns access to CJI and access to hardware and software in the use, retention, transmission, reception, and hosting of CJI for criminal justice purposes and not for noncriminal justice purposes. In that regard, this Directive is not only applicable to such data, but also to the hardware and software interacting with such data, their location(s), and persons having the ability to access such data. The CJIS data applicable to the Security Policy is the data described as such in said Policy **plus all data transmitted over the Oklahoma Law Enforcement Telecommunications System (“OLETS”) which is operated by DPS.**

In order to have access to CJI or to the aforesaid hardware or software, the vendor must be familiar with the FBI CJIS Security Policy, including but not limited to the following portions of said Security Policy:

1. the Definitions and Acronyms in §3 & Appendices “A” & “B”;

2. the general policies in §4;
3. the Policies in §5;
4. the appropriate forms in Appendices “D”, “E”, “F” & “H”; and
5. the Supplemental Guidance in Appendices “J” & “K”.

This FBI Security Policy is located and may be downloaded at: <https://www.fbi.gov/services/cjis/cjis-security-policy-resource-center>.

By executing the Contract to which this Directive is attached, the vendor hereby CERTIFIES that the foregoing directive has and will be followed, including but not limited to full compliance with the FBI CJIS Security Policy, as amended and as applicable.

Policy Requirement Checklist		Compliance checklist –
Policy Area 1	Information Exchange Agreements	
Policy Area 2	Security Awareness Training	
Policy Area 3	Incident Response	
Policy Area 4	Auditing and Accountability	
Policy Area 5	Access Control	
Policy Area 6	Identification and Authentication	
Policy Area 7	Configuration Management	
Policy Area 8	Media Protection	
Policy Area 9	Physical Protection	
Policy Area 10	Systems and Communications Protection and Information Integrity	
Policy Area 11	Formal Audits	
Policy Area 12	Personnel Security	

Attachment D-1

Information Security Requirements

1. General Information Security Requirements

- a. No employee of Contractor or its subcontractors will be granted access to State of Oklahoma agency information systems without the prior completion and approval of applicable logon authorization and acceptable use requests.
- b. Contractor or its subcontractors will notify applicable State of Oklahoma agencies when employees who have access to agency information systems are terminated.
- c. Contractor or its subcontractors will disclose to Client any suspected breach of the security of the information system or the data contained therein in the most expedient time possible and without unreasonable delay and will cooperate with Client during the investigation of any such incident.
- d. Contractor or its subcontractors agree to adhere to the State of Oklahoma "Information Security Policy, Procedures, and Guidelines" available at: <https://oklahoma.gov/content/dam/ok/en/omes/documents/InfoSecPPG.pdf>

2. HIPAA Requirements

- a. Contractor shall agree to use and disclose Protected Health Information in its possession or control in compliance with the Standards for Privacy of Individually Identifiable Health Information (Privacy Rule) (45 C.F.R. Parts 160 and 164) under the Health Insurance Portability and Accountability Act (HIPAA) of 1996. The definitions set forth in the Privacy Rule are incorporated by reference into this Contract (45 C.F.R. §§ 160.103 and 164.501).
- b. If applicable, Contractor will sign and adhere to a Business Associate Agreement (BAA). The Business Associate Agreement provides for satisfactory assurances that Contractor will use the information only for the purposes for which it was engaged. Contractor agrees it will safeguard the information from misuse, and will comply with HIPAA as it pertains to the duties stated within the contract. Failure to comply with the requirements of this standard may result in funding being withheld from Contractor, and/or full audit and inspection of Contractor's security compliance as it pertains to this contract.
- c. Business Associate Terms Definitions:
 - i. Unless otherwise defined in this BAA, all capitalized terms used in this BAA have the meanings ascribed in the HIPAA Regulations, provided; however, that "PHI" and "ePHI" shall mean Protected Health Information and Electronic Protected Health Information, respectively, as defined in 45 C.F.R. § 160.103, limited to the information Business Associate received from or created or received on behalf of the applicable State of Oklahoma agency as a Business Associate. "Administrative Safeguards" shall have the same meaning as the term "administrative safeguards in 45 C.F.R. § 164.304, with the exception that it shall apply to the management of the conduct of Business

- Associate's workforce, not the State of Oklahoma agency workforce, in relation to the protection of that information.
- ii. Business Associate. "Business Associate" shall generally have the same meaning as the term "Business Associate" at 45 C.F.R. 160.103, and in reference to the party to this agreement, shall mean the entity whose name appears below.
 - iii. Covered Entity. "Covered Entity" shall generally have the same meaning as the term "Covered Entity" at 45 C.F.R. 160.103.
 - iv. HIPAA Rules. "HIPAA Rules" shall mean the Privacy, Security, Breach Notification, and Enforcement Rules at 45 C.F.R. Part 160 and Part 164, all as may be amended.
 - v. The following terms used in this Agreement shall have the same meaning as those terms in the HIPAA Rules: Breach, Data Aggregation, Designated Record Set, Disclosure, Health Care Operations, Individual, Minimum Necessary, Notice of Privacy Practices, Protected Health Information, required by law, Secretary, Security Incident, Sub-Contractor, Unsecured PHI, and Use.
- d. Obligations of Business Associate: Business Associate may use Electronic PHI and PHI (collectively, "PHI") solely to perform its duties and responsibilities under this Agreement and only as provided in this Agreement. Business Associate acknowledges and agrees that PHI is confidential and shall not be used or disclosed, in whole or in part, except as provided in this Agreement or as required by law. Specifically, Business Associate agrees it will, as applicable:
- i. use or further disclose PHI only as permitted in this Agreement or as Required by Law, including, but not limited to the Privacy and Security Rule;
 - ii. use appropriate safeguards, and comply with Subpart C of 45 C.F.R. Part 164 with respect to Electronic PHI, to prevent use or disclosure of PHI other than as provided for by this Agreement;
 - iii. implement and document appropriate administrative, physical, and technical safeguards to protect the confidentiality, integrity, and availability of PHI that it creates, receives, maintains, or transmits for or on behalf of Covered Entity in accordance with 45 C.F.R. 164;
 - iv. implement and document administrative safeguards to prevent, detect, contain, and correct security violations in accordance with 45 C.F.R. 164;
 - v. make its applicable policies and procedures required by the Security Rule available to Covered Entity solely for purposes of verifying BA's compliance and the Secretary of the Department of Health and Human Services (HHS);
 - vi. not receive remuneration from a third party in exchange for disclosing PHI received from or on behalf of Covered Entity;
 - vii. in accordance with 45 C.F.R. 164.502(e)(1) and 164.308(b), if applicable, require that any Sub-Contractors that create, receive, maintain or transmit PHI on behalf of the Business Associate agree to the same restrictions, conditions, and requirements that apply to the Business Associate with respect to such information; this shall be in the

form of a written HIPAA Business Associate Contract and a fully executed copy will be provided to the Contract Monitor;

- viii. report to Covered Entity in writing any use or disclosure of PHI that is not permitted under this Agreement as soon as reasonably practicable but in no event later than five calendar days from becoming aware of it and mitigate, to the extent practicable and in cooperation with Covered Entity, any harmful effects known to it of a use or disclosure made in violation of this Agreement;
- ix. promptly report to Covered Entity in writing and without unreasonable delay and in no case later than five calendar days any successful Security Incident, as defined in the Security Rule, with respect to Electronic PHI;
- x. with the exception of law enforcement delays that satisfy the requirements of 45 C.F.R. 164.412, notify Covered Entity promptly, in writing and without unreasonable delay and in no case later than five calendar days, upon the discovery of a breach of Unsecured PHI. Such notice shall include, to the extent possible, the name of each individual who's Unsecured PHI has been, or is reasonably believed by Business Associate to have been, accessed, acquired, or disclosed during such Breach. Business Associate shall also, to the extent possible, furnish Covered Entity with any other available information that Covered Entity is required to include in its notification to Individuals under 45 C.F.R. § 164.404(c) at the time of Business Associate's notification to Covered Entity or promptly thereafter as such information becomes available. As used in this Section, "breach" shall have the meaning given such term at 45 C.F.R. 164.402;
- xi. to the extent allowed by law, indemnify and hold Covered Entity harmless from all claims, liabilities costs, and damages arising out of or in any manner related to the unauthorized disclosure by Business Associate of any PHI resulting from the negligent acts or omissions of Business Associate or to the breach by Business Associate of any applicable obligation related to PHI;
- xii. provide access to PHI it maintains in a Designated Record Set to Covered Entity, or if directed by Covered Entity to an Individual in order to meet the requirements of 45 C.F.R. 164.524. In the event that any Individual requests access to PHI directly from Business Associate, Business Associate shall forward such request to Covered Entity within five working days of receiving a request. This shall be in the form of a written HIPAA Business Associate Contract and a fully executed copy will be provided to the Contract Monitor. Any denials of access to the PHI requested shall be the responsibility of Covered Entity;
- xiii. make PHI it maintains in a Designated Record Set available to Covered Entity for amendment and incorporate any amendments to PHI in accordance with 45 C.F.R. 164.526;
- xiv. document disclosure of PHI it maintains in a Designated Record Set and information related to such disclosure as would be required for Covered Entity to

- respond to a request by an Individual for an accounting of disclosures of PHI, in accordance with 45 C.F.R. 164.528, and within five working days of receiving a request from Covered Entity, make such disclosure documentation and information available to Covered Entity. In the event the request for an accounting is delivered directly to Business Associate, Business Associate shall forward within five working days of receiving a request such request to Covered Entity;
- xv. make its internal practices, books, and records related to the use and disclosure of PHI received from or created or received by Business Associate on behalf of Covered Entity available to the Secretary of the Department of HHS, authorized governmental officials, and Covered entity for the purpose of determining Business Associate's compliance with the Privacy Rule. Business Associate shall give Covered Entity advance written notice of requests from HHS or government officials and provide Covered Entity with a copy of all documents made available; and
 - xvi. require that all of its Sub-Contractors, vendors, and agents to whom it provides PHI or who create, receive, use, disclose, maintain, or have access to Covered Entity's PHI shall agree in writing to requirements, restrictions, and conditions at least as stringent as those that apply to Business Associate under this Agreement, including but not limited to implementing reasonable and appropriate safeguards to protect PHI, and shall require that its Sub-Contractors, vendors, and agents agree to indemnify and hold harmless Covered Entity for their failure to comply with each of the provisions of this Agreement.
- e. Permitted Uses and Disclosures of PHI by Business Associate: Except as otherwise provided in this Agreement, Business Associate may use or disclose PHI on behalf of or to provide services to Covered Entity for the purposes specified in this Agreement, if such use or disclosure of PHI would not violate the Privacy Rule if done by Covered Entity. Unless otherwise limited herein, Business Associate may:
- i. use PHI for its proper management and administration or to fulfill any present or future legal responsibilities of Business Associate;
 - ii. disclose PHI for its proper management and administration or to fulfill any present or future legal responsibilities of Business Associate, provided that; (i) the disclosures required by law; or (ii) Business Associate obtains reasonable assurances from any person to whom the PHI is disclosed that such PHI will be kept confidential and will be used or further disclosed only as Required by Law or for the purpose(s) for which it was disclosed to the person, and the person commits to notifying Business Associate of any instances of which it is aware in which the confidentiality of the PHI has been breached;
 - iii. disclose PHI to report violations of law to appropriate federal and state authorities; or
 - iv. aggregate the PHI with other data in its possession for purposes of Covered Entity's Health Care Operations;

- v. make uses and disclosures and requests for protected health information consistent with Covered Entity's minimum necessary policies and procedures;
 - vi. de-identify any and all PHI obtained by Business Associate under this BAA, and use such de-identified data, all in accordance with the de-identification requirements of the Privacy Rule [45 C.F.R. § (d)(1)].
- f. Obligations of Covered Entity
- i. Covered Entity shall notify Business Associate of any changes in, or revocation of, the permission by an individual to use or disclose his or her PHI, to the extent that such changes may affect Business Associate's use or disclosure of PHI.
 - ii. Covered Entity shall notify Business Associate of any restriction on the use or disclosure of PHI that Covered Entity has agreed to or is required to abide by under 45 C.F.R. 164.522, to the extent that such restriction may affect Business Associate's use or disclosure of protected health information.
 - iii. Covered Entity shall not request Business Associate use or disclose PHI in any manner that would violate the Privacy Rule if done by Covered Entity.
 - iv. Covered Entity agrees to timely notify Business Associate, in writing, of any arrangements between Covered Entity and the Individual that is the subject of PHI that may impact in any manner the use and/or disclosure of the PHI by Business Associate under this BAA.
 - v. Covered Entity shall provide the minimum necessary PHI to Business Associate.
- g. Term and Termination:
- i. Obligations of Business Associate upon Termination. Upon termination of this Agreement for any reason, Business Associate, with respect to PHI received from Covered Entity, or created, maintained, or received by Business Associate on behalf of Covered Entity, shall as applicable:
 - (1) retain only that PHI that is necessary for Business Associate to continue its proper management and administration or to carry out its legal responsibilities;
 - (2) return to Covered Entity (or, if agreed to by Covered Entity, destroy) the remaining PHI that the Business Associate still maintains in any form;
 - (3) continue to use appropriate safeguards and comply with Subpart C of 45 C.F.R. Part 164 with respect to PHI to prevent use or disclosure of the PHI, other than as provided for in this Section, for as long as Business Associate retains the PHI;
 - (4) not use or disclose the PHI retained by Business Associate other than for the purposes for which such PHI was retained and subject to the same conditions set out at above under "Permitted Uses and Disclosures By Business Associate" that applied prior to termination; and
 - (5) return to Covered Entity (or, if agreed to by Covered Entity, destroy) the PHI retained by Business Associate when it is no longer needed by Business Associate for its proper management and administration or to carry out its legal responsibilities.

- ii. All other applicable obligations of Business Associate under this Agreement shall survive termination.
- iii. Should the applicable State of Oklahoma agency become aware of a pattern of activity or practice that constitutes a material breach of a material term of this BAA by Business Associate, the agency shall provide Business Associate with written notice of such a breach in sufficient detail to enable Contractor to understand the specific nature of the breach. The Client shall be entitled to terminate the Underlying Contract associated with such breach if, after the applicable State of Oklahoma agency provides the notice to Business Associate, Business Associate fails to cure the breach within a reasonable time period not less than thirty (30) days specified in such notice; provided, however, that such time period specified shall be based on the nature of the breach involved per 45 C.F.R. §§ 164.504(e)(1)(ii)(A),(B) & 164.314 (a)(2)(i)(D).

h. Miscellaneous Provisions:

- i. No Third Party Beneficiaries: Nothing in this Agreement shall confer upon any person other than the parties and their respective successors or assigns, any rights, remedies, obligations, or liabilities whatsoever.
- ii. Business Associate recognizes that any material breach of this Business Associate Terms section or breach of confidentiality or misuse of PHI may result in the termination of this Agreement and/or legal action. Said termination may be immediate and need not comply with any termination provision in the parties' underlying agreement, if any.
- iii. The parties agree to amend this Agreement from time to time as is necessary for Covered Entity or Business Associate to comply with the requirements of the Privacy Rule and related laws and regulations.
- iv. The applicable State of Oklahoma agency shall make available its Notice of Privacy Practices.
- v. Any ambiguity in this Agreement shall be resolved in a manner that causes this Agreement to comply with HIPAA.
- vi. If Business Associate maintains a designated record set in an electronic format on behalf of Covered Entity, then Business Associate agrees that within 30 calendar days of expiration or termination of the parties' agreement, Business Associate shall provide to Covered Entity a complete report of all disclosures of and access to the designated record set covering the three years immediately preceding the termination or expiration. The report shall include patient name, date and time of disclosures/access, description of what was disclosed/accessed, purpose of disclosure/access, name of individual who received or accessed the information, and, if available, what action was taken within the designated record set.
- vii. Amendment: To the extent that any relevant provision of the HIPAA Regulations is materially amended in a manner that changes the obligations of Business Associates or Covered Entities, the Parties agree to negotiate in good faith appropriate amendment(s)

to this Agreement to give effect to these revised obligations. The parties agree to amend this Agreement from time to time as is necessary for Covered Entity or to comply with the requirements of the Privacy Rule and related laws and regulations.

3. 42 C.F.R. Part 2 Related Provisions

- a. Confidentiality of Information. Contractor's employees and agents shall have access to private data to the extent necessary to carry out the responsibilities, limited by the terms of this Agreement. Contractor accepts the responsibilities for providing adequate administrative supervision and training to their employees and agents to ensure compliance with relevant confidentiality, privacy laws, regulations and contractual provisions. No private or confidential data collected, maintained, or used shall be disseminated except as authorized by statute and by terms of this Agreement, whether during the period of the Agreement or thereafter. Furthermore, Contractor:
 - i. Acknowledges that in receiving, transmitting, transporting, storing, processing, or otherwise dealing with any information received pursuant to this agreement that identifies or otherwise relates to the individuals under the care of or in the custody of a State of Oklahoma agency, it is fully bound by the provisions of the federal regulations governing the confidentiality of Alcohol and Drug Abuse Patient Records, 42 C.F.R. Part 2 and the HIPAA, 45 C.F.R. 45 Parts 142, 160, and 164, Title 43 A § 1-109 of Oklahoma Statutes, and may not use or disclose the information except as permitted or required by this Agreement or by law;
 - ii. Acknowledges that pursuant to 43A O.S. §1-109, all mental health and drug or alcohol treatment information and all communications between physician or psychotherapist and patient are both privileged and confidential and that such information is available only to persons actively engaged in treatment of the client or consumer or in related administrative work. Contractor agrees that such protected information shall not be available or accessible to staff in general and shall not be used for punishment or prosecution of an kind;
 - iii. Agrees to resist any efforts in judicial proceedings to obtain access to the protected information except as expressly provided for in the regulations governing the Confidentiality of Alcohol and Drug Abuse Patient Records, 42 C.F.R. Part 2;
 - iv. Agrees to, when applicable and to the extent within Contractor's control, use appropriate administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of the electronic protected health information that it creates, receives, maintains, or transmits on behalf of the State of Oklahoma agency and to use appropriate safeguards to prevent the unauthorized use or disclosure of the protected health information, and agrees that protected information will not be placed in the Child Protective Services (CPS) record of any individual involved with the Oklahoma Department of Human Services (DHS).

- v. Agrees to report to the State of Oklahoma agency any use or disclosure or any security incident involving protected information not provided for by this Agreement. Such a report shall be made immediately when an employee becomes aware of such a disclosure, use, or security incident.
- vi. Agrees to provide access to the protected information at the request of the State of Oklahoma agency or to an authorized individual as directed by the State of Oklahoma agency, in order to meet the requirement of 45 C.F.R. §164.524 which provides clients with the right to access and copy their own protected information;
- vii. Agrees to make any amendments to the protected information as directed or agreed to by the State of Oklahoma agency, pursuant to 45 C.F.R. §164.526;
- viii. Agrees to make available its internal practices, books, and records, including policies and procedures, relating to the use and disclosure of protected information received from the State of Oklahoma agency or created or received by the Contractor on behalf of the State of Oklahoma agency, to the State of Oklahoma agency and to the Secretary of the Department of Health and Human Services for purpose of the Secretary determining the giving party's compliance with HIPAA;
- ix. Agrees to provide the State of Oklahoma agency, or an authorized individual, information to permit the State of Oklahoma agency to respond to a request by an individual for an accounting of disclosures in accordance with 45 C.F.R. §164.528.
- b. Data Security. The Contractor agrees to, when applicable and to the extent within Contractor's control, maintain the data in a secure manner compatible with the content and use. The Contractor will, when applicable to the extent within Contractor's control, control access to the data in Contractor's possession or control compliance with the terms of this Agreement. Only the Contractor's personnel whose duties require the use of such information, will have regular access to the data. The Contractor's employees will be allowed access to the data only for the purpose set forth in this Agreement.
- c. Data Destruction. Contractor agrees to, when applicable and to the extent within Contractor's control, follow State of Oklahoma agency policies regarding secure data destruction.
- d. Use of Information. Contractor agrees that the information received or accessed through this Agreement shall not be used to the detriment of any individual nor for any purpose other than those stated in this Agreement.
- e. Redisclosure of Data. The Contractor agrees not to redisclose any information to a third party not covered by the Agreement unless written permission by the State of Oklahoma agency is received and redisclosure is permitted under applicable law.

4. Federal Tax Information Requirements IRS Publication 1075 (If Applicable)

- a. **PERFORMANCE:** If Contractor takes possession or control of Federal Tax Information in performance of this contract, the Contractor agrees to, when applicable and to the extent

within Contractor's control, comply with and assume responsibility for compliance by officers or employees with the following requirements:

- i. All work will be performed under the supervision of the State of Oklahoma.
- ii. The contractor and contractor's officers or employees to be authorized access to FTI must meet background check requirements defined in IRS Publication 1075. The contractor will maintain a list of officers or employees authorized access to FTI. Such list will be provided to the agency and, upon request, to the IRS.
- iii. FTI in hardcopy or electronic format shall be used only for the purpose of carrying out the provisions of this contract. FTI in any format shall be treated as confidential and shall not be divulged or made known in any manner to any person except as may be necessary in the performance of this contract. Inspection or disclosure of FTI to anyone other than the contractor or the contractor's officers or employees authorized is prohibited.
- iv. FTI will be accounted for upon receipt and properly stored before, during, and after processing. In addition, any related output and products require the same level of protection as required for the source material.
- v. The contractor will certify that FTI processed during the performance of this contract will be completely purged from all physical and electronic data storage with no output to be retained by the contractor at the time the work is completed. If immediate purging of physical and electronic data storage is not possible, the contractor will certify that any FTI in physical or electronic storage will remain safeguarded to prevent unauthorized disclosures.
- vi. Any spoilage or any intermediate hard copy printout that may result during the processing of FTI will be given to the agency. When this is not possible, the contractor will be responsible for the destruction of the spoilage or any intermediate hard copy printouts and will provide the agency with a statement containing the date of destruction, description of material destroyed, and the destruction method.
- vii. All Contractor computer systems receiving, processing, storing, or transmitting FTI must meet the requirements in IRS Publication 1075. To meet functional and assurance requirements, the security features of the environment must provide for the managerial, operational, and technical controls. All security features must be available and activated to protect against unauthorized use of and access to FTI.
- viii. No work involving FTI furnished under this contract will be subcontracted without the prior written approval of the IRS.
- ix. Contractor will ensure that the terms of FTI safeguards described herein are included, without modification, in any approved subcontract for work involving FTI.
- x. To the extent the terms, provisions, duties, requirements, and obligations of this contract apply to performing services with FTI, the contractor shall assume toward the subcontractor all obligations, duties and responsibilities that the agency under this contract assumes toward the contractor, and the subcontractor shall assume toward the contractor all the same obligations, duties and responsibilities which the contractor assumes toward the agency under this contract.

- xi. In addition to the subcontractor's obligations and duties under an approved subcontract, the terms and conditions of this contract apply to the subcontractor, and the subcontractor is bound and obligated to the contractor hereunder by the same terms and conditions by which the contractor is bound and obligated to the agency under this contract.
- xii. For purposes of this contract, the term "contractor" includes any officer or employee of the contractor with access to or who uses FTI, and the term "subcontractor" includes any officer or employee of the subcontractor with access to or who uses FTI.
- xiii. The agency will have the right to void the contract if the contractor fails to meet the terms of FTI safeguards described herein.

b. CRIMINAL/CIVIL SANCTIONS

- i. Each officer or employee of a contractor to whom FTI is or may be disclosed shall be notified in writing that FTI disclosed to such officer or employee can be used only for a purpose and to the extent authorized herein, and that further disclosure of any FTI for a purpose not authorized herein constitutes a felony punishable upon conviction by a fine of as much as \$5,000 or imprisonment for as long as 5 years, or both, together with the costs of prosecution.
- ii. Each officer or employee of a contractor to whom FTI is or may be accessible shall be notified in writing that FTI accessible to such officer or employee may be accessed only for a purpose and to the extent authorized herein, and that access/inspection of FTI without an official need-to-know for a purpose not authorized herein constitutes a criminal misdemeanor punishable upon conviction by a fine of as much as \$1,000 or imprisonment for as long as 1 year, or both, together with the costs of prosecution.
- iii. Each officer or employee of a contractor to whom FTI is or may be disclosed shall be notified in writing that any such unauthorized access, inspection or disclosure of FTI may also result in an award of civil damages against the officer or employee in an amount equal to the sum of the greater of \$1,000 for each unauthorized access, inspection, or disclosure, or the sum of actual damages sustained as a result of such unauthorized access, inspection, or disclosure, plus in the case of a willful unauthorized access, inspection, or disclosure or an unauthorized access/inspection or disclosure which is the result of gross negligence, punitive damages, plus the cost of the action. These penalties are prescribed by IRC sections 7213, 7213A and 7431 and set forth at 26 CFR 301.6103(n)-1.
- iv. Additionally, it is incumbent upon the contractor to inform its officers and employees of the penalties for improper disclosure imposed by the Privacy Act of 1974, 5 U.S.C. 552a. Specifically, 5 U.S.C. 552a(i)(1), which is made applicable to contractors by 5 U.S.C. 552a(m)(1), provides that any officer or employee of a contractor, who by virtue of his/her employment or official position, has possession of or access to agency records which contain individually identifiable information, the disclosure of which is prohibited by the Privacy Act or regulations established thereunder, and who knowing that disclosure of the specific material is so prohibited, willfully discloses the material

in any manner to any person or agency not entitled to receive it, shall be guilty of a misdemeanor and fined not more than \$5,000.

- v. Granting a contractor access to FTI must be preceded by certifying that each officer or employee understands the agency's security policy and procedures for safeguarding FTI. A contractor and each officer or employee must maintain their authorization to access FTI through annual recertification of their understanding of the agency's security policy and procedures for safeguarding FTI. The initial certification and recertifications must be documented and placed in the agency's files for review. As part of the certification and at least annually afterwards, a contractor and each officer or employee must be advised of the provisions of IRC sections 7213, 7213A, and 7431 (see IRS Publication 1075, Exhibit 4, Sanctions for Unauthorized Disclosure, and IRS Publication 1075, Exhibit 5, Civil Damages for Unauthorized Disclosure). The training on the agency's security policy and procedures provided before the initial certification and annually thereafter must also cover the incident response policy and procedure for reporting unauthorized disclosures and data breaches. For the initial certification and the annual recertifications, the contractor and each officer or employee must sign, either with ink or electronic signature, a confidentiality statement certifying their understanding of the security requirements.

c. INSPECTION: The IRS and the Agency, with 24 hour notice, shall have the right to send its inspectors into the offices and plants of the contractor to inspect facilities and operations performing any work with FTI under this contract for compliance with requirements defined in IRS Publication 1075. The IRS' right of inspection shall include the use of manual and/or automated scanning tools to perform compliance and vulnerability assessments of information technology (IT) assets that access, store, process or transmit FTI. Based on the inspection, corrective actions may be required in cases where the contractor is found to be noncompliant with FTI safeguard requirements.

5. SSA Requirements (If applicable)

- a. PERFORMANCE: If Contractor takes possession or control of in SSA provided information in the performance of this contract, the contractor agrees to, where applicable and to the extent within Contractor's control comply with and assume responsibility for compliance by his or her employees with the following requirements:
 - i. All work will be done under the supervision of the State of Oklahoma.
 - ii. Any SSA provided information made available shall be used only for carrying out the provisions of this Agreement. Information contained in such material shall be treated as confidential and shall not be divulged or made known in any manner to any person except as may be necessary in the performance of this contract. Inspection by or disclosure to anyone other than an officer or employee of the Contractor is prohibited.
 - iii. All SSA provided information shall be accounted for upon receipt and properly stored before, during, and after processing. In addition, all related output and products will be given the same level of protection as required for the source material.

- iv. No work involving SSA provided information furnished under this contract shall be subcontracted without prior written approval by the applicable State of Oklahoma agency and the SSA.
- v. The Contractor shall maintain a list of employees authorized access. Such list shall be provided upon request to the applicable State of Oklahoma agency or the SSA.
- vi. Contractor or agents may not legally process, transmit, or store SSA-provided information in a cloud environment without explicit permission from SSA's Chief Information Officer. Proof of this authorization shall be provided to the Contractor by the applicable State of Oklahoma agency prior to accessing SSA provided information.
- vii. Contractor shall provide security awareness training to all employees, contractors, and agents who access SSA-provided information. The training should be annual, mandatory, and certified by the personnel who receive the training. Contractor is also required to certify that each employee, contractor, and agent who views SSA-provided information certify that they understand the potential criminal, civil, and administrative sanctions or penalties for unlawful assess and/or disclosure.
- viii. Contractor shall require employees, contractors, and agents to sign a non-disclosure agreement, attest to their receipt of Security Awareness Training, and acknowledge the rules of behavior concerning proper use and security in systems that process SSA-provided information. Contractor shall retain non-disclosure attestations for at least five (5) to seven (7) years for each employee who processes, views, or encounters SSA-provided information as part of their duties.
- ix. The applicable State of Oklahoma agency shall provide the Contractor a copy of the SSA exchange agreement and all related attachments before initial disclosure of SSA data. Contractor is required to follow the terms of the applicable State of Oklahoma agency's data exchange agreement with the SSA. Prior to signing this Agreement, and thereafter at SSA's request, the applicable State of Oklahoma agency shall obtain from the Contractor a current list of the employees of such Contractor with access to SSA data and provide such list to the SSA.
- x. Where the Contractor processes, handles, or transmits information provided to the applicable State of Oklahoma agency by SSA or has authority to perform on the agency's behalf, the applicable State of Oklahoma agency shall clearly state the specific roles and functions of the Contractor within the Agreement.
- xi. SSA requires all parties subject to this Agreement to exercise due diligence to avoid hindering legal actions, warrants, subpoenas, court actions, court judgments, state or Federal investigations, and SSA special inquiries for matters pertaining to SSA-provided information.
- xii. SSA requires all parties subject to this Agreement to agree that any Client-owned or subcontracted facility involved in the receipt, processing, storage, or disposal of SSA-provided information operate as a "de facto" extension of the Client and is subject to onsite inspection and review by the Client or SSA with prior notice.

- xiii. If the Contractor must send a Contractor computer, hard drive, or other computing or storage device offsite for repair, the Contractor must have a non-disclosure clause in their contract with the vendor. If the Contractor used the item in a business process that involved SSA-provided information and the vendor will retrieve or may view SSA-provided information during servicing, SSA reserves the right to inspect the Contractor's vendor contract. The Contractor must remove SSA-provided information from electronic devices before sending it to an external vendor for service. SSA expects the Contractor to render SSA-provided information unrecoverable or destroy the electronic device if they do not need to recover the information. The same applies to excessed, donated, or sold equipment placed into the custody of another organization.
 - xiv. In the event of a suspected or verified data breach involving SSA provided information, the Contractor shall notify the Client immediately.
 - xv. The Client shall have the right to void the contract if the contractor fails to provide the safeguards described above.
- b. **CRIMINAL/CIVIL SANCTIONS:** The Act specifically provides civil remedies, 5 U.S.C. Sec. 552a(g), including damages, and criminal penalties, 5 U.S.C. Sec. 552a(i), for violations of the Act. The civil action provisions are premised violations of the Act committed by parties subject to this Agreement or regulations promulgated thereunder. An individual claiming such a violation by parties subject to this Agreement may bring civil action in a federal district court. If the individual substantially prevails, the court may assess reasonable attorney fees and other litigation costs. In addition, the court may direct the parties subject to this Agreement to grant the plaintiff access to his/her records, and when appropriate direct an amendment or correction of records subject to the Act. Actual damages may be awarded to the plaintiff for intentional or willful refusal by parties subject to this Agreement to comply with the Act.
- i. **Civil Remedies.**
 - (1) In any suit brought under the provisions of 5 U.S.C. § 552a(g)(1)(C) or (D) in which the court determines that the parties subject to this Agreement acted in a manner which was intentional or willful, shall be liable in an amount equal to the sum of —
 - (a) actual damages sustained by the individual because of the refusal or failure, but in no case, shall a person entitled to recovery receive less than the sum of \$1,000; and
 - (b) the costs of the action together with reasonable attorney fees as determined by the court.
 - (2) An action to enforce any liability created under 5 U.S.C. § 552a may be brought in the district court of the United States in the district in which the complainant resides, or has his principal place of business, or in which the records are situated, or in the District of Columbia, without regard to the amount in controversy, within two years from the date on which the cause of action arises, except that where

parties subject to this Agreement have materially and willfully misrepresented any information required under this section to be disclosed to an individual and the information so misrepresented is material to establishment of the liability of the agency to the individual under 5 U.S.C. § 552a, the action may be brought at any time within two years after discovery by the individual of the misrepresentation. Nothing in this section shall be construed to authorize any civil action because of any injury sustained as the result of a disclosure of a record prior to September 27, 1975.

ii. Criminal Penalties

- (1) Any officer or employee of an agency, who by virtue of his employment or official position, has possession of, or access to, agency records which contain individually identifiable information the disclosure of which is prohibited by this section or by rules or regulations established thereunder, and who knowing that disclosure of the specific material is so prohibited, willfully discloses the material in any manner to any person or agency not entitled to receive it, shall be guilty of a misdemeanor and fined not more than \$5,000. See 5 U.S.C. § 552a(i)(1).
- (2) Any officer or employee of any agency who willfully maintains a system of records without meeting the notice requirements of subsection (e)(4) of this section shall be guilty of a misdemeanor and fined not more than \$5,000. See 5 U.S.C. § 552a(i)(2).
- (3) Any person who knowingly and willfully requests or obtains any record concerning an individual from an agency under false pretenses shall be guilty of a misdemeanor and fined not more than \$5,000. See 5 U.S.C. § 552a(i)(3).

6. Child Support FPLS Requirements (If applicable)

- a. Contractor, when applicable and to the extent within Contractor's control, and the applicable State of Oklahoma agency must comply with the security requirements established by the Social Security Act, the Privacy Act of 1974, the Federal Information Security Management Act of 2002 (FISMA), 42 United States Code (USC) 654(26), 42 UCS 654a(d)(1)-(5), the U.S. Department of Health and Human Services (HHS), the U.S. Department of Health and Human Services Administration of Children and Families Office of Child Support Enforcement Security Agreement and the Automated Systems for Child Support Enforcement: A Guide for States Section H Security and Privacy. Contractor and applicable State of Oklahoma agency also agree to use Federal Parent Locator Service (FPLS) information and Child Support (CS) program information solely for the authorized purposes in accordance with the terms in this agreement. The information exchanged between state Child Support agencies and all other state program information must be used for authorized purposes and protected against unauthorized access to reduce fraudulent activities and protect the privacy rights of individuals against unauthorized disclosure of confidential information.

- i. This is applicable to the personnel, facilities, documentation, data, electronic and physical records and other machine-readable information systems of the applicable State of Oklahoma agency and Contractor, including, but not limited to, state employees and contractors working with FPLS information and CS program information and state CS agency data centers, statewide centralized data centers, contractor data centers, state Health and Human Services' data centers, comprehensive tribal agencies, data centers serving comprehensive tribes, and any other individual or entity collecting, storing, transmitting or processing FPLS information and CS program information. This is applicable to all FPLS information, which consists of the National Directory of New Hires (NDNH), Debtor File, and the Federal Case Registry (FCR). The NDNH, Debtor File and FCR are components of an automated national information system.
- ii. This is also applicable to all CS program information, which includes the state CS program information, other state and tribal program information, and confidential information. Confidential information means any information relating to a specified individual or an individual who can be identified by reference to one or more factors specific to him or her, including but not limited to the individual's Social Security number, residential and mailing addresses, employment information, and financial information. Ref. 45 Code of Federal Regulations (CFR) 303.21(a).

7. FERPA Requirements (If applicable)

- a. If Contractor takes possession or control of Information covered by FERPA in performance of this Agreement, Contractor agrees to, when applicable and to the extent within Contractor's control comply with and assume responsibility for compliance by its employees with the Family Educational Rights and Privacy Act; (20 U.S.C. § 1232g; 34 CFR Part 99) ("FERPA") and the Oklahoma Student Data Accessibility, Transparency, and Accountability Act of 2013; (70 O.S. § 3-168), where personally identifiable student education data is exchanged.

8. CJIS Requirements (If applicable)

- a. INTRODUCTION

This section shall be applicable to the extent that Contractor takes possession or control of CJIS data. The use and maintenance of all items of software or equipment offered for purchase herein must be in compliance with the most current version of the U.S. Department of Justice, Federal Bureau of Investigation ("FBI"), Criminal Justice Information Services (CJIS) Division's CJIS Security Policy ("CJIS Security Policy" or "Security Policy" herein).

The Entity or Affiliate acquiring the data or system is hereby ultimately responsible for compliance with the CJIS Security Policy and will be subject to an audit by the State of Oklahoma CJIS Systems Officer ("CSO") and the FBI CJIS Division's Audit Staff.

b. CJIS SECURITY POLICY REQUIREMENTS GENERALLY

The CJIS Security Policy outlines a number of administrative, procedural, and technical controls agencies must have in place to protect Criminal Justice Information (“CJI”). Our experience is that agencies will generally have many of the administrative and procedural controls in place but will need to implement additional technical safeguards in order to be in complete compliance with the mandate. A Criminal Justice Agency (“CJA”) and certain other governmental agencies procuring technology equipment and services that could be used in hosting or connecting or transmitting or receiving CJI data may need to use the check list herein to make sure that the software, equipment, location, security, and persons having the ability to access CJI will meet the CJIS requirements per the then current CJIS Security Policy. A completed Appendix H to said Security Policy will need to be signed by Vendor or a 3rd party if it has access to CJI, such as incident to the maintenance or support of the purchased hardware or software within which resides CJI. Per Appendix “A” to said Security Policy, “access to CJI is the physical or logical (electronic) ability, right or privilege to view, modify or make use of CJI.”

c. DIRECTIVE CONCERNING ACCESS TO CRIMINAL JUSTICE INFORMATION AND TO HARDWARE OR SOFTWARE WHICH INTERACTS WITH CJI AND CERTIFICATION

The FBI CJIS Division provides state-of-the-art identification and information services to the local, state, tribal, federal, and international criminal justice communities for criminal justice purposes, as well as the noncriminal justice communities for noncriminal justice purposes.

This Directive primarily concerns access to CJI and access to hardware and software in the use, retention, transmission, reception, and hosting of CJI for criminal justice purposes and not for noncriminal justice purposes. In that regard, this Directive is not only applicable to such data, but also to the hardware and software interacting with such data, their location(s), and persons having the ability to access such data. The CJIS data applicable to the Security Policy is the data described as such in said Policy plus all data transmitted over the Oklahoma Law Enforcement Telecommunications System (“OLETS”) which is operated by DPS.

In order to have access to CJI or to the aforesaid hardware or software, the vendor must be familiar with the FBI CJIS Security Policy, including but not limited to the following portions of said Security Policy:

1. the Definitions and Acronyms in §3 & Appendices “A” & “B”;

2. the general policies in §4;
3. the Policies in §5;
4. the appropriate forms in Appendices “D”, “E”, “F” & “H”; and
5. the Supplemental Guidance in Appendices “J” & “K”.

This FBI Security Policy is located and may be downloaded at:
<https://www.fbi.gov/services/cjis/cjissecurity-policy-resource-center>.

By executing the Contract to which this Directive is attached, the vendor hereby CERTIFIES that the foregoing directive has and will be followed, including but not limited to full compliance with the FBI CJIS Security Policy, as amended and as applicable.

Software Publishers		Description	Maximum Cost + % Markup	% off List Price
Pulselight Torch® Program Integrity Standard Solution 1st Year License & Implementation			\$ 1,650,000	
Pulselight Torch® Program Integrity Standard Solution Annual License Subscription			\$ 540,000	
Pulselight Torch® Program Integrity Premier Solution 1st Year License & Implementation			\$ 2,250,000	
Pulselight Torch® Program Integrity Premier Solution Annual License Subscription			\$ 540,000	
Pulselight Torch® Program Integrity Premier Solution with Expanded Database 1st Year License & Implementation			\$ 2,495,000	
Pulselight Torch® Program Integrity Premier Solution with Expanded Database Annual License Subscription			\$ 648,000	
Pulselight Torch® Incident Detection Standard Solution 1st Year License & Implementation			\$ 1,650,000	
Pulselight Aura™ Incident Detection Standard Solution Annual License Subscription			\$ 540,000	
Pulselight Aura™ Incident Detection Premier Solution 1st Year License & Implementation			\$ 1,900,000	
Pulselight Aura™ Incident Detection Premier Solution Annual License Subscription			\$ 540,000	
Pulselight Aura™ Incident Detection Premier Solution with Expanded Database 1st Year License & Implementation			\$ 2,200,000	
Pulselight Aura™ Incident Detection Premier Solution with Expanded Database Annual License Subscription			\$ 648,000	
Pulselight Aura™ Multi-Agency Incident Detection Standard Solution 1st Year License & Implementation			\$ 2,200,000	
Pulselight Aura™ Multi-Agency Incident Detection Standard Solution Annual License Subscription			\$ 600,000	
Pulselight Aura™ Multi-Agency Incident Detection Premier Solution 1st Year License & Implementation			\$ 2,400,000	
Pulselight Aura™ Multi-Agency Incident Detection Premier Solution Annual License Subscription			\$ 600,000	
Pulselight Aura™ Multi-Agency Incident Detection Premier Solution with Expanded Database 1st Year License & Implementation			\$ 2,650,000	
Pulselight Aura™ Multi-Agency Incident Detection Premier Solution with Expanded Database Annual License Subscription			\$ 675,000	
Pulselight Opioid/Drug Utilization Solution 1st Year License & Implementation			\$ 750,000	
Pulselight Opioid/Drug Utilization Solution Annual License Subscription			\$ 360,000	
Pulselight Maestro Case Tracker Solution 1st Year License & Implementation			\$ 1,200,000	
Pulselight Maestro Case Tracker Solution Annual License Subscription			\$ 420,000	
Pulselight EVV Analytics Solution 1st Year License & Implementation			\$ 1,125,000	
Pulselight EVV Analytics Solution Annual License Subscription			\$ 475,000	
Pulselight Bundled Discounts - 20% off above pricing for multiple product families				20%

Other Value Add Products and Services		Description	Maximum Cost + % Markup	% off List Price

Professional Services - Hourly Not-to-Exceed Rates			
	Description	List Price	Discounted Hourly Rates
Subject Matter Expert - Healthcare		\$ 320.00	\$ 295.00
Subject Matter Expert - Analytics		\$ 320.00	\$ 295.00
Subject Matter Expert - Data		\$ 320.00	\$ 295.00
Project Manager		\$ 200.00	\$ 185.00
Principal Data Scientist		\$ 385.00	\$ 355.00
Security Expert		\$ 300.00	\$ 275.00
Software Architect		\$ 320.00	\$ 295.00
Sr. SW Engineer		\$ 285.00	\$ 260.00
Sr. UI Engineer		\$ 260.00	\$ 240.00
Data Engineer		\$ 250.00	\$ 230.00
Sr. Data Analyst		\$ 225.00	\$ 205.00
Data Analyst		\$ 195.00	\$ 180.00
Investigator		\$ 150.00	\$ 140.00
Analyst		\$ 125.00	\$ 115.00

Attachment E-2 to
STATE OF OKLAHOMA CONTRACT WITH PULSELIGHT HOLDINGS, INC.
RESULTING FROM SOLICITATION NO. 0900000556

The Statement of Work is hereby amended as set forth below and supersedes all prior documents submitted by Pulselight Holdings, Inc. or discussed by the parties. The parties agree to use this Statement of Work or a document substantially similar in the form of this Statement of Work.

Supplier ID Number: _____

**PULSELIGHT ENTERPRISE SAAS SOFTWARE/SERVICES LICENSE
REQUIREMENTS AGREEMENT**

This Enterprise SaaS Software/Services License Requirements Agreement (“Agreement”) is entered into by and between **Pulselight Holdings, Inc.** (“Licensor”) and the _____ (“Customer”).

The parties intending to be legally bound, agree as follows:

- 1. Order of Precedence.** Reserved.
- 2. Effective Date.** Reserved.
- 3. Enterprise Language.**
 - (a) The parties agree that more than one agency of the Customer (“Customer Agency”) may license products subject to this Agreement, provided that the procurement of any Licensed Products by any Customer Agency must be made pursuant to one or more executed purchase orders or purchase documents submitted by each Customer Agency seeking to use the Licensed Products.
 - (b) The terms and conditions of SW Contract No. 1041 apply to the procurement of any Licensed Products made by the Customer, and that the terms and conditions of this Agreement become part of the purchase order or other procurement document without further need for execution.
- 4. List of Licensed Products.**
 - (a) Attached hereto and made a part of this Agreement by reference is Attachment 1, which lists the Licensed Products that may be licensed under this Agreement. With the consent of the Customer, the list of Licensed Products on Attachment 1 may be

updated by the Licensor providing the Customer with a revised Attachment 1 that adds the new product to the list. The Customer, in its sole discretion, may consent either via written communication directly to the Licensor or, if applicable, providing the Customer's reseller with a copy of Licensor's notification to update Attachment 1.

- (b) No amendment will be required to add a new Licensed Product to the list. If, however, the Licensor desires to add a new Licensed Product to the list that requires additional licensing terms or other requirements, either an amendment to this Agreement or a new agreement will be required.

5. Choice of Law/Venue. Reserved.

6. Indemnification/Immunity.

- (a) Resereved.

7. Patent, Copyright, Trademark and Trade Secret Protection.

- (a) Reserved.

8. Virus, Malicious, Mischievous or Destructive Programming.

- (a) The Licensor warrants that the Licensed Products as delivered by the Licensor does not contain any viruses, worms, Trojan Horses, or other malicious or destructive code to allow unauthorized intrusion upon, disabling of, or erasure of the Licensed Products (each a "Virus"). However, the Licensed Products may contain a key limiting use to the scope and quantity of the license(s) granted, and license keys issued by the Licensor for temporary use are time-sensitive.

9. Limitation of Liability.

- (a) Reserved.

10. Payment.

Reserved.

11. Termination.

- (a) Reserved.

12. Background Checks.

- (a) Reserved.

13. Confidentiality.

(a) Reserved.

14. Reserved

15. Data Breach or Loss.

(a) Reserved.

16. Hyperlink Content. Any terms and conditions contained in any hyperlink content referenced in this Agreement (“Hyperlink Content”) shall not apply. Terms and conditions in the Hyperlink Content that are materially inconsistent with the Agreement are rejected, unenforceable by the Licensor, and shall not become part of this Agreement unless such terms and conditions are to the benefit of the Customer.

17. Publicity/Advertisement. Reserved.

18. Portability. The parties agree that a Customer Agency may move a Licensed Product from machine to machine, whether physical or virtual, and to other locations, where those machines and locations are internal to the Customer or to a Customer contractor, as long as such relocation and the use being made of the Licensed Product comports with the license grant and restrictions. Notwithstanding the foregoing, a Customer Agency may move the machine or appliance provided by the Licensor upon which the Licensed Product is installed.

19. Taxes-Federal, State and Local; Interest.

(a) Reserved.

20. Customer Audit Responsibilities.

(a) Reserved.

21. Reserved.

22. Third-Party Software. If a Licensed Product utilizes or includes third party software and other copyrighted material, any additional licensing terms, acknowledgements or disclaimers associated with the third-party software and materials shall not be applicable to the Customer unless agreed to in writing. The parties agree that the Customer, by acknowledging third-party software, does not agree to any terms and conditions of the third-party software agreements.

23. Attorneys’ Fees. The Customer is not responsible for and shall not pay attorneys’ fees incurred by or paid by the Licensor.

24. Controversies.

- (a) Reserved.

25. Insurance.

- (a) Reserved.

26. Signatures.

- (a) The parties agree that: (1) a record or signature may not be denied legal effect or enforceability solely because it is in electronic form; (2) a contract may not be denied legal effect or enforceability solely because an electronic record was used in its formation; (3) if a law requires a record to be in writing, an electronic record satisfies the law; and (4) if law requires a signature, an electronic signature satisfies the law.
- (b) The fully executed Agreement may not contain ink signatures by the Customer. If this Agreement does not contain ink signatures by the Customer, the Licensor understands and agrees that the receipt of an electronically-printed Agreement with the printed name of the Customer purchasing agent constitutes a valid, binding contract with the Customer. The printed name of the purchasing agent represents the signature of that individual who is authorized to bind the Customer to the obligations contained in this Agreement. The printed name also indicates that all approvals required by Customer contracting procedures have been obtained.

27. Independent Contractor. The parties are independent contractors, and this Agreement does not create an agency, partnership or joint venture.

28. Travel. Reserved.

29. Entire Agreement. Reserved.

30. Assignment. Reserved.

31. Notice. Reserved.

32. **Survival.** Reserved.
33. **Waiver.** Failure to enforce any provision will not constitute a waiver.
34. **Severability.** Reserved.
35. **Nonexclusive Remedy.** Reserved.
36. **Integration.** Reserved.

The parties to this Agreement have executed it, through their respective duly authorized representatives.

Witness:

Licensor:

Signature Date

Signature Date

Printed Name

Printed Name

Title

Title

.

CUSTOMER

Agency Head or Designee

ATTACHMENT 1

LIST OF LICENSED PRODUCTS

With the consent of the Customer, additional Licensed Products may be added to this attachment by Licensor providing the Customer with a new copy of this Attachment 1.

Licensed Products:

The Licensed Products include:

Pulselight Torch® Program Integrity Solution
Pulselight Aura™ Incident Detection Solution
Pulselight Opioid/Drug Utilization Solution
Pulselight Maestro Case Tracker Solution
Pulselight EVV Analytics Solution

Attachment E-3 to

STATE OF OKLAHOMA CONTRACT WITH PULSELIGHT HOLDINGS, INC.
RESULTING FROM SOLICITATION NO. 0900000556

The Statement of Work is hereby amended as set forth below and supersedes all prior documents submitted by Pulselight Holdings, Inc. or discussed by the parties. The parties agree to use this Statement of Work or a document substantially similar in the form of this Statement of Work.

PULSELIGHT AUTHORIZED USER TERMS OF USE AGREEMENT

(v1412 1/1/2020)

These Authorized User Terms of Use ("**Terms of Use**") govern your use of the Pulselight software and the Pulselight web-based application (collectively, the "**Software**"), including all user manuals, technical manuals and any other materials provided by Pulselight, in printed, electronic or other form, that describe the Software or its use or specifications (the "**Documentation**") provided to you ("**you**" or "**your**") for use pursuant to and subject to the Software Subscription Agreement or other Pulselight license agreement (such agreement, including all subsequent amendments, the "**Statewide Contract No. 1041**"), between Pulselight Holdings, Inc. ("**Licensor**") and the Pulselight licensee with which you are employed, affiliated, or associated ("**Licensee**").

BY ACCEPTING AND USING THE PULSELIGHT ACCESS CREDENTIALS YOU: (i) ACKNOWLEDGE THAT YOU HAVE READ AND UNDERSTOOD THESE TERMS OF USE; (ii) ARE DULY AUTHORIZED BY LICENSEE TO AGREE TO THESE TERMS OF USE AND TO ACCESS AND USE THE SOFTWARE; AND (iii) ACCEPT AND AGREE TO BE LEGALLY BOUND BY THESE TERMS OF USE. IF YOU DO NOT AGREE TO THESE TERMS OF USE, DO NOT USE THE PULSELIGHT ACCESS CREDENTIALS AND YOU WILL HAVE NO LICENSE TO, AND MUST NOT ACCESS OR USE, THE SOFTWARE.

1. **Access Grant.** Subject to your strict compliance with these Terms of Use, Licensor hereby grants you a non-exclusive, non-transferable, non-sublicensable, access to use the Software solely in accordance with the Master Agreement and all amendments thereto, the Documentation, and for Licensee's authorized internal business purposes. The foregoing access will terminate immediately on the earlier to occur of:

- (a) the expiration or earlier termination of the Master Agreement; or
- (b) your ceasing to be authorized by Licensee to use the Software for any or no reason.

2. **Use Conditions.** You shall not, directly or indirectly:

- (a) use the Software or Documentation except as set forth in Section 1;
- (b) copy the Software or Documentation, in whole or in part;
- (c) modify, translate, adapt or otherwise create derivative works or improvements, whether or not patentable, of the Software or any part thereof;
- (d) combine the Software or any part thereof with, or incorporate the Software or any part thereof in, any other programs;
- (e) reverse engineer, disassemble, decompile, decode or otherwise attempt to derive or gain access to the source code of the Software or any part thereof;
- (f) remove, delete, alter or obscure any trademarks or any copyright, trademark, patent or other intellectual property or proprietary rights notices included on or in the Software or Documentation, including any copy thereof;
- (g) rent, lease, lend, sell, sublicense, assign, distribute, publish, transfer or otherwise provide

any access to or use of the Software or any features or functionality of the Software, for any reason, to any other person or entity, including any subcontractor, independent contractor, affiliate or service provider of Licensee, whether or not over a network and whether or not on a hosted basis, including in connection with the internet, web hosting, wide area network (WAN), virtual private network (VPN), virtualization, time-sharing, service bureau, software as a service, cloud or other technology or service;

(i) use the Software or Documentation in violation of any law, regulation or rule; or
(j) use the Software or Documentation for purposes of competitive analysis of the Software, the development of a competing software product or service or any other purpose that is to the Licensor's commercial disadvantage.

3. Security and Protection of Confidential and Private Information.

(a) Through your use of and access to the Software you may have access to confidential information protected under federal or state law, including but not limited to patient/client identifying or medical information, protected health information, personal identification information, Internal Revenue Service (IRS) or other federal or state tax Information, information relating to any fraud investigation, and any other information that is classified or deemed confidential by federal or state law ("Confidential Information"). "Confidential Information" also includes Documentation or other information identified as Confidential by Licensor, security features designed to detect or prevent unauthorized use of the Software, and information regarding the design, structure, construction, and operation of the Software. You will safeguard all such Confidential Information and you will not use or disclose Confidential Information except as authorized by law.

(b) You will safeguard the access credentials provided to you for your access and use of the Software. You will not: (i) use or disclose access credentials except as authorized by law; (ii) use or disclose access credentials of another; (iii) let another use your access credentials, and (iv) disclose your access credentials to another.

(c) If any unauthorized access, disclosure, or use of Confidential Information or access credentials comes to your attention, you will immediately notify Licensor and your Licensee supervisor.

4. Collection and Use of Information.

(a) Licensor may, directly or indirectly through the services of others, and in ways that may not be disclosed to you or apparent to you at the time, monitor your use of the Software and collect and store information regarding your use of the Software and about equipment on which the Software is installed or through which it otherwise is accessed and used.

5. Intellectual Property Rights. You acknowledge that the Software is provided under license, and not sold, to you. You do not acquire any ownership interest in the Software under these Terms of Use, nor do you acquire any other rights to the Software other than to use the Software in accordance with the license granted under these Terms of Use and the Master Agreement, subject to all terms, conditions and restrictions. Licensor, and any of its third party licensors,

reserve and shall retain its entire right, title and interest in and to the Software and all intellectual property rights arising out of or relating to the Software, subject to the license expressly granted to the Licensee in the Master Agreement. You shall safeguard the Software (including all copies thereof) and Documentation from infringement, misappropriation, theft, misuse or unauthorized access.

6. **Export Regulation.** The Software may be subject to US export control laws, including the US Export Administration Act and its associated regulations. You shall not, directly or indirectly, export, re-export or release the Software to, or make the Software or Documentation accessible from, any jurisdiction or country to which export, re-export or release is prohibited by law, rule or regulation. You shall comply with all applicable federal laws, regulations and rules, and complete all required undertakings (including obtaining any necessary export license or other governmental approval), prior to exporting, re-exporting, releasing or otherwise making the Software available outside the United States of America.

7. **LIMITATIONS OF RIGHTS AND REMEDIES; DISCLAIMER OF WARRANTIES.** Reserved.

8. **Governing Law.** Reserved.

9. **Entire Agreement; Severability.** Reserved.

**Attachment F to
STATE OF OKLAHOMA CONTRACT WITH PULSELIGHT HOLDINGS, INC.
RESULTING FROM SOLICITATION NO. 0900000556**

Negotiated Exceptions and Additional Terms to the Contract

The Contract is hereby amended to include the terms as set forth below and supersedes all prior terms and exceptions submitted by PULSELIGHT HOLDINGS, INC. or discussed by the parties.

Requested Exceptions and Additional Terms not addressed below are declined by the State of Oklahoma.

Term & Section	Language
General Terms, Definitions (Attachment B, Section 4.21, pgs. 5-6)	Work Product means any and all deliverables produced by Supplier <u>solely</u> under a statement of work or similar Contract Document issued pursuant to this Contract, <u>and excludes Supplier Intellectual Property as defined in this Agreement</u> , including any and all tangible or intangible items or things that have been or will be prepared, created, developed, invented or conceived at any time following the Contract effective date including but not limited to any (i) works of authorship (such as manuals, instructions, printed material, graphics, artwork, images, illustrations, photographs, computer programs, computer software, scripts, object code, source code or other programming code, HTML code, flow charts, notes, outlines, lists, compilations, manuscripts, writings, pictorial materials, schematics, formulae, processes, algorithms, data, information, multimedia files, text web pages or web sites, other written or machine readable expression of such works fixed in any tangible media, and all other copyrightable works), (ii) trademarks, service marks, trade dress, trade names, logos, or other indicia of source or origin, (iii) ideas, designs, concepts, personality rights, methods, processes, techniques, apparatuses, inventions, formulas, discoveries, or improvements, including any patents, trade secrets and know-how, (iv) domain names, (v) any copies, and similar or derivative works to any of the foregoing <u>solely for the Customer under this Contract</u> , (vi) all documentation and materials related to any of the foregoing, (vii) all other goods, services or deliverables to be provided by or on behalf of Supplier under the Contract and (viii) all Intellectual Property Rights in any of the foregoing, and which are or were created, prepared, developed, invented or conceived for the use of benefit of Customer in connection with this Contract or with funds appropriated by or for Customer or Customer's benefit (a) by any Supplier personnel or Customer personnel or (b) any Customer personnel who then became personnel to Supplier or any of its affiliates or subcontractors, where, although creation or reduction-to-practice is completed while the person is affiliated with Supplier or its personnel, any portion of same was created, invented or conceived by such person while affiliated with Customer, <u>solely for the purpose of the Customer under this Contract</u> .
General Terms, Invoices and Payment (Attachment B, Section 7.1.C, pg. 8)	Payment of all fees under the Contract shall be due NET 45 days. Payment and interest on late payments are governed by 62 O.S. §34.72. Such interest is the sole and exclusive remedy for late payments by a State agency and no other late fees are authorized to be assessed pursuant to Oklahoma law.

<p>Information Technology Terms, Definitions (Attachment D, Section 1.13, pgs. 2-3)</p>	<p>Work Product means any and all deliverables produced by Supplier <u>solely</u> under a statement of work or similar Contract Document issued pursuant to this Contract, <u>and excludes Supplier Intellectual Property as defined in this Agreement</u>, including any and all tangible or intangible items or things that have been or will be prepared, created, developed, invented or conceived at any time following the Contract effective date including but not limited to any (i) works of authorship (such as manuals, instructions, printed material, graphics, artwork, images, illustrations, photographs, computer programs, computer software, scripts, object code, source code or other programming code, HTML code, flow charts, notes, outlines, lists, compilations, manuscripts, writings, pictorial materials, schematics, formulae, processes, algorithms, data, information, multimedia files, text web pages or web sites, other written or machine readable expression of such works fixed in any tangible media, and all other copyrightable works), (ii) trademarks, service marks, trade dress, trade names, logos, or other indicia of source or origin, (iii) ideas, designs, concepts, personality rights, methods, processes, techniques, apparatuses, inventions, formulas, discoveries, or improvements, including any patents, trade secrets and know-how, (iv) domain names, (v) any copies, and similar or derivative works to any of the foregoing <u>solely for the Customer under this Contract</u>, (vi) all documentation and materials related to any of the foregoing, (vii) all other goods, services or deliverables to be provided by or on behalf of Supplier under the Contract and (viii) all Intellectual Property Rights in any of the foregoing, and which are or were created, prepared, developed, invented or conceived for the use of benefit of Customer in connection with this Contract or with funds appropriated by or for Customer or Customer's benefit (a) by any Supplier personnel or Customer personnel or (b) any Customer personnel who then became personnel to Supplier or any of its affiliates or subcontractors, where, although creation or reduction-to-practice is completed while the person is affiliated with Supplier or its personnel, any portion of same was created, invented or conceived by such person while affiliated with Customer, <u>solely for the purpose of the Customer under this Contract</u>.</p>
<p>Information Technology Terms, Emerging Technologies (Attachment D, Section 7, pg. 5)</p>	<p>The State of Oklahoma reserves the right to enter into an Addendum to the Contract at any time to allow for emerging technologies not identified elsewhere in the Contract Documents if there are repeated requests for such emerging technology or the State determines it is warranted to add such technology, <u>subject to additional fees and scope to be negotiated by the parties</u>.</p>
<p>Information Technology Terms, Extension Right (Attachment D, Section 8, pg. 5)</p>	<p>In addition to extension rights of the State set forth in the Contract, the State CIO reserves the right to extend any Contract if the State CIO determines such extension to be in the best interest of the State, <u>subject to additional fees and scope to be negotiated by the parties</u>.</p>

<p>Information Technology Terms, Ownership Rights (Attachment D, Section 11, pgs. 6-7)</p>	<p><u>Except for Supplier's Intellectual Property, A</u>any software developed by the Supplier <u>solely</u> under the terms of the Contract is for the sole and exclusive use of the State including but not limited to the right to use, reproduce, re-use, alter, modify, edit, or change the software as it sees fit and for any purpose. Moreover, except with regard to any deliverable based on Supplier Intellectual Property, the State shall be deemed the sole and exclusive owner of all right, title, and interest therein, including but not limited to all source data, information and materials furnished to the State, together with all plans, system analysis, and design specifications and drawings, completed programs and documentation thereof, reports and listing, all data and test procedures and all other items pertaining to the work and services to be performed pursuant to this Contract including all copyright and proprietary rights relating thereto. With respect to Supplier Intellectual Property, the Supplier grants the State, for no additional consideration, a perpetual, irrevocable, royalty-free license, solely for the internal business use of the State, to use, copy, modify, display, perform, transmit and prepare derivative works of Supplier Intellectual Property embodied in or delivered to the State in conjunction with the products. Except for any Supplier Intellectual Property, all work performed by the Supplier of developing, modifying or customizing software and any related supporting documentation shall be considered as Work for Hire (as defined under the U.S. copyright laws) and, as such, shall be owned by and for the benefit of State. In the event that it should be determined that any portion of such software or related supporting documentation does not qualify as "Work for Hire", Supplier hereby irrevocably grants to the State, for no additional consideration, a non-exclusive, irrevocable, royalty-free license to use, copy, modify, display, perform, transmit and prepare derivative works of any such software and any Supplier Intellectual Property embodied in or delivered to the State in conjunction with the products. Supplier shall assist the State and its agents, upon request, in preparing U.S. and foreign copyright, trademark, and/or patent applications covering software developed, modified or customized for the State. Supplier shall sign any such applications, upon request, and deliver them to the State. The State shall bear all expenses that incurred in connection with such copyright, trademark, and/or patent applications. If any Acquisition pursuant to this Contract is funded wholly or in part with federal funds, the source code and all associated software and related documentation owned by the State may be shared with other publicly funded agencies at the discretion of the State without permission from or additional compensation to the Supplier, <u>except for Supplier's Intellectual Property, including without limitation, the product for which Customer is getting a license and paying a fee under this Contract.</u></p>
<p>Information Technology Terms, Intellectual Property Ownership (Attachment D, Section 12.1, pg. 7)</p>	<p><u>Except for Supplier's Intellectual Property, including without limitation, the products for which Customer is getting a license and paying a fee under this Contract A</u>as between Supplier and Customer, the Work Product and Intellectual Property Rights therein are and shall be owned exclusively by Customer, and not Supplier. Supplier specifically agrees that the Work Product shall be considered "works made for hire" and that the Work Product shall, upon creation, be owned exclusively by Customer. To the extent that the Work Product, under applicable law, may not be considered works made for hire, Supplier hereby agrees that all right, title and interest in and to all ownership rights and all Intellectual Property Rights in the Work Product is hereby effectively transferred, granted, conveyed, assigned and relinquished</p>

	<p>exclusively to Customer, without the necessity of any further consideration, and Customer shall be entitled to obtain and hold in its own name all Intellectual Property Rights in and to the Work Product. Supplier acknowledges that Supplier and Customer do not intend Supplier to be a joint author of the Work Product within the meaning of the Copyright Act of 1976. Customer shall have access, during normal business hours (Monday through Friday, 8:00 a.m. to 5:00 p.m.) and upon reasonable prior notice to Supplier, to all Supplier materials, premises and computer files containing the Work Product. Supplier and Customer, as appropriate, will cooperate with one another and execute such other documents as may be reasonably appropriate to achieve the objectives herein. No license or other right is granted under the Contract to any Third Party</p> <p>Intellectual Property, except as may be incorporated in the Work Product by Supplier.</p>
Information Technology Terms, Intellectual Property Ownership (Attachment D, Section 12.2, pgs. 7-8)	<p>Supplier, upon request and without further consideration, shall perform any acts that may be deemed reasonably necessary or desirable by Customer to evidence more fully the transfer of ownership and/or registration of all Intellectual Property Rights in all Work Product to Customer, <u>excluding Supplier's Intellectual Property</u>, to the fullest extent possible including, but not limited to, the execution, acknowledgement and delivery of such further documents in a form determined by Customer. In the event Customer shall be unable to obtain Supplier's signature due to the dissolution of Supplier or Supplier's failure to respond to Customer's repeated requests for such signature on any document reasonably necessary for any purpose set forth in the foregoing sentence, Supplier hereby irrevocably designates and appoints Customer and its duly authorized officers and agents as Supplier's agent and Supplier's attorney-in-fact to act for and in Supplier's behalf and stead to execute and file any such document and to do all other lawfully permitted acts to further any such purpose with the same force and effect as if executed and delivered by Supplier, provided however that no such grant of right to Customer is applicable if Supplier fails to execute any document due to a good faith dispute by Supplier with respect to such document. It is understood that such power is coupled with an interest and is therefore irrevocable. Customer shall have the full and sole power to prosecute such applications and to take all other action concerning the Work Product, and Supplier shall cooperate, at Customer's sole expense, in the preparation and prosecution of all such applications and in any legal actions and proceedings concerning the Work Product.</p>
Information Technology Terms, Intellectual Property Ownership (Attachment D, Section 12.3, pg. 8)	<p><u>Each partySupplier</u> hereby irrevocably and forever waives, and agrees never to assert, any Moral Rights in or to the <u>other's</u> Work Product which <u>that partySupplier</u> may now have or which may accrue to <u>the owning party'sSupplier's</u> benefit under U.S. or foreign copyright or other laws and any and all other residual rights and benefits which arise under any other applicable law now in force or hereafter enacted. <u>Each partySupplier</u> acknowledges the receipt of equitable compensation for its assignment and waiver of such Moral Rights.</p>
Information Technology Terms, Intellectual Property Ownership (Attachment D, Section 12.4, pg. 8)	<p><u>Except for Supplier's Intellectual Property</u>, <u>All</u> documents, information and materials forwarded to Supplier by Customer for use in and preparation of the Work Product shall be deemed the confidential information of Customer, subject to the license granted by Customer to Supplier hereunder. Supplier shall not otherwise use, disclose, or permit any third party to use or obtain the Work Product, or any portion thereof, in any manner without the prior written approval of Customer.</p>
Information	<p>These provisions are intended to protect Customer's <u>and Supplier's</u></p>

Technology Terms, Intellectual Property Ownership (Attachment D, Section 12.5, pg. 8)	proprietary rights pertaining to the Work Product, and the Intellectual Property Rights <u>and Supplier's Intellectual Property</u> therein and any misuse of such rights would cause substantial and irreparable harm to Customer's <u>and/or Supplier's</u> business. Therefore, <u>each party</u> Supplier acknowledges and stipulates that a court of competent jurisdiction may immediately enjoin a material breach of the other's <u>Supplier's</u> obligations with respect to confidentiality provisions of the Contract and the Work Product and a Customer's <u>or Supplier's</u> Intellectual Property Rights, upon a request by <u>either party</u> Customer , without requiring proof of irreparable injury, as same is presumed.
Information Technology Terms, Intellectual Property Ownership (Attachment D, Section 12.11, pg. 9)	If any Acquisition pursuant to the Contract is funded wholly or in part with federal funds, the source code and all associated software and related documentation and materials owned by a Customer may be shared with other publicly funded agencies at the discretion of such Customer without permission from or additional compensation to the Supplier, <u>except for Supplier's Intellectual Property, including without limitation, the product for which Customer is getting a license and paying a fee under this Contract.</u>



Official signed contract documents are on file with OMES Central Purchasing.

Contract title: Software Value Added Reseller

Contract Number: SW1041R

Date of Contract issuance: 12/13/2023

Contract period: 12/13/2023 through 03/13/2025

Agreement period: 12/13/2023 through 03/14/2028

Type of contract: Mandatory ☐ Non-Mandatory ☒

OMES Central Purchasing contact: Barry Timberlake

Title: Procurement Specialist

Phone: (405) - 521 - 6721

Email: barry.timberlake@omes.ok.gov

Supplier name: Rattan Consulting

Supplier ID #: 62786

Contract ID #: 7521

Supplier Point of Contact:

Supplier address: 4334 Northwest Expressway, Ste 259

City: Oklahoma City

State: OK

Zip Code: 73116 -

Phone #: 1 - - -

Email

Contract Overview:

Authorized Users: All state departments, boards, commissions, agencies, and institutions, in Addition to counties, school districts and municipalities which may avail themselves of this contract.

How to order:

Available Brands:

Available Products and Services:

Authorized Dealer/Reseller(s):

Supplier name:

Supplier ID #:

Contract ID #:

Supplier Point of Contact:

Supplier address:

City:

State:

Zip Code:

-

Phone #: 1 - - -

Email:

Supplier name:

Supplier ID #:

Contract ID #:

Supplier Point of Contact:

Supplier address:

City:

State:

Zip Code:

-

Phone #: 1 - - -

Email:



**STATE OF OKLAHOMA STATEWIDE CONTRACT WITH
RATTAN CONSULTING, INC.**

This State of Oklahoma Statewide Contract No. 1041 (“Contract”) is entered into between the state of Oklahoma by and through the Office of Management and Enterprise Services and Rattan Consulting, Inc. (“Supplier”) and is effective as the date of the last signature to this Contract. The initial Contract term, which begins on the effective date of the Contract, is one year and there are four (4) one-year options to renew the Contract.

Purpose

The State is awarding this Contract to Supplier for software and services to support State agencies and other eligible Oklahoma Interlocal Entities. This Supplier will provide software, training, presales assistance, documentation, installation, maintenance, support, configuration, customization, and license agreement administration, as more particularly described in certain Contract Documents. Supplier submitted a proposal which did not contain exceptions to the Solicitation and a best and final offer. This Contract memorializes the agreement of the parties with respect to negotiated terms of the Contract that is being awarded to Supplier.

Now, therefore, in consideration of the foregoing and the mutual promises set forth herein, the receipt and sufficiency of which are hereby acknowledged the parties agree as follows:

1. The parties agree that Supplier has not yet begun performance of work under this Contract. Upon full execution of this Contract, Supplier may begin work. Issuance of a purchase order is required prior to payment to a Supplier.
2. The following Contract Documents are attached hereto and incorporated herein:
 - 2.1. Solicitation, Attachment A;
 - 2.2. General Terms, Attachment B;
 - 2.3. Oklahoma Statewide Contract Terms, Attachment C;
 - 2.4. State of Oklahoma Information Technology Terms, Attachment D;
 - 2.5. Information Security Requirements, Attachment D1;
 - 2.6. Additional Terms, Attachment E1;
 - 2.7. Master Terms, Attachment E2;
 - 2.8. Pricing, Attachment E3;
 - 2.9. Value-Add, Attachment E4;
 - 2.10. Third Party, Attachment E5;


- 2.11. Negotiated Exceptions to Contract, Attachment F; and
 - 2.12. Template for Contract Modifications for Quotes, Statements of Work, or other Ordering Documents, Attachment F1;
3. The parties additionally agree:
- 3.1. Except for information deemed confidential by the State pursuant to applicable law, rule, regulation or policy, the parties agree Contract terms and information are not confidential and are disclosable without further approval of or notice to Supplier.
 - 3.2. Unless mutually agreed to in writing by the Chief Information Officer (CIO) utilizing Attachment F-1, no Contract Document or other terms and conditions or clauses, including via a hyperlink or uniform resource locator shall supersede or conflict with the terms of this Contract or expand the State's or Customer's liability or reduce the rights of Customer or the State. If supplier is acting as a reseller, any third-party terms provided are also subject to the foregoing.
 - 3.3. To the extent any term or condition in any Contract Document, including via a hyperlink or uniform resource locator, conflicts with an applicable Oklahoma and/or United States law or regulation, such term or condition is void and unenforceable. By executing any Contract Document which contains a conflicting term or condition, the State or Customer makes no representation or warranty regarding the enforceability of such term or condition and the State or Customer does not waive the applicable Oklahoma and/or United States law or regulation which conflicts with the term or condition.
 - 3.4. Supplier, as a software value added reseller, is required to ensure that any software or information technology resold complies with applicable law and the Compliance and Electronic and Information Technology Accessibility clause in the Contract. This includes providing the State with a Voluntary Product Accessibility Template ("VPAT"). If the software or information technology is not compliant. Supplier holds an affirmative obligation to ensure that the software or information technology becomes compliant or provide notice to the State that the software or information technology becomes compliant or provide notice to the State that the software or information technology cannot be made compliant and why.
 - 3.5. Third party products resold under this Contract shall also be governed by the negotiated electronic license, subscription, maintenance, support or similar agreement between the State and the third-party publisher or supplier. Supplier agrees that all such agreements will pass to any applicable Acquisition placed by the State or Customer hereunder. Any other third-party product terms and conditions or clauses in an electronic license, subscription, maintenance, support or similar agreement shall be binding only upon the State's acceptance of those additional terms.


Attachments referenced in this section are attached hereto and incorporated herein.

4. Any reference to a Contract Document refers to such Contract Document as it may have been amended. If and to the extent any provision is in multiple documents and addresses the same or substantially the same subject matter but does not create an actual conflict, the more recent provision is deemed to supersede earlier versions.

STATE OF OKLAHOMA
by and through the
OFFICE OF MANAGEMENT AND
ENTERPRISE SERVICES

RATTAN CONSULTING, INC.

By: 
Joe McIntosh (Dec 13, 2023 16:37 CST)
Name: Joe McIntosh
Title: CIO
Date: Dec 13, 2023

By: 
Name: Travis Rattan
Title: President
Date: Dec 13, 2023

ATTACHMENT A
SOLICITATION NO. 0900000556

This Solicitation is a Contract Document and is a request for proposal in connection with the Contract awarded by the Office of Management and Enterprise Services as more particularly described below. Any defined term used herein but not defined herein shall have the meaning ascribed in the General Terms or other Contract Document.

PURPOSE

The Contract is awarded as a statewide contract on behalf of the Office of Management and Enterprise Services for software and services to support State agencies and other eligible Oklahoma Interlocal Entities. This Supplier will provide software, training, pre-sales assistance, documentation, installation, maintenance, support, configuration, customization, and license agreement administration.

1. Contract Term and Renewal Options

The initial Contract term, which begins on the effective date of the Contract, is one year and there are [4] one-year options to renew the Contract.

ATTACHMENT B

STATE OF OKLAHOMA GENERAL TERMS

This State of Oklahoma General Terms (“General Terms”) is a Contract Document in connection with a Contract awarded by the Office of Management and Enterprise Services on behalf of the State of Oklahoma.

In addition to other terms contained in an applicable Contract Document, Supplier and State agree to the following General Terms:

1 Scope and Contract Renewal

- 1.1** Supplier may not add products or services to its offerings under the Contract without the State’s prior written approval. Such request may require a competitive bid of the additional products or services. If the need arises for goods or services outside the scope of the Contract, Supplier shall contact the State.
- 1.2** At no time during the performance of the Contract shall the Supplier have the authority to obligate any Customer for payment for any products or services (a) when a corresponding encumbering document is not signed or (b) over and above an awarded Contract amount. Likewise, Supplier is not entitled to compensation for a product or service provided by or on behalf of Supplier that is neither requested nor accepted as satisfactory.
- 1.3** If applicable, prior to any Contract renewal, the State shall subjectively consider the value of the Contract to the State, the Supplier’s performance under the Contract, and shall review certain other factors, including but not limited to the: a) terms and conditions of Contract Documents to determine validity with current State and other applicable statutes and rules; b) current pricing and discounts offered by Supplier; and c) current products, services and support offered by Supplier. If the State determines changes to the Contract are required as a condition precedent to renewal, the State and Supplier will cooperate in good faith to evidence such required changes in an Addendum. Further, any request for a price increase in connection with a renewal or otherwise will be conditioned on the Supplier providing appropriate documentation supporting the request.
- 1.4** The State may extend the Contract for ninety (90) days beyond a final renewal term at the Contract compensation rate for the extended period. If the State

exercises such option to extend ninety (90) days, the State shall notify the Supplier in writing prior to Contract end date. The State, at its sole option and to the extent allowable by law, may choose to exercise subsequent ninety (90) day extensions at the Contract pricing rate, to facilitate the finalization of related terms and conditions of a new award or as needed for transition to a new Supplier.

- 1.5** Supplier understands that supplier registration expires annually and, pursuant to OAC 260:115-3-3, Supplier shall maintain its supplier registration with the State as a precondition to a renewal of the Contract.

2 Contract Effectiveness and Order of Priority

- 2.1** Unless specifically agreed in writing otherwise, the Contract is effective upon the date last signed by the parties. Supplier shall not commence work, commit funds, incur costs, or in any way act to obligate the State until the Contract is effective.

- 2.2** Contract Documents shall be read to be consistent and complementary. Any conflict among the Contract Documents shall be resolved by giving priority to Contract Documents in the following order of precedence:

- A.** any Addendum;
- B.** any applicable Solicitation;
- C.** any Contract-specific State terms contained in a Contract Document including, without limitation, information technology terms and terms specific to a statewide Contract or a State agency Contract;
- D.** the terms contained in this Contract Document;
- E.** any successful Bid as may be amended through negotiation and to the extent the Bid does not otherwise conflict with the Solicitation or applicable law;
- F.** any statement of work, work order, or other similar ordering document as applicable; and
- G.** other mutually agreed Contract Documents.

- 2.3** If there is a conflict between the terms contained in this Contract Document or in Contract-specific terms and an agreement provided by or on behalf of Supplier including but not limited to linked or supplemental documents which alter or diminish the rights of Customer or the State, the conflicting terms

provided by Supplier shall not take priority over this Contract Document or Acquisition-specific terms. In no event will any linked document alter or override such referenced terms except as specifically agreed in an Addendum.

- 2.4 Any Contract Document shall be legibly written in ink or typed. All Contract transactions, and any Contract Document related thereto, may be conducted by electronic means pursuant to the Oklahoma Uniform Electronic Transactions Act.

3 **Modification of Contract Terms and Contract Documents**

- 3.1 The Contract may only be modified, amended, or expanded by an Addendum. Any change to the Contract, including the addition of work or materials, the revision of payment terms, or the substitution of work or materials made unilaterally by the Supplier, is a material breach of the Contract. Unless otherwise specified by applicable law or rules, such changes, including without limitation, any unauthorized written Contract modification, shall be void and without effect and the Supplier shall not be entitled to any claim under the Contract based on those changes. No oral statement of any person shall modify or otherwise affect the terms, conditions, or specifications stated in the Contract.
- 3.2 Any additional terms on an ordering document provided by Supplier are of no effect and are void unless mutually executed. OMES bears no liability for performance, payment or failure thereof by the Supplier or by a Customer other than OMES in connection with an Acquisition.

4 **Definitions**

In addition to any defined terms set forth elsewhere in the Contract, the Oklahoma Central Purchasing Act and the Oklahoma Administrative Code, Title 260, the parties agree that, when used in the Contract, the following terms are defined as set forth below and may be used in the singular or plural form:

- 4.1 **Acquisition** means items, products, materials, supplies, services and equipment acquired by purchase, lease purchase, lease with option to purchase, value provided or rental under the Contract.
- 4.2 **Addendum** means a mutually executed, written modification to a Contract Document.
- 4.3 **Amendment** means a written change, addition, correction or revision to the Solicitation.
- 4.4 **Bid** means an offer a Bidder submits in response to the Solicitation.

- 4.5 **Bidder** means an individual or business entity that submits a Bid in response to the Solicitation.
- 4.6 **Contract** means the written, mutually agreed and binding legal relationship resulting from the Contract Documents and an appropriate encumbering document as may be amended from time to time, which evidences the final agreement between the parties with respect to the subject matter of the Contract.
- 4.7 **Contract Document** means this document; any master or enterprise agreement terms entered into between the parties that are mutually agreed to be applicable to the Contract; any Solicitation; any Contract-specific terms; any Supplier's Bid as may be negotiated; any statement of work, work order, or other similar mutually executed ordering document; other mutually executed documents and any Addendum.
- 4.8 **Customer** means the entity receiving goods or services contemplated by the Contract.
- 4.9 **Debarment** means action taken by a debarring official under federal or state law or regulations to exclude any business entity from inclusion on the Supplier list; bidding; offering to bid; providing a quote; receiving an award of contract with the State and may also result in cancellation of existing contracts with the State.
- 4.10 **Destination** means delivered to the receiving dock or other point specified in the applicable Contract Document.
- 4.11 **Indemnified Parties** means the State and Customer and/or its officers, directors, agents, employees, representatives, contractors, assignees and designees thereof.
- 4.12 **Inspection** means examining and testing an Acquisition (including, when appropriate, raw materials, components, and intermediate assemblies) to determine whether the Acquisition meets Contract requirements.
- 4.13 **Moral Rights** means any and all rights of paternity or integrity of the Work Product and the right to object to any modification, translation or use of the Work Product and any similar rights existing under the judicial or statutory law of any country in the world or under any treaty, regardless of whether or not such right is denominated or referred to as a moral right.
- 4.14 **OAC** means the Oklahoma Administrative Code.
- 4.15 **OMES** means the Office of Management and Enterprise Services.

- 4.16 Solicitation** means the document inviting Bids for the Acquisition referenced in the Contract and any amendments thereto.
- 4.17 State** means the government of the state of Oklahoma, its employees and authorized representatives, including without limitation any department, agency, or other unit of the government of the state of Oklahoma.
- 4.18 Supplier** means the Bidder with whom the State enters into the Contract awarded pursuant to the Solicitation or the business entity or individual that is a party to the Contract with the State.
- 4.19 Suspension** means action taken by a suspending official under federal or state law or regulations to suspend a Supplier from inclusion on the Supplier list; be eligible to submit Bids to State agencies and be awarded a contract by a State agency subject to the Central Purchasing Act.
- 4.20 Supplier Confidential Information** means certain confidential and proprietary information of Supplier that is clearly marked as confidential and agreed by the State Purchasing Director or Customer, as applicable, but does not include information excluded from confidentiality in provisions of the Contract or the Oklahoma Open Records Act.
- 4.21 Work Product** means any and all deliverables produced by Supplier under a statement of work or similar Contract Document issued pursuant to this Contract, including any and all tangible or intangible items or things that have been or will be prepared, created, developed, invented or conceived at any time following the Contract effective date including but not limited to any (i) works of authorship (such as manuals, instructions, printed material, graphics, artwork, images, illustrations, photographs, computer programs, computer software, scripts, object code, source code or other programming code, HTML code, flow charts, notes, outlines, lists, compilations, manuscripts, writings, pictorial materials, schematics, formulae, processes, algorithms, data, information, multimedia files, text web pages or web sites, other written or machine readable expression of such works fixed in any tangible media, and all other copyrightable works), (ii) trademarks, service marks, trade dress, trade names, logos, or other indicia of source or origin, (iii) ideas, designs, concepts, personality rights, methods, processes, techniques, apparatuses, inventions, formulas, discoveries, or improvements, including any patents, trade secrets and know-how, (iv) domain names, (v) any copies, and similar or derivative works to any of the foregoing, (vi) all documentation and materials related to any of the foregoing, (vii) all other goods, services or deliverables to be provided by or on behalf of Supplier under the Contract and (viii) all Intellectual Property Rights in any of the foregoing, and which are or were created,

prepared, developed, invented or conceived for the use of benefit of Customer in connection with this Contract or with funds appropriated by or for Customer or Customer's benefit (a) by any Supplier personnel or Customer personnel or (b) any Customer personnel who then became personnel to Supplier or any of its affiliates or subcontractors, where, although creation or reduction-to-practice is completed while the person is affiliated with Supplier or its personnel, any portion of same was created, invented or conceived by such person while affiliated with Customer.

5 Pricing

- 5.1** Pursuant to 68 O.S. §§ 1352, 1356, and 1404, State agencies are exempt from the assessment of State sales, use, and excise taxes. Further, State agencies and political subdivisions of the State are exempt from Federal Excise Taxes pursuant to Title 26 of the United States Code. Any taxes of any nature whatsoever payable by the Supplier shall not be reimbursed.
- 5.2** Pursuant to 74 O.S. §85.40, all travel expenses of Supplier must be included in the total Acquisition price.
- 5.3** The price of a product offered under the Contract shall include and Supplier shall prepay all shipping, packaging, delivery and handling fees. All product deliveries will be free on board Customer's Destination. No additional fees shall be charged by Supplier for standard shipping and handling. If Customer requests expedited or special delivery, Customer may be responsible for any charges for expedited or special delivery.

6 Ordering, Inspection, and Acceptance

- 6.1** Any product or service furnished under the Contract shall be ordered by issuance of a valid purchase order or other appropriate payment mechanism, including a pre-encumbrance, or by use of a valid Purchase Card. All orders and transactions are governed by the terms and conditions of the Contract. Any purchase order or other applicable payment mechanism dated prior to termination or expiration of the Contract shall be performed unless mutually agreed in writing otherwise.
- 6.2** Services will be performed in accordance with industry best practices and are subject to acceptance by the Customer. Notwithstanding any other provision in the Contract, deemed acceptance of a service or associated deliverable shall not apply automatically upon receipt of a deliverable or upon provision of a service.

Supplier warrants and represents that a product or deliverable furnished by or through the Supplier shall individually, and where specified by Supplier to perform as a system, be substantially uninterrupted and error-free in operation and guaranteed against faulty material and workmanship for a warranty period of the greater of ninety (90) days from the date of acceptance or the maximum allowed by the manufacturer. A defect in a product or deliverable furnished by or through the Supplier shall be repaired or replaced by Supplier at no additional cost or expense to the Customer if such defect occurs during the warranty period.

Any product to be delivered pursuant to the Contract shall be subject to final inspection and acceptance by the Customer at Destination. The Customer assumes no responsibility for a product until accepted by the Customer. Title and risk of loss or damage to a product shall be the responsibility of the Supplier until accepted. The Supplier shall be responsible for filing, processing, and collecting any and all damage claims accruing prior to acceptance.

Pursuant to OAC 260:115-9-5, payment for an Acquisition does not constitute final acceptance of the Acquisition. If subsequent inspection affirms that the Acquisition does not meet or exceed the specifications of the order or that the Acquisition has a latent defect, the Supplier shall be notified as soon as is reasonably practicable. The Supplier shall retrieve and replace the Acquisition at Supplier's expense or, if unable to replace, shall issue a refund to Customer. Refund under this section shall not be an exclusive remedy.

- 6.3 Supplier shall deliver products and services on or before the required date specified in a Contract Document. Failure to deliver timely may result in liquidated damages as set forth in the applicable Contract Document. Deviations, substitutions, or changes in a product or service, including changes of personnel directly providing services, shall not be made unless expressly authorized in writing by the Customer. Any substitution of personnel directly providing services shall be a person of comparable or greater skills, education and experience for performing the services as the person being replaced. Additionally, Supplier shall provide staff sufficiently experienced and able to perform with respect to any transitional services provided by Supplier in connection with termination or expiration of the Contract.
- 6.4 Product warranty and return policies and terms provided under any Contract Document will not be more restrictive or more costly than warranty and return policies and terms for other similarly situated customers for a like product.

7 Invoices and Payment

- 7.1** Supplier shall be paid upon submission of a proper invoice(s) at the prices stipulated in the Contract in accordance with 74 O.S. §85.44B which requires that payment be made only after products have been provided and accepted or services rendered and accepted.

The following terms additionally apply:

- A.** An invoice shall contain the purchase order number, description of products or services provided and the dates of such provision.
- B.** Failure to provide a timely and proper invoice may result in delay of processing the invoice for payment. Proper invoice is defined at OAC 260:10-1-2.
- C.** Payment of all fees under the Contract shall be due NET 45 days. Payment and interest on late payments are governed by 62 O.S. §34.72. Such interest is the sole and exclusive remedy for late payments by a State agency and no other late fees are authorized to be assessed pursuant to Oklahoma law.
- D.** The date from which an applicable early payment discount time is calculated shall be from the receipt date of a proper invoice. There is no obligation, however, to utilize an early payment discount.
- E.** If an overpayment or underpayment has been made to Supplier any subsequent payments to Supplier under the Contract may be adjusted to correct the account. A written explanation of the adjustment will be issued to Supplier.
- F.** Supplier shall have no right of setoff.
- G.** Because funds are typically dedicated to a particular fiscal year, an invoice will be paid only when timely submitted, which shall in no instance be later than six (6) months after the end of the fiscal year in which the goods are provided or services performed.
- H.** The Supplier shall accept payment by Purchase Card as allowed by Oklahoma law.

8 Maintenance of Insurance, Payment of Taxes, and Workers' Compensation

- 8.1** As a condition of this Contract, Supplier shall procure at its own expense, and provide proof of, insurance coverage with the applicable liability limits set

forth below and any approved subcontractor of Supplier shall procure and provide proof of the same coverage. The required insurance shall be underwritten by an insurance carrier with an A.M. Best rating of A- or better.

Such proof of coverage shall additionally be provided to the Customer if services will be provided by any of Supplier's employees, agents or subcontractors at any Customer premises and/or employer vehicles will be used in connection with performance of Supplier's obligations under the Contract. Supplier may not commence performance hereunder until such proof has been provided. Additionally, Supplier shall ensure each insurance policy includes a thirty (30) day notice of cancellation and name the State and its agencies as certificate holder and shall promptly provide proof to the State of any renewals, additions, or changes to such insurance coverage. Supplier's obligation to maintain insurance coverage under the Contract is a continuing obligation until Supplier has no further obligation under the Contract. Any combination of primary and excess or umbrella insurance may be used to satisfy the limits of coverage for Commercial General Liability, Auto Liability and Employers' Liability. Unless agreed between the parties and approved by the State Purchasing Director, the minimum acceptable insurance limits of liability are as follows:

- A.** Workers' Compensation and Employer's Liability Insurance in accordance with and to the extent required by applicable law;
- B.** Commercial General Liability Insurance covering the risks of personal injury, bodily injury (including death) and property damage, including coverage for contractual liability, with a limit of liability of not less than \$5,000,000 per occurrence;
- C.** Automobile Liability Insurance with limits of liability of not less than \$5,000,000 combined single limit each accident;
- D.** Directors and Officers Insurance which shall include Employment Practices Liability as well as Consultant's Computer Errors and Omissions Coverage, if information technology services are provided under the Contract, with limits not less than \$5,000,000 per occurrence;
- E.** Security and Privacy Liability insurance, including coverage for failure to protect confidential information and failure of the security of Supplier's computer systems that results in unauthorized access to Customer data with limits \$5,000,000 per occurrence; and
- F.** Additional coverage required in writing in connection with a particular Acquisition.

- 8.2** Supplier shall be entirely responsible during the existence of the Contract for the liability and payment of taxes payable by or assessed to Supplier or its employees, agents and subcontractors of whatever kind, in connection with the Contract. Supplier further agrees to comply with all state and federal laws applicable to any such persons, including laws regarding wages, taxes, insurance, and Workers' Compensation. Neither Customer nor the State shall be liable to the Supplier, its employees, agents, or others for the payment of taxes or the provision of unemployment insurance and/or Workers' Compensation or any benefit available to a State or Customer employee.
- 8.3** Supplier agrees to indemnify Customer, the State, and its employees, agents, representatives, contractors, and assignees for any and all liability, actions, claims, demands, or suits, and all related costs and expenses (including without limitation reasonable attorneys' fees and costs required to establish the right to indemnification) relating to tax liability, unemployment insurance and/or Workers' Compensation in connection with its performance under the Contract.

9 Compliance with Applicable Laws

- 9.1** As long as Supplier has an obligation under the terms of the Contract and in connection with performance of its obligations, the Supplier represents its present compliance, and shall have an ongoing obligation to comply, with all applicable federal, State, and local laws, rules, regulations, ordinances, and orders, as amended, including but not limited to the following:
- A.** Drug-Free Workplace Act of 1988 set forth at 41 U.S.C. §81.
 - B.** Section 306 of the Clean Air Act, Section 508 of the Clean Water Act, Executive Order 11738, and Environmental Protection Agency Regulations which prohibit the use of facilities included on the EPA List of Violating Facilities under nonexempt federal contracts, grants or loans;
 - C.** Prospective participant requirements set at 45 C.F.R. part 76 in connection with Debarment, Suspension and other responsibility matters;
 - D.** 1964 Civil Rights Act, Title IX of the Education Amendment of 1972, Section 504 of the Rehabilitation Act of 1973, Americans with Disabilities Act of 1990, and Executive Orders 11246 and 11375;
 - E.** Anti-Lobbying Law set forth at 31 U.S.C. §1325 and as implemented at 45 C.F.R. part 93;

- F.** Requirements of Internal Revenue Service Publication 1075 regarding use, access and disclosure of Federal Tax Information (as defined therein);
 - G.** Obtaining certified independent audits conducted in accordance with Government Auditing Standards and Office of Management and Budget Uniform Guidance, 2 CFR 200 Subpart F §200.500 et seq. with approval and work paper examination rights of the applicable procuring entity;
 - H.** Requirements of the Oklahoma Taxpayer and Citizen Protection Act of 2007, 25 O.S. §1312 and applicable federal immigration laws and regulations and be registered and participate in the Status Verification System. The Status Verification System is defined at 25 O.S. §1312, includes but is not limited to the free Employment Verification Program (E-Verify) through the Department of Homeland Security, and is available at www.dhs.gov/E-Verify;
 - I.** Requirements of the Health Insurance Portability and Accountability Act of 1996; Health Information Technology for Economic and Clinical Health Act; Payment Card Industry Security Standards; Criminal Justice Information System Security Policy and Security Addendum; and Family Educational Rights and Privacy Act; and
 - J.** Be registered as a business entity licensed to do business in the State, have obtained a sales tax permit, and be current on franchise tax payments to the State, as applicable.
- 9.2** The Supplier's employees, agents and subcontractors shall adhere to applicable Customer policies including, but not limited to acceptable use of Internet and electronic mail, facility and data security, press releases, and public relations. As applicable, the Supplier shall adhere to the State Information Security Policy, Procedures, Guidelines set forth at https://omes.ok.gov/sites/g/files/gmc316/f/InfoSecPPG_0.pdf. Supplier is responsible for reviewing and relaying such policies covering the above to the Supplier's employees, agents and subcontractors.
- 9.3** At no additional cost to Customer, the Supplier shall maintain all applicable licenses and permits required in association with its obligations under the Contract.
- 9.4** In addition to compliance under subsection 9.1 above, Supplier shall have a continuing obligation to comply with applicable Customer-specific mandatory

contract provisions required in connection with the receipt of federal funds or other funding source.

- 9.5** The Supplier is responsible to review and inform its employees, agents, and subcontractors who provide a product or perform a service under the Contract of the Supplier's obligations under the Contract and Supplier certifies that its employees and each such subcontractor shall comply with minimum requirements and applicable provisions of the Contract. At the request of the State, Supplier shall promptly provide adequate evidence that such persons are its employees, agents or approved subcontractors and have been informed of their obligations under the Contract.
- 9.6** As applicable, Supplier agrees to comply with the Governor's Executive Orders related to the use of any tobacco product, electronic cigarette or vaping device on any and all properties owned, leased, or contracted for use by the State, including but not limited to all buildings, land and vehicles owned, leased, or contracted for use by agencies or instrumentalities of the State.
- 9.7** The execution, delivery and performance of the Contract and any ancillary documents by Supplier will not, to the best of Supplier's knowledge, violate, conflict with, or result in a breach of any provision of, or constitute a default (or an event which, with notice or lapse of time or both, would constitute a default) under, or result in the termination of, any written contract or other instrument between Supplier and any third party.
- 9.8** Supplier represents that it has the ability to pay its debts when due and it does not anticipate the filing of a voluntary or involuntary bankruptcy petition or appointment of a receiver, liquidator or trustee.
- 9.9** Supplier represents that, to the best of its knowledge, any litigation or claim or any threat thereof involving Supplier has been disclosed in writing to the State and Supplier is not aware of any other litigation, claim or threat thereof.
- 9.10** If services provided by Supplier include delivery of an electronic communication, Supplier shall ensure such communication and any associated support documents are compliant with Section 508 of the Federal Rehabilitation Act and with State standards regarding accessibility. Should any communication or associated support documents be non-compliant, Supplier shall correct and re-deliver such communication immediately upon discovery or notice, at no additional cost to the State. Additionally, as part of compliance with accessibility requirements where documents are only provided in non-electronic format, Supplier shall promptly provide such communication and any associated support documents in an alternate format

usable by individuals with disabilities upon request and at no additional cost, which may originate from an intended recipient or from the State.

10 Audits and Records Clause

- 10.1** As used in this clause and pursuant to 67 O.S. §203, “record” includes a document, book, paper, photograph, microfilm, computer tape, disk, record, sound recording, film recording, video record, accounting procedures and practices, and other data, regardless of type and regardless of whether such items are in written form, in the form of computer data, or in any other form. Supplier agrees any pertinent federal or State agency or governing entity of a Customer shall have the right to examine and audit, at no additional cost to a Customer, all records relevant to the execution and performance of the Contract except, unless otherwise agreed, costs of Supplier that comprise pricing under the Contract.
- 10.2** The Supplier is required to retain records relative to the Contract for the duration of the Contract and for a period of seven (7) years following completion or termination of an Acquisition unless otherwise indicated in the Contract terms. If a claim, audit, litigation or other action involving such records is started before the end of the seven-year period, the records are required to be maintained for two (2) years from the date that all issues arising out of the action are resolved, or until the end of the seven (7) year retention period, whichever is later.
- 10.3** Pursuant to 74 O.S. §85.41, if professional services are provided hereunder, all items of the Supplier that relate to the professional services are subject to examination by the State agency, State Auditor and Inspector and the State Purchasing Director.

11 Confidentiality

- 11.1** The Supplier shall maintain strict security of all State and citizen data and records entrusted to it or to which the Supplier gains access, in accordance with and subject to applicable federal and State laws, rules, regulations, and policies and shall use any such data and records only as necessary for Supplier to perform its obligations under the Contract. The Supplier further agrees to evidence such confidentiality obligation in a separate writing if required under such applicable federal or State laws, rules and regulations. The Supplier warrants and represents that such information shall not be sold, assigned, conveyed, provided, released, disseminated or otherwise disclosed by Supplier, its employees, officers, directors, subsidiaries, affiliates, agents, representatives, assigns, subcontractors, independent contractors, successor or any other persons or entities without Customer’s prior express written

permission. Supplier shall instruct all such persons and entities that the confidential information shall not be disclosed or used without the Customer's prior express written approval except as necessary for Supplier to render services under the Contract. The Supplier further warrants that it has a tested and proven system in effect designed to protect all confidential information.

- 11.2** Supplier shall establish, maintain and enforce agreements with all such persons and entities that have access to State and citizen data and records to fulfill Supplier's duties and obligations under the Contract and to specifically prohibit any sale, assignment, conveyance, provision, release, dissemination or other disclosure of any State or citizen data or records except as required by law or allowed by written prior approval of the Customer.
- 11.3** Supplier shall immediately report to the Customer any and all unauthorized use, appropriation, sale, assignment, conveyance, provision, release, access, acquisition, disclosure or other dissemination of any State or citizen data or records of which it or its parent company, subsidiaries, affiliates, employees, officers, directors, assignees, agents, representatives, independent contractors, and subcontractors is aware or have knowledge or reasonable should have knowledge. The Supplier shall also promptly furnish to Customer full details of the unauthorized use, appropriation, sale, assignment, conveyance, provision, release, access, acquisition, disclosure or other dissemination, or attempt thereof, and use its best efforts to assist the Customer in investigating or preventing the reoccurrence of such event in the future. The Supplier shall cooperate with the Customer in connection with any litigation and investigation deemed necessary by the Customer to protect any State or citizen data and records and shall bear all costs associated with the investigation, response and recovery in connection with any breach of State or citizen data or records including but not limited to credit monitoring services with a term of at least three (3) years, all notice-related costs and toll free telephone call center services.
- 11.4** Supplier further agrees to promptly prevent a reoccurrence of any unauthorized use, appropriation, sale, assignment, conveyance, provision, release, access, acquisition, disclosure or other dissemination of State or citizen data and records.
- 11.5** Supplier acknowledges that any improper use, appropriation, sale, assignment, conveyance, provision, release, access, acquisition, disclosure or other dissemination of any State data or records to others may cause immediate and irreparable harm to the Customer and certain beneficiaries and may violate state or federal laws and regulations. If the Supplier or its affiliates, parent company, subsidiaries, employees, officers, directors, assignees, agents,

representatives, independent contractors, and subcontractors improperly use, appropriate, sell, assign, convey, provide, release, access, acquire, disclose or otherwise disseminate such confidential information to any person or entity in violation of the Contract, the Customer will immediately be entitled to injunctive relief and/or any other rights or remedies available under this Contract, at equity or pursuant to applicable statutory, regulatory, and common law without a cure period.

11.6 The Supplier shall immediately forward to the State Purchasing Director, and any other applicable person listed in the Notices section(s) of the Contract, any request by a third party for data or records in the possession of the Supplier or any subcontractor or to which the Supplier or subcontractor has access and Supplier shall fully cooperate with all efforts to protect the security and confidentiality of such data or records in response to a third party request.

11.7 Customer may be provided access to Supplier Confidential Information. State agencies are subject to the Oklahoma Open Records Act and Supplier acknowledges information marked confidential information will be disclosed to the extent permitted under the Open Records Act and in accordance with this section. Nothing herein is intended to waive the State Purchasing Director's authority under OAC 260:115-3-9 in connection with Bid information requested to be held confidential by a Bidder. Notwithstanding the foregoing, Supplier Confidential Information shall not include information that: (i) is or becomes generally known or available by public disclosure, commercial use or otherwise and is not in contravention of this Contract; (ii) is known and has been reduced to tangible form by the receiving party before the time of disclosure for the first time under this Contract and without other obligations of confidentiality; (iii) is independently developed without the use of any of Supplier Confidential Information; (iv) is lawfully obtained from a third party (without any confidentiality obligation) who has the right to make such disclosure or (v) résumé, pricing or marketing materials provided to the State. In addition, the obligations in this section shall not apply to the extent that the applicable law or regulation requires disclosure of Supplier Confidential Information, provided that the Customer provides reasonable written notice, pursuant to Contract notice provisions, to the Supplier so that the Supplier may promptly seek a protective order or other appropriate remedy.

12 Conflict of Interest

In addition to any requirement of law or of a professional code of ethics or conduct, the Supplier, its employees, agents and subcontractors are required to disclose any outside activity or interest that conflicts or may conflict with the best interest of the State. Prompt disclosure is required under this section if the activity or interest is

related, directly or indirectly, to any person or entity currently under contract with or seeking to do business with the State, its employees or any other third-party individual or entity awarded a contract with the State. Further, as long as the Supplier has an obligation under the Contract, any plan, preparation or engagement in any such activity or interest shall not occur without prior written approval of the State. Any conflict of interest shall, at the sole discretion of the State, be grounds for partial or whole termination of the Contract.

13 Assignment and Permitted Subcontractors

- 13.1** Supplier's obligations under the Contract may not be assigned or transferred to any other person or entity without the prior written consent of the State which may be withheld at the State's sole discretion. Should Supplier assign its rights to payment, in whole or in part, under the Contract, Supplier shall provide the State and all affected Customers with written notice of the assignment. Such written notice shall be delivered timely and contain details sufficient for affected Customers to perform payment obligations without any delay caused by the assignment.
- 13.2** Notwithstanding the foregoing, the Contract may be assigned by Supplier to any corporation or other entity in connection with a merger, consolidation, sale of all equity interests of the Supplier, or a sale of all or substantially all of the assets of the Supplier to which the Contract relates. In any such case, said corporation or other entity shall by operation of law or expressly in writing assume all obligations of the Supplier as fully as if it had been originally made a party to the Contract. Supplier shall give the State and all affected Customers prior written notice of said assignment. Any assignment or delegation in violation of this subsection shall be void.
- 13.3** If the Supplier is permitted to utilize subcontractors in support of the Contract, the Supplier shall remain solely responsible for its obligations under the terms of the Contract, for its actions and omissions and those of its agents, employees and subcontractors and for payments to such persons or entities. Prior to a subcontractor being utilized by the Supplier, the Supplier shall obtain written approval of the State of such subcontractor and each employee, as applicable to a particular Acquisition, of such subcontractor proposed for use by the Supplier. Such approval is within the sole discretion of the State. Any proposed subcontractor shall be identified by entity name, and by employee name, if required by the particular Acquisition, in the applicable proposal and shall include the nature of the services to be performed. As part of the approval request, the Supplier shall provide a copy of a written agreement executed by the Supplier and subcontractor setting forth that such subcontractor is bound by and agrees, as applicable, to perform the same covenants and be subject to

the same conditions and make identical certifications to the same facts and criteria, as the Supplier under the terms of all applicable Contract Documents. Supplier agrees that maintaining such agreement with any subcontractor and obtaining prior written approval by the State of any subcontractor and associated employees shall be a continuing obligation. The State further reserves the right to revoke approval of a subcontractor or an employee thereof in instances of poor performance, misconduct or for other similar reasons.

13.4 All payments under the Contract shall be made directly to the Supplier, except as provided in subsection A above regarding the Supplier's assignment of payment. No payment shall be made to the Supplier for performance by unapproved or disapproved employees of the Supplier or a subcontractor.

13.5 Rights and obligations of the State or a Customer under the terms of this Contract may be assigned or transferred, at no additional cost, to other Customer entities.

14 Background Checks and Criminal History Investigations

Prior to the commencement of any services, background checks and criminal history investigations of the Supplier's employees and subcontractors who will be providing services may be required and, if so, the required information shall be provided to the State in a timely manner. Supplier's access to facilities, data and information may be withheld prior to completion of background verification acceptable to the State. The costs of additional background checks beyond Supplier's normal hiring practices shall be the responsibility of the Customer unless such additional background checks are required solely because Supplier will not provide results of its otherwise acceptable normal background checks; in such an instance, Supplier shall pay for the additional background checks. Supplier will coordinate with the State and its employees to complete the necessary background checks and criminal history investigations. Should any employee or subcontractor of the Supplier who will be providing services under the Contract not be acceptable as a result of the background check or criminal history investigation, the Customer may require replacement of the employee or subcontractor in question and, if no suitable replacement is made within a reasonable time, terminate the purchase order or other payment mechanism associated with the project or services.

15 Patents and Copyrights

Without exception, a product or deliverable price shall include all royalties or costs owed by the Supplier to any third party arising from the use of a patent, intellectual property, copyright or other property right held by such third party. Should any third party threaten or make a claim that any portion of a product or service provided by Supplier under the Contract infringes that party's patent, intellectual property,

copyright or other property right, Supplier shall enable each affected Customer to legally continue to use, or modify for use, the portion of the product or service at issue or replace such potentially infringing product, or re-perform or redeliver in the case of a service, with at least a functional non-infringing equivalent. Supplier's duty under this section shall extend to include any other product or service rendered materially unusable as intended due to replacement or modification of the product or service at issue. If the Supplier determines that none of these alternatives are reasonably available, the State shall return such portion of the product or deliverable at issue to the Supplier, upon written request, in exchange for a refund of the price paid for such returned goods as well as a refund or reimbursement, if applicable, of the cost of any other product or deliverable rendered materially unusable as intended due to removal of the portion of product or deliverable at issue. Any remedy provided under this section is not an exclusive remedy and is not intended to operate as a waiver of legal or equitable remedies because of acceptance of relief provided by Supplier.

16 Indemnification

16.1 Acts or Omissions

- A.** Supplier shall defend and indemnify the Indemnified Parties, as applicable, for any and all liability, claims, damages, losses, costs, expenses, demands, suits and actions of third parties (including without limitation reasonable attorneys' fees and costs required to establish the right to indemnification) arising out of, or resulting from any action or claim for bodily injury, death, or property damage brought against any of the Indemnified parties to the extent arising from any negligent act or omission or willful misconduct of the Supplier or its agents, employees, or subcontractors in the execution or performance of the Contract.
- B.** To the extent Supplier is found liable for loss, damage, or destruction of any property of Customer due to negligence, misconduct, wrongful act, or omission on the part of the Supplier, its employees, agents, representatives, or subcontractors, the Supplier and Customer shall use best efforts to mutually negotiate an equitable settlement amount to repair or replace the property unless such loss, damage or destruction is of such a magnitude that repair or replacement is not a reasonable option. Such amount shall be invoiced to, and is payable by, Supplier sixty (60) calendar days after the date of Supplier's receipt of an invoice for the negotiated settlement amount.

16.2 Infringement

Supplier shall indemnify the Indemnified Parties, as applicable, for all liability, claims, damages, losses, costs, expenses, demands, suits and actions of third parties (including without limitation reasonable attorneys' fees and costs required to establish the right to indemnification) arising from or in connection with Supplier's breach of its representations and warranties in the Contract or alleged infringement of any patent, intellectual property, copyright or other property right in connection with a product or service provided under the Contract. Supplier's duty under this section is reduced to the extent a claimed infringement results from: (a) a Customer's or user's content; (b) modifications by Customer or third party to a product delivered under the Contract or combinations of the product with any non-Supplier-provided services or products unless Supplier recommended or participated in such modification or combination; (c) use of a product or service by Customer in violation of the Contract unless done so at the direction of Supplier, or (d) a non-Supplier product that has not been provided to the State by, through or on behalf of Supplier as opposed to its combination with products Supplier provides to or develops for the State or a Customer as a system.

16.3 Notice and Cooperation

In connection with indemnification obligations under the Contract, the parties agree to furnish prompt written notice to each other of any third-party claim. Any Customer affected by the claim will reasonably cooperate with Supplier and defense of the claim to the extent its interests are aligned with Supplier. Supplier shall use counsel reasonably experienced in the subject matter at issue and will not settle a claim without the written consent of the party being defended, which consent will not be unreasonably withheld or delayed, except that no consent will be required to settle a claim against Indemnified Parties that are not a State agency, where relief against the Indemnified Parties is limited to monetary damages that are paid by the defending party under indemnification provisions of the Contract.

16.4 Coordination of Defense

In connection with indemnification obligations under the Contract, when a State agency is a named defendant in any filed or threatened lawsuit, the defense of the State agency shall be coordinated by the Attorney General of Oklahoma, or the Attorney General may authorize the Supplier to control the defense and any related settlement negotiations; provided, however, Supplier shall not agree to any settlement of claims against the State without obtaining advance written concurrence from the Attorney General. If the Attorney General does not authorize sole control of the defense and settlement negotiations to Supplier, Supplier shall have authorization to equally

participate in any proceeding related to the indemnity obligation under the Contract and shall remain responsible to indemnify the applicable Indemnified Parties.

16.5 Limitation of Liability

- A.** With respect to any claim or cause of action arising under or related to the Contract, neither the State nor any Customer shall be liable to Supplier for lost profits, lost sales or business expenditures, investments, or commitments in connection with any business, loss of any goodwill, or for any other indirect, incidental, punitive, special or consequential damages, even if advised of the possibility of such damages.
- B.** Notwithstanding anything to the contrary in the Contract, no provision shall limit damages, expenses, costs, actions, claims, and liabilities arising from or related to property damage, bodily injury or death caused by Supplier or its employees, agents or subcontractors; indemnity, security or confidentiality obligations under the Contract; the bad faith, negligence, intentional misconduct or other acts for which applicable law does not allow exemption from liability of Supplier or its employees, agents or subcontractors.
- C.** The limitation of liability and disclaimers set forth in the Contract will apply regardless of whether Customer has accepted a product or service. The parties agree that Supplier has set its fees and entered into the Contract in reliance on the disclaimers and limitations set forth herein, that the same reflect an allocation of risk between the parties and form an essential basis of the bargain between the parties. These limitations shall apply notwithstanding any failure of essential purpose of any limited remedy.

17 Termination for Funding Insufficiency

- 17.1** Notwithstanding anything to the contrary in any Contract Document, the State may terminate the Contract in whole or in part if funds sufficient to pay obligations under the Contract are not appropriated or received from an intended third-party funding source. In the event of such insufficiency, Supplier will be provided at least fifteen (15) calendar days' written notice of termination. Any partial termination of the Contract under this section shall not be construed as a waiver of, and shall not affect, the rights and obligations of any party regarding portions of the Contract that are not terminated. The determination by the State of insufficient funding shall be accepted by, and shall be final and binding on, the Supplier.

- 17.2** Upon receipt of notice of a termination, Supplier shall immediately comply with the notice terms and take all necessary steps to minimize the incurrence of costs allocable to the work affected by the notice. If a purchase order or other payment mechanism has been issued and a product or service has been accepted as satisfactory prior to the effective date of termination, the termination does not relieve an obligation to pay for the product or service but there shall not be any liability for further payments ordinarily due under the Contract or for any damages or other amounts caused by or associated with such termination. Any amount paid to Supplier in the form of prepaid fees that are unused when the Contractor certain obligations are terminated shall be refunded.
- 17.3** The State's exercise of its right to terminate the Contract under this section shall not be considered a default or breach under the Contract or relieve the Supplier of any liability for claims arising under the Contract.

18 Termination for Cause

- 18.1** Supplier may terminate the Contract if (i) it has provided the State with written notice of material breach and (ii) the State fails to cure such material breach within thirty (30) days of receipt of written notice. If there is more than one Customer, material breach by a Customer does not give rise to a claim of material breach as grounds for termination by Supplier of the Contract as a whole. The State may terminate the Contract in whole or in part if (i) it has provided Supplier with written notice of material breach, and (ii) Supplier fails to cure such material breach within thirty (30) days of receipt of written notice. Any partial termination of the Contract under this section shall not be construed as a waiver of, and shall not affect, the rights and obligations of any party regarding portions of the Contract that are not terminated.
- 18.2** The State may terminate the Contract in whole or in part immediately without a thirty (30) day written notice to Supplier if (i) Supplier fails to comply with confidentiality, privacy, security, environmental or safety requirements applicable to Supplier's performance or obligations under the Contract; (ii) Supplier's material breach is reasonably determined to be an impediment to the function of the State and detrimental to the State or to cause a condition precluding the thirty (30) day notice or (iii) when the State determines that an administrative error in connection with award of the Contract occurred prior to Contract performance.
- 18.3** Upon receipt of notice of a termination, Supplier shall immediately comply with the notice terms and take all necessary steps to minimize the incurrence

of costs allocable to the work affected by the notice. If a purchase order or other payment mechanism has been issued and a product or service has been accepted as satisfactory prior to the effective date of termination, the termination does not relieve an obligation to pay for the product or service but there shall not be any liability for further payments ordinarily due under the Contract or for any damages or other amounts caused by or associated with such termination. Such termination is not an exclusive remedy but is in addition to any other rights and remedies provided for by law. Any amount paid to Supplier in the form of prepaid fees that are unused when the Contract or certain obligations are terminated shall be refunded. Termination of the Contract under this section, in whole or in part, shall not relieve the Supplier of liability for claims arising under the Contract.

- 18.4** The Supplier's repeated failure to provide an acceptable product or service; Supplier's unilateral revision of linked or supplemental terms that have a materially adverse impact on a Customer's rights or obligations under the Contract (except as required by a governmental authority); actual or anticipated failure of Supplier to perform its obligations under the Contract; Supplier's inability to pay its debts when due; assignment for the benefit of Supplier's creditors; or voluntary or involuntary appointment of a receiver or filing of bankruptcy of Supplier shall constitute a material breach of the Supplier's obligations, which may result in partial or whole termination of the Contract. This subsection is not intended as an exhaustive list of material breach conditions. Termination may also result from other instances of failure to adhere to the Contract provisions and for other reasons provided for by applicable law, rules or regulations; without limitation, OAC 260:115-9-9 is an example.

19 Termination for Convenience

- 19.1** The State may terminate the Contract, in whole or in part, for convenience if it is determined that termination is in the State's best interest. In the event of a termination for convenience, Supplier will be provided at least thirty (30) days' written notice of termination. Any partial termination of the Contract shall not be construed as a waiver of, and shall not affect, the rights and obligations of any party regarding portions of the Contract that remain in effect.
- 19.2** Upon receipt of notice of such termination, Supplier shall immediately comply with the notice terms and take all necessary steps to minimize the incurrence of costs allocable to the work affected by the notice. If a purchase order or other payment mechanism has been issued and a product or service has been accepted as satisfactory prior to the effective date of termination, the termination does not relieve an obligation to pay for the product or service but

there shall not be any liability for further payments ordinarily due under the Contract or for any damages or other amounts caused by or associated with such termination. Such termination shall not be an exclusive remedy but shall be in addition to any other rights and remedies provided for by law. Any amount paid to Supplier in the form of prepaid fees that are unused when the Contract or certain obligations are terminated shall be refunded. Termination of the Contract under this section, in whole or in part, shall not relieve the Supplier of liability for claims arising under the Contract.

20 Suspension of Supplier

- 20.1** Supplier may be subject to Suspension without advance notice and may additionally be suspended from activities under the Contract if Supplier fails to comply with confidentiality, privacy, security, environmental or safety requirements applicable to Supplier's performance or obligations under the Contract.
- 20.2** Upon receipt of a notice pursuant to this section, Supplier shall immediately comply with the notice terms and take all necessary steps to minimize the incurrence of costs allocable to the work affected by the notice. If a purchase order or other payment mechanism has been issued and a product or service has been accepted as satisfactory prior to receipt of notice by Supplier, the Suspension does not relieve an obligation to pay for the product or service but there shall not be any liability for further payments ordinarily due under the Contract during a period of Suspension or suspended activity or for any damages or other amounts caused by or associated with such Suspension or suspended activity. A right exercised under this section shall not be an exclusive remedy but shall be in addition to any other rights and remedies provided for by law. Any amount paid to Supplier in the form of prepaid fees attributable to a period of Suspension or suspended activity shall be refunded.
- 20.3** Such Suspension may be removed, or suspended activity may resume, at the earlier of such time as a formal notice is issued that authorizes the resumption of performance under the Contract or at such time as a purchase order or other appropriate encumbrance document is issued. This subsection is not intended to operate as an affirmative statement that such resumption will occur.

21 Certification Regarding Debarment, Suspension, and Other Responsibility Matters

The certification made by Supplier with respect to Debarment, Suspension, certain indictments, convictions, civil judgments and terminated public contracts is a material representation of fact upon which reliance was placed when entering into the Contract.

A determination that Supplier knowingly rendered an erroneous certification, in addition to other available remedies, may result in whole or partial termination of the Contract for Supplier's default. Additionally, Supplier shall promptly provide written notice to the State Purchasing Director if the certification becomes erroneous due to changed circumstances.

22 Certification Regarding State Employees Prohibition From Fulfilling Services

Pursuant to 74 O.S. § 85.42, the Supplier certifies that no person involved in any manner in development of the Contract employed by the State shall be employed to fulfill any services provided under the Contract.

23 Force Majeure

23.1 Either party shall be temporarily excused from performance to the extent delayed as a result of unforeseen causes beyond its reasonable control including fire or other similar casualty, act of God, strike or labor dispute, war or other violence, or any law, order or requirement of any governmental agency or authority provided the party experiencing the force majeure event has prudently and promptly acted to take any and all steps within the party's control to ensure continued performance and to shorten duration of the event. If a party's performance of its obligations is materially hindered as a result of a force majeure event, such party shall promptly notify the other party of its best reasonable assessment of the nature and duration of the force majeure event and steps it is taking, and plans to take, to mitigate the effects of the force majeure event. The party shall use commercially reasonable best efforts to continue performance to the extent possible during such event and resume full performance as soon as reasonably practicable.

23.2 Subject to the conditions set forth above, non-performance as a result of a force majeure event shall not be deemed a default. However, a purchase order or other payment mechanism may be terminated if Supplier cannot cause delivery of a product or service in a timely manner to meet the business needs of Customer. Supplier is not entitled to payment for products or services not received and, therefore, amounts payable to Supplier during the force majeure event shall be equitably adjusted downward.

23.3 Notwithstanding the foregoing or any other provision in the Contract, (i) the following are not a force majeure event under the Contract: (a) shutdowns, disruptions or malfunctions in Supplier's system or any of Supplier's telecommunication or internet services other than as a result of general and widespread internet or telecommunications failures that are not limited to Supplier's systems or (b) the delay or failure of Supplier or subcontractor personnel to perform any obligation of Supplier hereunder unless such delay

or failure to perform is itself by reason of a force majeure event and (ii) no force majeure event modifies or excuses Supplier's obligations related to confidentiality, indemnification, data security or breach notification obligations set forth herein.

24 Security of Property and Personnel

In connection with Supplier's performance under the Contract, Supplier may have access to Customer personnel, premises, data, records, equipment and other property. Supplier shall use commercially reasonable best efforts to preserve the safety and security of such personnel, premises, data, records, equipment, and other property of Customer. Supplier shall be responsible for damage to such property to the extent such damage is caused by its employees or subcontractors and shall be responsible for loss of Customer property in its possession, regardless of cause. If Supplier fails to comply with Customer's security requirements, Supplier is subject to immediate suspension of work as well as termination of the associated purchase order or other payment mechanism.

25 Notices

All notices, approvals or requests allowed or required by the terms of any Contract Document shall be in writing, reference the Contract with specificity and deemed delivered upon receipt or upon refusal of the intended party to accept receipt of the notice. In addition to other notice requirements in the Contract and the designated Supplier contact provided in a successful Bid, notices shall be sent to the State at the physical address set forth below. Notice information may be updated in writing to the other party as necessary. Notwithstanding any other provision of the Contract, confidentiality, breach and termination-related notices shall not be delivered solely via e-mail.

If sent to the State:

State Purchasing Director
2401 North Lincoln Boulevard, Suite 116
Oklahoma City, Oklahoma 73105

With a copy, which shall not constitute notice, to:

Purchasing Division Deputy General Counsel
2401 North Lincoln Boulevard, Suite 116
Oklahoma City, Oklahoma 73105

26 Miscellaneous

26.1 Choice of Law and Venue

Any claim, dispute, or litigation relating to the Contract Documents, in the singular or in the aggregate, shall be governed by the laws of the State without regard to application of choice of law principles. Pursuant to 74 O.S. §85.14, where federal granted funds are involved, applicable federal laws, rules and regulations shall govern to the extent necessary to insure benefit of such federal funds to the State. Venue for any action, claim, dispute, or litigation relating in any way to the Contract Documents, shall be in Oklahoma County, Oklahoma.

26.2 No Guarantee of Products or Services Required

The State shall not guarantee any minimum or maximum amount of Supplier products or services required under the Contract.

26.3 Employment Relationship

The Contract does not create an employment relationship. Individuals providing products or performing services pursuant to the Contract are not employees of the State or Customer and, accordingly are not eligible for any rights or benefits whatsoever accruing to such employees.

26.4 Transition Services

If transition services are needed at the time of Contract expiration or termination, Supplier shall provide such services on a month-to-month basis, at the contract rate or other mutually agreed rate. Supplier shall provide a proposed transition plan, upon request, and cooperate with any successor supplier and with establishing a mutually agreeable transition plan. Failure to cooperate may be documented as poor performance of Supplier.

26.5 Publicity

The existence of the Contract or any Acquisition is in no way an endorsement of Supplier, the products or services and shall not be so construed by Supplier in any advertising or publicity materials. Supplier agrees to submit to the State all advertising, sales, promotion, and other publicity matters relating to the Contract wherein the name of the State or any Customer is mentioned or language used from which, in the State's judgment, an endorsement may be inferred or implied. Supplier further agrees not to publish or use such advertising, sales promotion, or publicity matter or release any informational pamphlets, notices, press releases, research reports, or similar public notices concerning the Contract or any Acquisition hereunder without obtaining the prior written approval of the State.

26.6 Open Records Act

Supplier acknowledges that all State agencies and certain other Customers are subject to the Oklahoma Open Records Act set forth at 51 O.S. §24A-1 *et seq.* Supplier also acknowledges that compliance with the Oklahoma Open Records Act and all opinions of the Oklahoma Attorney General concerning the Act is required.

26.7 Failure to Enforce

Failure by the State or a Customer at any time to enforce a provision of, or exercise a right under, the Contract shall not be construed as a waiver of any such provision. Such failure to enforce or exercise shall not affect the validity of any Contract Document, or any part thereof, or the right of the State or a Customer to enforce any provision of, or exercise any right under, the Contract at any time in accordance with its terms. Likewise, a waiver of a breach of any provision of a Contract Document shall not affect or waive a subsequent breach of the same provision or a breach of any other provision in the Contract.

26.8 Mutual Responsibilities

- A.** No party to the Contract grants the other the right to use any trademarks, trade names, other designations in any promotion or publication without the express written consent by the other party.
- B.** The Contract is a non-exclusive contract and each party is free to enter into similar agreements with others.
- C.** The Customer and Supplier each grant the other only the licenses and rights specified in the Contract and all other rights and interests are expressly reserved.
- D.** The Customer and Supplier shall reasonably cooperate with each other and any Supplier to which the provision of a product and/or service under the Contract may be transitioned after termination or expiration of the Contract.
- E.** Except as otherwise set forth herein, where approval, acceptance, consent, or similar action by a party is required under the Contract, such action shall not be unreasonably delayed or withheld.

26.9 Invalid Term or Condition

To the extent any term or condition in the Contract conflicts with a compulsory applicable State or United States law or regulation, such Contract term or

condition is void and unenforceable. By executing any Contract Document which contains a conflicting term or condition, no representation or warranty is made regarding the enforceability of such term or condition. Likewise, any applicable State or federal law or regulation which conflicts with the Contract or any non-conflicting applicable State or federal law or regulation is not waived.

26.10 Severability

If any provision of a Contract Document, or the application of any term or condition to any party or circumstances, is held invalid or unenforceable for any reason, the remaining provisions shall continue to be valid and enforceable and the application of such provision to other parties or circumstances shall remain valid and in full force and effect. If a court finds that any provision of this contract is invalid or unenforceable, but that by limiting such provision it would become valid and enforceable, then such provision shall be deemed to be written, construed, and enforced as so limited.

26.11 Section Headings

The headings used in any Contract Document are for convenience only and do not constitute terms of the Contract.

26.12 Sovereign Immunity

Notwithstanding any provision in the Contract, the Contract is entered into subject to the State's Constitution, statutes, common law, regulations, and the doctrine of sovereign immunity, none of which are waived by the State nor any other right or defense available to the State.

26.13 Survival

As applicable, performance under all license, subscription, service agreements, statements of work, transition plans and other similar Contract Documents entered into between the parties under the terms of the Contract shall survive Contract expiration. Additionally, rights and obligations under the Contract which by their nature should survive including, without limitation, certain payment obligations invoiced prior to expiration or termination; confidentiality obligations; security incident and data breach obligations and indemnification obligations, remain in effect after expiration or termination of the Contract.

26.14 Entire Agreement

The Contract Documents taken together as a whole constitute the entire agreement between the parties. No statement, promise, condition,

understanding, inducement or representation, oral or written, expressed or implied, which is not contained in a Contract Document shall be binding or valid. The Supplier's representations and certifications, including any completed electronically, are incorporated by reference into the Contract.

26.15 Gratuities

The Contract may be immediately terminated, in whole or in part, by written notice if it is determined that the Supplier, its employee, agent, or another representative violated any federal, State or local law, rule or ordinance by offering or giving a gratuity to any State employee directly involved in the Contract. In addition, Suspension or Debarment of the Supplier may result from such a violation.

26.16 Import/Export Controls

Neither party will use, distribute, transfer or transmit any equipment, services, software or technical information provided under the Contract (even if incorporated into other products) except in compliance with all applicable import and export laws, conventions and regulations.

ATTACHMENT C

OKLAHOMA STATEWIDE CONTRACT TERMS

1. Statewide Contract Type

- 1.1** The Contract is a non-mandatory statewide contract for use by State agencies. Additionally, the Contract may be used by any governmental entity specified as a political subdivision of the State pursuant to the Governmental Tort Claims Act including any associated institution, instrumentality, board, commission, committee, department or other entity designated to act on behalf of the political subdivision; a state, county or local governmental entity in its state of origin; and entities authorized to utilize contracts by the State via a multistate or multigovernmental contract.
- 1.2** The Contract is a firm, fixed price contract for indefinite delivery and quantity for the Acquisitions available under the Contract.

2. Orders and Addendums

- 2.1** Unless mutually agreed in writing otherwise, orders shall be placed directly with the Supplier by issuance of written purchase orders or by Purchase Card by state agencies and other authorized entities. All orders are subject to the Contract terms and any order dated prior to Contract expiration shall be performed. Delivery to multiple destinations may be required.
- 2.2** Any ordering document shall be effective between Supplier and the Customer only and shall not be an Addendum to the Contract in its entirety or apply to any Acquisition by another Customer.
- 2.3** Additional terms added to a Contract Document by a Customer shall be effective if the additional terms do not conflict with the General Terms and are acceptable to Supplier. However, an Addendum to the Contract shall be signed by the State Purchasing Director or designee. Regarding information technology and telecommunications contracts, pursuant to 62 O.S., §34.11.1, the Chief Information Officer acts as the Information Technology and Telecommunications Purchasing Director.

3. Termination for Funding Insufficiency

In addition to Contract terms relating to termination due to insufficient funding, a Customer may terminate any purchase order or other payment mechanism if funds sufficient to pay obligations under the Contract are not appropriated or received from an intended third-party funding source. The determination by the Customer of insufficient funding shall be accepted by, and shall be final and binding on, the Supplier.

4. Termination for Cause

In addition to Contract terms relating to termination for cause, a customer may terminate its obligations, in whole or in part, to Supplier if it has provided Supplier with written notice of material breach and Supplier fails to cure such material breach within thirty (30) days of receipt of written notice. The Customer may also terminate a purchase order or other payment mechanism or Supplier's activities under the Contract immediately without a thirty (30) day written notice to Supplier, if Supplier fails to comply with confidentiality, privacy, security, environmental or safety requirements if such non-compliance relates or may relate to Supplier provision of products or services to the Customer or if Supplier's material breach is reasonably determined (i) to be an impediment to the function of the Customer and detrimental to the Customer, or (ii) when conditions preclude the thirty (30) day notice.

5. Termination for Convenience

In addition to any termination for convenience provisions in the Contract, a Customer may terminate a purchase order or other payment mechanism for convenience if it is determined that termination is in the Customer's best interest. Supplier will be provided at least thirty (30) days' written notice of termination.

6. Contract Management Fee and Usage Report

6.1 Pursuant to 74 O.S. § 85.33A, the State assesses a contract management fee on all transactions under a statewide contract. The payment of such fee will be calculated for all transactions, net of returns and the Supplier has no right of setoff against such fee regardless of the payment status of any Customer or any aggregate accounts receivable percentage. Supplier acknowledges and agrees that all prices quoted under any statewide contract shall include the contract management fee and the contract management fee shall not be reflected as a separate line item in Supplier's billing. The State reserves the

right to change this fee upward or downward upon sixty (60) calendar days' written notice to Supplier without further requirement for an Addendum.

6.2 While Supplier is the awardee of a statewide contract, transactions that occur under the terms of the statewide contract are subject to a one percent (1%) contract management fee to be paid by Supplier. Supplier shall submit a Contract Usage Report on a quarterly basis for each contract using a form provided by the State and such report shall include applicable information for each transaction. Reports shall include usage of the statewide contract by every Customer during the applicable quarter. A singular report provided late will not be considered a breach of the statewide contract; provided, however, repeated failure to submit accurate quarterly usage reports and submit timely payments may result in suspension or termination, in whole or in part, of the Contract.

6.3 All Contract Usage Reports shall meet the following criteria:

- i. Electronic submission in Microsoft Excel format to strategic.sourcing@omes.ok.gov;
- ii. Quarterly submission regardless of whether there were transactions under the Contract during the applicable quarterly reporting period;
- iii. Submission no later than forty-five (45) days following the end of each calendar quarter;
- iv. Contract quarterly reporting periods shall be as follows:
 - a. January 01 through March 31;
 - b. April 01 through June 30;
 - c. July 01 through September 30; and
 - d. October 01 through December 31.
- v. Reports must include the following information:
 - a. Procuring entity;
 - b. Order date;

- c. Purchase Order number or note that the transaction was paid by Purchase Card;
- d. City in which products or services were received or specific office or subdivision title;
- e. Product manufacturer or type of service;
- f. Manufacturer item number, if applicable;
- g. Product description;
- h. General product category, if applicable;
- i. Quantity;
- j. Unit list price or MSRP, as applicable;
- k. Unit price charged to the purchasing entity; and
- l. Other Contract usage information requested by the State.

6.4 Payment of the contract management fee shall be delivered to the following address within forty-five (45) calendar days after the end of each quarterly reporting period:

State of Oklahoma
Office of Management and Enterprise Services, Central Purchasing
2401 North Lincoln Boulevard, Suite 116
Oklahoma City, Oklahoma 73105

To ensure payment is properly accounted for, Supplier shall provide the following information with payment: (i) reference to the applicable Contract Usage Report and quarterly reporting period and (ii) the applicable statewide contract number(s) and the amount of the contract management fee being paid for each contract number.

ATTACHMENT D

STATE OF OKLAHOMA INFORMATION TECHNOLOGY TERMS

The parties further agree to the following terms (“Information Technology Terms”), as applicable, for any Acquisition of products or services with an information technology or telecommunication component. Pursuant to the Oklahoma Information Technology Consolidation and Coordination Act, OMES-Information Services (“OMES-IS”) is designated to purchase information technology and telecommunication products and services on behalf of the State. The Act directs OMES-IS to acquire necessary hardware, software and services and to authorize the use by other State agencies. OMES, as the owner of information technology and telecommunication assets and contracts on behalf of the State, allows other State agencies to use the assets while retaining ownership and the right to reassign the assets, at no additional cost, upon written notification to Supplier. OMES-IS is the data custodian for State agency data; however, such data is owned by the respective State agency.

1 Definitions

- 1.1 **COTS** means software that is commercial off the shelf.
- 1.2 **Customer Data** means all data supplied by or on behalf of a Customer in connection with the Contract, excluding any confidential information of Supplier.
- 1.3 **Data Breach** means the unauthorized access by an unauthorized person that results in the use, disclosure or theft of Customer Data.
- 1.4 **Host** includes the terms **Hosted** or **Hosting** and means the accessing, processing or storing of Customer Data.
- 1.5 **Intellectual Property Rights** means the worldwide legal rights or interests evidenced by or embodied in any idea, design, concept, personality right, method, process, technique, apparatus, invention, discovery or improvement including any patents, trade secrets and know-how; any work of authorship including any copyrights, Moral Rights or neighboring rights; any trademark, service mark, trade dress, trade name or other indicia of source or origin; domain name registrations; and any other proprietary or similar rights. Intellectual Property Rights of a party also includes all worldwide legal rights or interests that the party may have acquired by assignment or license with the right to grant sublicenses.
- 1.6 **Moral Rights** means any and all rights of paternity or integrity of the Work Product and the right to object to any modification, translation or use of the Work Product and any similar rights existing under the judicial or statutory law of any country in the world or under any treaty, regardless of whether or not such right is denominated or referred to as a moral right.
- 1.7 **Non-Public Data** means Customer Data, other than Personal Data, that is not subject to distribution to the public as public information. It is deemed to be sensitive and confidential

by Customer because it contains information that is exempt by statute, ordinance or administrative rule from access by the general public as public information. Non-Public Data includes any data deemed confidential pursuant to the Contract, otherwise identified by Customer as Non-Public Data, or that a reasonable person would deem confidential.

- 1.8 Personal Data** means Customer Data that contains 1) any combination of an individual's name, social security numbers, driver's license, state/federal identification number, account number, credit or debit card number and/or 2) data subject to protection under a federal, state or local law, rule, regulation or ordinance.
- 1.9 Security Incident** means the attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with the Hosted environment used to perform the services.
- 1.10 State CIO** means the State Chief Information Officer or authorized designee.
- 1.11 Supplier Intellectual Property** means all tangible or intangible items or things, including the Intellectual Property Rights therein, created or developed by Supplier and identified in writing as such (a) prior to providing any services or Work Product to Customer and prior to receiving any documents, materials, information or funding from or on behalf of a Customer relating to the services or Work Product, or (b) after the effective date of the Contract if such tangible or intangible items or things were independently developed by Supplier outside Supplier's provision of services or Work Product for Customer under the Contract and were not created, prepared, developed, invented or conceived by any Customer personnel who then became personnel to Supplier or any of its affiliates or subcontractors, where, although creation or reduction-to-practice is completed while the person is affiliated with Supplier or its personnel, any portion of same was created, invented or conceived by such person while affiliated with Customer.
- 1.12 Third Party Intellectual Property** means the Intellectual Property Rights of any third party that is not a party to the Contract, and that is not directly or indirectly providing any goods or services to a Customer under the Contract.
- 1.13 Work Product** means any and all deliverables produced by Supplier for Customer under a statement of work issued pursuant to the Contract, including any and all tangible or intangible items or things that have been or will be prepared, created, developed, invented or conceived at any time following the effective date of the Contract, including but not limited to any (i) works of authorship (such as manuals, instructions, printed material, graphics, artwork, images, illustrations, photographs, computer programs, computer software, scripts, object code, source code or other programming code, HTML code, flow charts, notes, outlines, lists, compilations, manuscripts, writings, pictorial materials, schematics, formulae, processes, algorithms, data, information, multimedia files, text web pages or web sites, other written or machine readable expression of such works fixed in any tangible media, and all other copyrightable works), (i) trademarks, service marks, trade dress, trade names, logos, or other indicia of source or origin, (iii) ideas, designs, concepts,

personality rights, methods, processes, techniques, apparatuses, inventions, formulas, discoveries, or improvements, including any patents, trade secrets and know-how, (iv) domain names, (v) any copies, and similar or derivative works to any of the foregoing, (vi) all documentation and materials related to any of the foregoing, (vii) all other goods, services or deliverables to be provided to Customer under the Contract or statement of work, and (viii) all Intellectual Property Rights in any of the foregoing, and which are or were created, prepared, developed, invented or conceived for the use of benefit of Customer in connection with this Contract or a statement of work, or with funds appropriated by or for Customer or Customer's benefit: (a) by any Supplier personnel or Customer personnel, or (b) any Customer personnel who then became personnel to Supplier or any of its affiliates or subcontractors, where, although creation or reduction-to-practice is completed while the person is affiliated with Supplier or its personnel, any portion of same was created, invented or conceived by such person while affiliated with Customer.

2 Termination of Maintenance and Support Services

Customer may terminate maintenance or support services without an adjustment charge, provided any of the following circumstances occur:

- 2.1** Customer removes the product for which the services are provided, from productive use or;
- 2.2** The location at which the services are provided is no longer controlled by Customer (for example, because of statutory or regulatory changes or the sale or closing of a facility).

If Customer chooses to renew maintenance or support after maintenance has lapsed, Customer may choose to pay the additional fee, if any, associated with renewing a license after such maintenance or support has lapsed, or to purchase a new license. Any amount paid to Supplier in the form of prepaid fees that are unused when services under the Contract or purchase order are terminated shall be refunded to Customer.

3 Compliance and Electronic and Information Technology Accessibility

State procurement of information technology is subject to certain federal and State laws, rules and regulations related to information technology accessibility, including but not limited to Oklahoma Information Technology Accessibility Standards ("Standards") set forth at <https://omes.ok.gov/services/information-services/accessibility-standards>. Supplier shall provide a Voluntary Product Accessibility Template ("VPAT") describing accessibility compliance via a URL linking to the VPAT and shall update the VPAT as necessary in order to allow a Customer to obtain current VPAT information as required by State law. If products require development or customization, additional requirements and documentation may be required and compliance shall be necessary by Supplier. Such requirements may be stated in appropriate documents including but not limited to a statement of work, riders, agreement, purchase order or Addendum.

All representations contained in the VPAT provided will be relied upon by the State or a Customer, as applicable, for accessibility compliance purposes.

4 Media Ownership (Disk Drive and/or Memory Chip Ownership)

- 4.1** Any disk drives and memory cards purchased with or included for use in leased or purchased products under the Contract remain the property of the Customer.
- 4.2** Personal information may be retained within electronic media devices and components; therefore, electronic media shall not be released either between Customers or for the resale, of refurbished equipment that has been in use by a Customer, by the Supplier to the general public or other entities. This provision applies to replacement devices and components, whether purchased or leased, supplied by Supplier, its agents or subcontractors during the downtime (repair) of products purchased or leased through the Contract. If a device is removed from a location for repairs, the Customer shall have sole discretion, prior to removal, to determine and implement sufficient safeguards (such as a record of hard drive serial numbers) to protect personal information that may be stored within the hard drive or memory of the device.

5 Offshore Services

No offshore services are provided for under the Contract. State data shall not be used or accessed internationally for troubleshooting or any other use not specifically provided for herein without the prior written permission, which may be withheld in the State's sole discretion, from the appropriate authorized representative of the State. Notwithstanding the above, back office administrative functions of the Supplier may be located offshore and the follow-the-sun support model may be used by the Supplier to the extent allowed by law applicable to any Customer data being accessed or used.

6 Compliance with Technology Policies

- 6.1** The Supplier agrees to adhere to the State of Oklahoma "Information Security Policy, Procedures, and Guidelines" available at https://omes.ok.gov/s/g/files/gmc316/f/InfoSecPPG_0.pdf.

Supplier's employees and subcontractors shall adhere to the applicable State IT Standard Methodologies and Templates including but not limited to Project Management, Business Analysis, System Analysis, Enterprise and IT Architecture, Quality, Application and Security Methodologies and Templates as set forth at <http://eclipse.omes.ok.gov>.

- 6.2** Supplier shall comply with applicable Federal Information Processing Standards including, without limitation, FIPS 200, FIPS 140-2 or successor standards and all recommendations from the National Institute of Standards and Technology. The confidentiality of Customer Data shall be protected and maintained in accordance with these standards as well as other applicable Customer standards.

6.3 Supplier shall comply with the CJIS Security Policy as more particularly described at Appendix 2 attached hereto and incorporated herein.

7 Emerging Technologies

The State of Oklahoma reserves the right to enter into an Addendum to the Contract at any time to allow for emerging technologies not identified elsewhere in the Contract Documents if there are repeated requests for such emerging technology or the State determines it is warranted to add such technology.

8 Extension Right

In addition to extension rights of the State set forth in the Contract, the State CIO reserves the right to extend any Contract if the State CIO determines such extension to be in the best interest of the State.

9 Source Code Escrow

Pursuant to 62 O.S. § 34.31, if customized computer software is developed or modified exclusively for a State agency, the Supplier has a continuing obligation to comply with such law and place the source code for such software and any modifications thereto into escrow with an independent third party escrow agent. Supplier shall pay all fees charged by the escrow agent and enter into an escrow agreement, the terms of which are subject to the prior written approval of the State, including terms that provide the State receives ownership of all escrowed source code upon the occurrence of any of the following:

- 9.1** A bona fide material default of the obligations of the Supplier under the agreement with the applicable Customer;
- 9.2** An assignment by the Supplier for the benefit of its creditors;
- 9.3** A failure by the Supplier to pay, or an admission by the Supplier of its inability to pay, its debts as they mature;
- 9.4** The filing of a petition in bankruptcy by or against the Supplier when such petition is not dismissed within sixty (60) days of the filing date;
- 9.5** The appointment of a receiver, liquidator or trustee appointed for any substantial part of the Supplier's property;
- 9.6** The inability or unwillingness of the Supplier to provide the maintenance and support services in accordance with the agreement with the agency;
- 9.7** Supplier's ceasing of maintenance and support of the software; or
- 9.8** Such other condition as may be statutorily imposed by the future amendment or enactment of applicable Oklahoma law.

10 Commercial Off The Shelf Software

If Supplier specifies terms and conditions or clauses in an electronic license, subscription, maintenance, support or similar agreement that conflict with the terms of this Contract, the additional terms and conditions or conflicting clauses shall not be binding on the State and the provisions of this Contract shall prevail.

11 Ownership Rights

Any software developed by the Supplier under the terms of the Contract is for the sole and exclusive use of the State including but not limited to the right to use, reproduce, re-use, alter, modify, edit, or change the software as it sees fit and for any purpose. Moreover, except with regard to any deliverable based on Supplier Intellectual Property, the State shall be deemed the sole and exclusive owner of all right, title, and interest therein, including but not limited to all source data, information and materials furnished to the State, together with all plans, system analysis, and design specifications and drawings, completed programs and documentation thereof, reports and listing, all data and test procedures and all other items pertaining to the work and services to be performed pursuant to this Contract including all copyright and proprietary rights relating thereto. With respect to Supplier Intellectual Property, the Supplier grants the State, for no additional consideration, a perpetual, irrevocable, royalty-free license, solely for the internal business use of the State, to use, copy, modify, display, perform, transmit and prepare derivative works of Supplier Intellectual Property embodied in or delivered to the State in conjunction with the products.

Except for any Supplier Intellectual Property, all work performed by the Supplier of developing, modifying or customizing software and any related supporting documentation shall be considered as Work for Hire (as defined under the U.S. copyright laws) and, as such, shall be owned by and for the benefit of State.

In the event that it should be determined that any portion of such software or related supporting documentation does not qualify as “Work for Hire”, Supplier hereby irrevocably grants to the State, for no additional consideration, a non-exclusive, irrevocable, royalty-free license to use, copy, modify, display, perform, transmit and prepare derivative works of any such software and any Supplier Intellectual Property embodied in or delivered to the State in conjunction with the products.

Supplier shall assist the State and its agents, upon request, in preparing U.S. and foreign copyright, trademark, and/or patent applications covering software developed, modified or customized for the State. Supplier shall sign any such applications, upon request, and deliver them to the State. The State shall bear all expenses that incurred in connection with such copyright, trademark, and/or patent applications.

If any Acquisition pursuant to this Contract is funded wholly or in part with federal funds, the source code and all associated software and related documentation owned by the State may be

shared with other publicly funded agencies at the discretion of the State without permission from or additional compensation to the Supplier.

12 Intellectual Property Ownership

The following terms apply to ownership and rights related to Intellectual Property:

- 12.1** As between Supplier and Customer, the Work Product and Intellectual Property Rights therein are and shall be owned exclusively by Customer, and not Supplier. Supplier specifically agrees that the Work Product shall be considered “works made for hire” and that the Work Product shall, upon creation, be owned exclusively by Customer. To the extent that the Work Product, under applicable law, may not be considered works made for hire, Supplier hereby agrees that all right, title and interest in and to all ownership rights and all Intellectual Property Rights in the Work Product is hereby effectively transferred, granted, conveyed, assigned and relinquished exclusively to Customer, without the necessity of any further consideration, and Customer shall be entitled to obtain and hold in its own name all Intellectual Property Rights in and to the Work Product. Supplier acknowledges that Supplier and Customer do not intend Supplier to be a joint author of the Work Product within the meaning of the Copyright Act of 1976. Customer shall have access, during normal business hours (Monday through Friday, 8:00 a.m. to 5:00 p.m.) and upon reasonable prior notice to Supplier, to all Supplier materials, premises and computer files containing the Work Product. Supplier and Customer, as appropriate, will cooperate with one another and execute such other documents as may be reasonably appropriate to achieve the objectives herein. No license or other right is granted under the Contract to any Third Party Intellectual Property, except as may be incorporated in the Work Product by Supplier.
- 12.2** Supplier, upon request and without further consideration, shall perform any acts that may be deemed reasonably necessary or desirable by Customer to evidence more fully the transfer of ownership and/or registration of all Intellectual Property Rights in all Work Product to Customer to the fullest extent possible including, but not limited to, the execution, acknowledgement and delivery of such further documents in a form determined by Customer. In the event Customer shall be unable to obtain Supplier’s signature due to the dissolution of Supplier or Supplier’s failure to respond to Customer’s repeated requests for such signature on any document reasonably necessary for any purpose set forth in the foregoing sentence, Supplier hereby irrevocably designates and appoints Customer and its duly authorized officers and agents as Supplier’s agent and Supplier’s attorney-in-fact to act for and in Supplier’s behalf and stead to execute and file any such document and to do all other lawfully permitted acts to further any such purpose with the same force and effect as if executed and delivered by Supplier, provided however that no such grant of right to Customer is applicable if Supplier fails to execute any document due to a good faith dispute by Supplier with respect to such document. It is understood that such power is coupled with an interest and is therefore irrevocable. Customer shall have the full and sole power to prosecute such applications and to take all other action concerning the Work Product, and Supplier shall cooperate, at Customer’s sole expense, in the preparation and

prosecution of all such applications and in any legal actions and proceedings concerning the Work Product.

- 12.3** Supplier hereby irrevocably and forever waives, and agrees never to assert, any Moral Rights in or to the Work Product which Supplier may now have or which may accrue to Supplier's benefit under U.S. or foreign copyright or other laws and any and all other residual rights and benefits which arise under any other applicable law now in force or hereafter enacted. Supplier acknowledges the receipt of equitable compensation for its assignment and waiver of such Moral Rights.
- 12.4** All documents, information and materials forwarded to Supplier by Customer for use in and preparation of the Work Product shall be deemed the confidential information of Customer, subject to the license granted by Customer to Supplier hereunder. Supplier shall not otherwise use, disclose, or permit any third party to use or obtain the Work Product, or any portion thereof, in any manner without the prior written approval of Customer.
- 12.5** These provisions are intended to protect Customer's proprietary rights pertaining to the Work Product and the Intellectual Property Rights therein and any misuse of such rights would cause substantial and irreparable harm to Customer's business. Therefore, Supplier acknowledges and stipulates that a court of competent jurisdiction may immediately enjoin a material breach of the Supplier's obligations with respect to confidentiality provisions of the Contract and the Work Product and a Customer's Intellectual Property Rights, upon a request by Customer, without requiring proof of irreparable injury, as same is presumed.
- 12.6** Upon the request of Customer, but in any event upon termination or expiration of this Contract or a statement of work, Supplier shall surrender to Customer all documents and things pertaining to the Work Product, generated or developed by Supplier or furnished by Customer to Supplier, including all materials embodying the Work Product, any Customer confidential information and Intellectual Property Rights in such Work Product, regardless of whether complete or incomplete. This section is intended to apply to all Work Product as well as to all documents and things furnished to Supplier by Customer or by anyone else that pertains to the Work Product.
- 12.7** Customer hereby grants to Supplier a non-transferable, non-exclusive, royalty-free, fully paid license to use any Work Product solely as necessary to provide services to Customer. Except as provided in this section, neither Supplier nor any subcontractor shall have the right to use the Work Product in connection with the provision of services to its other customers without the prior written consent of Customer, which consent may be withheld in Customer's sole discretion.
- 12.8** To the extent that any Third Party Intellectual Property is embodied or reflected in the Work Product or is necessary to provide services, Supplier shall obtain from the applicable third party for the Customer's benefit, an irrevocable, perpetual, non-exclusive, worldwide, royalty-free license, solely for Customer's internal business purposes; likewise, with respect to any Supplier Intellectual Property embodied or reflected in the Work Product or

necessary to provide services, Supplier grants to Customer an irrevocable, perpetual, non-exclusive, worldwide, royalty-free license, solely for the Customer's internal business purposes. Each such license shall allow the applicable Customer to (i) use, copy, modify, display, perform (by any means), transmit and prepare derivative works of any Third Party Intellectual Property or Supplier Intellectual Property embodied in or delivered to Customer in conjunction with the Work Product and (ii) authorize others to do any or all of the foregoing. Supplier agrees to notify Customer on delivery of the Work Product or services if such materials include any Third Party Intellectual Property. The foregoing license includes the right to sublicense third parties, solely for the purpose of engaging such third parties to assist or carry out Customer's internal business use of the Work Product. Except for the preceding license, all rights in Supplier Intellectual Property remain in Supplier. On request, Supplier shall provide Customer with documentation indicating a third party's written approval for Supplier to use any Third Party Intellectual Property that may be embodied or reflected in the Work Product.

- 12.9** Supplier agrees that it shall have written agreement(s) that are consistent with the provisions hereof related to Work Product and Intellectual Property Rights with any employees, agents, consultants, contractors or subcontractors providing services or Work Product pursuant to the Contract, prior to the provision of such services or Work Product and that it shall maintain such written agreements at all times during performance of this Contract which are sufficient to support all performance and grants of rights by Supplier. Copies of such agreements shall be provided to the Customer promptly upon request.
- 12.10** To the extent not inconsistent with Customer's rights in the Work Product or other provisions, nothing in this Contract shall preclude Supplier from developing for itself, or for others, materials which are competitive with those produced as a result of the services provided under the Contract, provided that no Work Product is utilized, and no Intellectual Property Rights of Customer therein are infringed by such competitive materials. To the extent that Supplier wishes to use the Work Product or acquire licensed rights in certain Intellectual Property Rights of Customer therein in order to offer competitive goods or services to third parties, Supplier and Customer agree to negotiate in good faith regarding an appropriate license and royalty agreement to allow for such.
- 12.11** If any Acquisition pursuant to the Contract is funded wholly or in part with federal funds, the source code and all associated software and related documentation and materials owned by a Customer may be shared with other publicly funded agencies at the discretion of such Customer without permission from or additional compensation to the Supplier.

13 Hosting Services

- 13.1** If Supplier or its subcontractor, affiliate or any other person or entity providing products or services under the Contract Hosts Customer Data in connection with an Acquisition, the provisions of Appendix 1, attached hereto and incorporated herein, apply to such Acquisition.

13.2 If the Hosting of Customer Data by Supplier or its subcontractor, affiliate or any other person or entity providing products or services under the Contract contributes to or directly causes a Data Breach, Supplier shall be responsible for the obligations set forth in Appendix 1 related to breach reporting requirements and associated costs. Likewise if such Hosting contributes to or directly causes a Security Incident, Supplier shall be responsible for the obligations set forth in Appendix 1, as applicable.

14 Change Management

When a scheduled change is made to products or services provided to a Customer that impacts the Customer's system related to such product or service, Supplier shall provide two (2) weeks' prior written notice of such change. When the change is an emergency change, Supplier shall provide twenty-four (24) hours' prior written notice of the change. Repeated failure to provide such notice may be an evaluation factor (as indicative of Supplier's past performance) upon renewal or if future bids submitted by Supplier are evaluated by the State.

15 Service Level Deficiency

In addition to other terms of the Contract, in instances of the Supplier's repeated failure to provide an acceptable level of service or meet service level agreement metrics, service credits shall be provided by Supplier and may be used as an offset to payment due.

16 Notices

In addition to notice requirements under the terms of the Contract otherwise, the following individuals shall also be provided the request, approval or notice, as applicable:

Chief Information Officer
3115 N. Lincoln Blvd
Oklahoma City, OK 73105

With a copy, which shall not constitute notice, to:

Information Services Deputy Counsel
3115 North Lincoln Boulevard
Oklahoma City, Oklahoma 73105

Appendix 1 to State of Oklahoma Information Technology Terms

The parties agree to the following provisions in connection with any Customer Data accessed, processed or stored by or on behalf of the Supplier and the obligations, representations and warranties set forth below shall continue as long as the Supplier has an obligation under the Contract

A. Customer Data

1. Customer will be responsible for the accuracy and completeness of all Customer Data provided to Supplier by Customer. Customer shall retain exclusive ownership of all Customer Data. Non-Public Data and Personal Data shall be deemed to be Customer's confidential information. Supplier shall restrict access to Customer Data to their employees with a need to know (and advise such employees of the confidentiality and non-disclosure obligations assumed herein).
2. Supplier shall promptly notify the Customer upon receipt of any requests from unauthorized third parties which in any way might reasonably require access to Customer Data or Customer's use of the Hosted environment. Supplier shall notify the Customer by the fastest means available and also in writing pursuant to Contract notice provisions and the notice provision herein. Except to the extent required by law, Supplier shall not respond to subpoenas, service or process, Freedom of Information Act or other open records requests, and other legal request related to Customer without first notifying the Customer and obtaining the Customer's prior approval, which shall not be unreasonably withheld, of Supplier's proposed responses. Supplier agrees to provide its completed responses to the Customer with adequate time for Customer review, revision and approval.
3. Supplier will use commercially reasonable efforts to prevent the loss of or damage to Customer Data in its possession and will maintain commercially reasonable back-up procedures and copies to facilitate the reconstruction of any Customer Data that may be lost or damaged by Supplier. Supplier will promptly notify Customer of any loss, damage to, or unauthorized access of Customer Data. Supplier will use commercially reasonable efforts to reconstruct any Customer Data that has been lost or damaged by Supplier as a result of its negligence or willful misconduct. If Customer Data is lost or damaged for reasons other than as a result of Supplier's negligence or willful misconduct, Supplier, at the Customer's expense, will, at the request of the State, use commercially reasonable efforts to reconstruct any Customer Data lost or damaged.

B. Data Security

1. Supplier will use commercially reasonable efforts, consistent with industry standards, to provide security for the Hosted environment and Customer Data and to protect against both unauthorized access to the Hosting environment, and unauthorized communications between the Hosting environment and the Customer's browser. Supplier shall implement and maintain appropriate administrative, technical and organizational security measures to safeguard against unauthorized access, disclosure or theft of Personal Data and Non-Public

Data. Such security measures shall be in accordance with recognized industry practice and not less stringent than the measures the service provider applies to its own personal data and non-public data of similar kind.

2. All Personal Data and Non-public Data shall be encrypted at rest and in transit with controlled access. Unless otherwise stipulated, the service provider is responsible for encryption of Personal Data.
3. Supplier represents and warrants to the Customer that the Hosting equipment and environment will be routinely checked with a commercially available, industry standard software application with up-to-date virus definitions. Supplier will regularly update the virus definitions to ensure that the definitions are as up-to-date as is commercially reasonable. Supplier will promptly purge all viruses discovered during virus checks. If there is a reasonable basis to believe that a virus may have been transmitted to Customer by Supplier, Supplier will promptly notify Customer of such possibility in a writing that states the nature of the virus, the date on which transmission may have occurred, and the means Supplier has used to remediate the virus. Should the virus propagate to Customer's IT infrastructure, Supplier is responsible for costs incurred by Customer for Customer to remediate the virus.
4. Supplier shall provide its services to Customer and its users solely from data centers in the U.S. Storage of Customer Data at rest shall be located solely in data centers in the U.S. Supplier shall not allow its personnel or contractors to store Customer Data on portable devices, including personal computers, except for devices that are used and kept only at its U.S. data centers. Supplier shall permit its personnel and contractors to access Customer Data remotely only as required to fulfill Supplier's obligations under the Contract.
5. Supplier shall allow the Customer to audit conformance to the Contract terms. The Customer may perform this audit or contract with a third party at its discretion and at Customer's expense.
6. Supplier shall perform an independent audit of its data centers at least annually at its expense and provide a redacted version of the audit report upon request. Supplier may remove its proprietary information from the redacted version. A Service Organization Control (SOC) 2 audit report or approved equivalent sets the minimum level of a third-party audit.
7. Any remedies provided in this Appendix are not exclusive and are in addition to other rights and remedies available under the terms of the Contract, at law or in equity.

C. Security Assessment

1. The State requires any entity or third-party Supplier Hosting Oklahoma Customer Data to submit to a State Certification and Accreditation Review process to assess initial security risk. Supplier submitted to the review and met the State's minimum security standards at time the Contract was executed. Failure to maintain the State's minimum security standards

during the term of the contract, including renewals, constitutes a material breach. Upon request, the Supplier shall provide updated data security information in connection with a potential renewal. If information provided in the security risk assessment changes, Supplier shall promptly notify the State and include in such notification the updated information; provided, however, Supplier shall make no change that results in lessened data protection or increased data security risk. Failure to provide the notice required by this section or maintain the level of security required in the Contract constitutes a material breach by Supplier and may result in a whole or partial termination of the Contract.

2. Any Hosting entity change must be approved in writing prior to such change. To the extent Supplier requests a different sub-contractor than the third-party Hosting Supplier already approved by the State, the different sub-contractor is subject to the State's approval. Supplier agrees not to migrate State's data or otherwise utilize the different third-party Hosting Supplier in connection with key business functions that are Supplier's obligations under the contract until the State approves the third-party Hosting Supplier's State Certification and Accreditation Review, which approval shall not be unreasonably withheld or delayed. In the event the third-party Hosting Supplier does not meet the State's requirements under the State Certification and Accreditation Review, Supplier acknowledges and agrees it will not utilize the third-party Supplier in connection with key business functions that are Supplier's obligations under the contract, until such third party meets such requirements.

D. Security Incident or Data Breach Notification: Supplier shall inform Customer of any Security Incident or Data Breach.

1. Supplier may need to communicate with outside parties regarding a Security Incident, which may include contacting law enforcement, fielding media inquiries and seeking external expertise as mutually agreed upon, defined by law or contained in the Contract. If a Security Incident involves Customer Data, Supplier will coordinate with Customer prior to any such communication.
2. Supplier shall report a Security Incident to the Customer identified contact set forth herein within five (5) days of discovery of the Security Incident or within a shorter notice period required by applicable law or regulation (i.e. HIPAA requires notice to be provided within 24 hours).
3. Supplier shall:
 - a. Maintain processes and procedures to identify, respond to and analyze Security Incidents;
 - b. Make summary information regarding such procedures available to Customer at Customer's request;
 - c. Mitigate, to the extent practicable, harmful effects of Security Incidents that are known to Supplier; and

d. Document all Security Incidents and their outcomes.

4. If Supplier has reasonable belief or actual knowledge of a Data Breach, Supplier shall (1) promptly notify the appropriate Customer identified contact set forth herein within 24 hours or sooner, unless shorter time is required by applicable law, and (2) take commercially reasonable measures to address the Data Breach in a timely manner.

E. **Breach Responsibilities:** This section only applies when a Data Breach occurs with respect to Personal Data or Non-Public Data within the possession or control of Supplier.

1. Supplier shall (1) cooperate with Customer as reasonably requested by Customer to investigate and resolve the Data Breach, (2) promptly implement necessary remedial measures, if necessary, and (3) document responsive actions taken related to the Data Breach, including any post-incident review of events and actions taken to make changes in business practices in providing the services, if necessary.
2. Unless otherwise stipulated, if a Data Breach is a direct result of Supplier's breach of its obligation to encrypt Personal Data and Non-Public Data or otherwise prevent its release, Supplier shall bear the costs associated with (1) the investigation and resolution of the Data Breach; (2) notifications to individuals, regulators or others required by state law; (3) credit monitoring services required by state or federal law; (4) a website or toll-free numbers and call center for affected individuals required by state law – all not to exceed the agency per record per person cost calculated for data breaches in the United States on the most recent Cost of Data breach Study: Global Analysis published by the Ponemon Institute at the time of the data breach; and (5) complete all corrective actions as reasonably determined by Supplier based on root cause.
3. If a Data Breach is a direct result of Supplier's breach of its obligations to encrypt Personal Data and Non-Public Data or otherwise prevent its release, Supplier shall indemnify and hold harmless the Customer against all penalties assessed to Indemnified Parties by governmental authorities in connection with the Data Breach.

F. **Notices**

In addition to notice requirements under the terms of the Contract and those set forth above, a request, an approval or a notice in connection with this Appendix provided by Supplier shall be provided to:

Chief Information Security Officer

3115 N. Lincoln Blvd

Oklahoma City, OK 73105

and

servicedesk@omes.ok.gov.

G. Supplier Representations and Warranties

Supplier represents and warrants the following:

1. The product and services provided in connection with Hosting services do not infringe a third party's patent or copyright or other intellectual property rights.
2. Supplier will protect Customer's Non-Public Data and Personal Data from unauthorized dissemination and use with the same degree of care that each such party uses to protect its own confidential information and, in any event, will use no less than a reasonable degree of care in protecting such confidential information.
3. The execution, delivery and performance of the Contract and any ancillary documents and the consummation of the transactions contemplated by the Contract or any ancillary documents by Supplier will not violate, conflict with, or result in a breach of any provision of, or constitute a default (or an event which, with notice or lapse of time or both, would constitute a default) under, or result in the termination of, any written contract or other instrument between Supplier and any third parties retained or utilized by Supplier to provide goods or services for the benefit of the Customer.
4. Supplier shall not knowingly upload, store, post, e-mail or otherwise transmit, distribute, publish or disseminate to or through the Hosting environment any material that contains software viruses, malware or other surreptitious code designed to interrupt, destroy or limit the functionality of any computer software or hardware or telecommunications equipment or circumvent any "copy-protected" devices, or any other harmful or disruptive program.

H. Indemnity

Supplier agrees to defend, indemnify and hold the State, its officers, directors, employees, and agents harmless from all liabilities, claims, damages, losses, costs, expenses, demands, suits and actions (including without limitation reasonable attorneys' fees and costs required to establish the right to indemnification), excluding damages that are the sole fault of Customer, arising from or in connection with Supplier's breach of its express representations and warranties in these Information Technology Terms and the Contract. If a third party claims that any portion of the products or services provided by Supplier under the terms of another Contract Document or these Information Technology Terms infringes that party's patent or copyright, Supplier shall defend, indemnify and hold harmless the State and Customer against the claim at Supplier's expense and pay all related costs, damages, and attorney's fees incurred by or assessed to, the State and/or Customer. The State and/or Customer shall promptly notify Supplier of any third party claims and to the extent authorized by the Attorney General of the State, allow Supplier to control the defense and any related settlement negotiations. If the Attorney General of the State does not authorize sole control of the defense and settlement negotiations to Supplier, Supplier shall be granted authorization to equally participate in any proceeding related to this section but Supplier shall remain responsible to indemnify Customer and the State for all associated costs, damages and fees incurred by or assessed to the State and/or Customer. Should the software become, or in Supplier's

opinion, be likely to become the subject of a claim or an injunction preventing its use as contemplated in connection with Hosting services, Supplier may, at its option (i) procure for the State the right to continue using the software or (ii) replace or modify the software with a like or similar product so that it becomes non-infringing.

I. Termination, Expiration and Suspension of Service

1. During any period of service suspension, Supplier shall not take any action to intentionally disclose, alter or erase any Customer Data.

2. In the event of a termination or expiration of the Contract, the parties further agree:

Supplier shall implement an orderly return of Customer Data in a format specified by the Customer and, as determined by the Customer:

a. return the Customer Data to Customer at no additional cost, at a time agreed to by the parties and the subsequent secure disposal of State Data;

b. transitioned to a different Supplier at a mutually agreed cost and in accordance with a mutually agreed data transition plan and the subsequent secure disposal of State Data or

c. a combination of the two immediately preceding options.

3. Supplier shall not take any action to intentionally erase any Customer Data for a period of:

a. 10 days after the effective date of termination, if the termination is in accordance with the contract period;

b. 30 days after the effective date of termination, if the termination is for convenience; or

c. 60 days after the effective date of termination, if the termination is for cause.

After such period, Supplier shall, unless legally prohibited or otherwise stipulated, delete all Customer Data in its systems or otherwise in its possession or under its control.

4. The State shall be entitled to any post termination or expiration assistance generally made available with respect to the services.

5. Disposal by Supplier of Customer Data in all of its forms, such as disk, CD/DVD, backup tape and paper, when requested by the Customer, shall be performed in a secure manner. Data shall be permanently deleted and shall not be recoverable, according to National Institute of Standards and Technology (NIST)-approved methods. Certificates of destruction shall be provided to Customer within thirty (30) calendar day of its request for disposal of data.

Appendix 2 to State of Oklahoma Information Technology Terms

INTRODUCTION

The use and maintenance of all items of software or equipment offered for purchase herein must be in compliance with the most current version of the U.S. Department of Justice, Federal Bureau of Investigation (“FBI”), Criminal Justice Information Services (CJIS) Division’s CJIS Security Policy (“CJIS Security Policy” or “Security Policy” herein).

The Entity or Affiliate acquiring the data or system is hereby ultimately responsible for compliance with the CJIS Security Policy and will be subject to an audit by the State of Oklahoma CJIS Systems Officer (“CSO”) and the FBI CJIS Division’s Audit Staff.

CJIS SECURITY POLICY REQUIREMENTS GENERALLY

The CJIS Security Policy outlines a number of administrative, procedural, and technical controls agencies must have in place to protect Criminal Justice Information (“CJI”). Our experience is that agencies will generally have many of the administrative and procedural controls in place but will need to implement additional technical safeguards in order to be in complete compliance with the mandate. A Criminal Justice Agency (“CJA”) and certain other governmental agencies procuring technology equipment and services that could be used in hosting or connecting or transmitting or receiving CJI data may need to use the check list herein to make sure that the software, equipment, location, security, and persons having the ability to access CJI will meet the CJIS requirements per the then current CJIS Security Policy. A completed Appendix H to said Security Policy will need to be signed by Vendor or a 3rd party if it has access to CJI, such as incident to the maintenance or support of the purchased hardware or software within which resides CJI. **Per Appendix “A” to said Security Policy, “access to CJI is the physical or logical (electronic) ability, right or privilege to view, modify or make use of CJI.”**

DIRECTIVE CONCERNING ACCESS TO CRIMINAL JUSTICE INFORMATION AND TO HARDWARE OR SOFTWARE WHICH INTERACTS WITH CJI and CERTIFICATION

The FBI CJIS Division provides state-of-the-art identification and information services to the local, state, tribal, federal, and international criminal justice communities for criminal justice purposes, as well as the noncriminal justice communities for noncriminal justice purposes.

This Directive primarily concerns access to CJI and access to hardware and software in the use, retention, transmission, reception, and hosting of CJI for criminal justice purposes and not for noncriminal justice purposes. In that regard, this Directive is not only applicable to such data, but also to the hardware and software interacting with such data, their location(s), and persons having the ability to access such data. The CJIS data applicable to the Security Policy is the data described as such in said Policy **plus all data transmitted over the Oklahoma Law Enforcement Telecommunications System (“OLETS”) which is operated by DPS.**

In order to have access to CJI or to the aforesaid hardware or software, the vendor must be familiar with the FBI CJIS Security Policy, including but not limited to the following portions of said Security Policy:

1. the Definitions and Acronyms in §3 & Appendices “A” & “B”;

2. the general policies in §4;
3. the Policies in §5;
4. the appropriate forms in Appendices “D”, “E”, “F” & “H”; and
5. the Supplemental Guidance in Appendices “J” & “K”.

This FBI Security Policy is located and may be downloaded at: <https://www.fbi.gov/services/cjis/cjis-security-policy-resource-center>.

By executing the Contract to which this Directive is attached, the vendor hereby CERTIFIES that the foregoing directive has and will be followed, including but not limited to full compliance with the FBI CJIS Security Policy, as amended and as applicable.

Policy Requirement Checklist		Compliance checklist –
Policy Area 1	Information Exchange Agreements	
Policy Area 2	Security Awareness Training	
Policy Area 3	Incident Response	
Policy Area 4	Auditing and Accountability	
Policy Area 5	Access Control	
Policy Area 6	Identification and Authentication	
Policy Area 7	Configuration Management	
Policy Area 8	Media Protection	
Policy Area 9	Physical Protection	
Policy Area 10	Systems and Communications Protection and Information Integrity	
Policy Area 11	Formal Audits	
Policy Area 12	Personnel Security	

Attachment D-1

Information Security Requirements

1. General Information Security Requirements

- a. No employee of Contractor or its subcontractors will be granted access to State of Oklahoma agency information systems without the prior completion and approval of applicable logon authorization and acceptable use requests.
- b. Contractor or its subcontractors will notify applicable State of Oklahoma agencies when employees who have access to agency information systems are terminated.
- c. Contractor or its subcontractors will disclose to Client any suspected breach of the security of the information system or the data contained therein in the most expedient time possible and without unreasonable delay and will cooperate with Client during the investigation of any such incident.
- d. Contractor or its subcontractors agree to adhere to the State of Oklahoma "Information Security Policy, Procedures, and Guidelines" available at: <https://oklahoma.gov/content/dam/ok/en/omes/documents/InfoSecPPG.pdf>

2. HIPAA Requirements

- a. Contractor shall agree to use and disclose Protected Health Information in its possession or control in compliance with the Standards for Privacy of Individually Identifiable Health Information (Privacy Rule) (45 C.F.R. Parts 160 and 164) under the Health Insurance Portability and Accountability Act (HIPAA) of 1996. The definitions set forth in the Privacy Rule are incorporated by reference into this Contract (45 C.F.R. §§ 160.103 and 164.501).
- b. If applicable, Contractor will sign and adhere to a Business Associate Agreement (BAA). The Business Associate Agreement provides for satisfactory assurances that Contractor will use the information only for the purposes for which it was engaged. Contractor agrees it will safeguard the information from misuse, and will comply with HIPAA as it pertains to the duties stated within the contract. Failure to comply with the requirements of this standard may result in funding being withheld from Contractor, and/or full audit and inspection of Contractor's security compliance as it pertains to this contract.
- c. Business Associate Terms Definitions:
 - i. Unless otherwise defined in this BAA, all capitalized terms used in this BAA have the meanings ascribed in the HIPAA Regulations, provided; however, that "PHI" and "ePHI" shall mean Protected Health Information and Electronic Protected Health Information, respectively, as defined in 45 C.F.R. § 160.103, limited to the information Business Associate received from or created or received on behalf of the applicable State of Oklahoma agency as a Business Associate. "Administrative Safeguards" shall have the same meaning as the term "administrative safeguards in 45 C.F.R. § 164.304, with the exception that it shall apply to the management of the conduct of Business

- Associate's workforce, not the State of Oklahoma agency workforce, in relation to the protection of that information.
- ii. Business Associate. "Business Associate" shall generally have the same meaning as the term "Business Associate" at 45 C.F.R. 160.103, and in reference to the party to this agreement, shall mean the entity whose name appears below.
 - iii. Covered Entity. "Covered Entity" shall generally have the same meaning as the term "Covered Entity" at 45 C.F.R. 160.103.
 - iv. HIPAA Rules. "HIPAA Rules" shall mean the Privacy, Security, Breach Notification, and Enforcement Rules at 45 C.F.R. Part 160 and Part 164, all as may be amended.
 - v. The following terms used in this Agreement shall have the same meaning as those terms in the HIPAA Rules: Breach, Data Aggregation, Designated Record Set, Disclosure, Health Care Operations, Individual, Minimum Necessary, Notice of Privacy Practices, Protected Health Information, required by law, Secretary, Security Incident, Sub-Contractor, Unsecured PHI, and Use.
- d. Obligations of Business Associate: Business Associate may use Electronic PHI and PHI (collectively, "PHI") solely to perform its duties and responsibilities under this Agreement and only as provided in this Agreement. Business Associate acknowledges and agrees that PHI is confidential and shall not be used or disclosed, in whole or in part, except as provided in this Agreement or as required by law. Specifically, Business Associate agrees it will, as applicable:
- i. use or further disclose PHI only as permitted in this Agreement or as Required by Law, including, but not limited to the Privacy and Security Rule;
 - ii. use appropriate safeguards, and comply with Subpart C of 45 C.F.R. Part 164 with respect to Electronic PHI, to prevent use or disclosure of PHI other than as provided for by this Agreement;
 - iii. implement and document appropriate administrative, physical, and technical safeguards to protect the confidentiality, integrity, and availability of PHI that it creates, receives, maintains, or transmits for or on behalf of Covered Entity in accordance with 45 C.F.R. 164;
 - iv. implement and document administrative safeguards to prevent, detect, contain, and correct security violations in accordance with 45 C.F.R. 164;
 - v. make its applicable policies and procedures required by the Security Rule available to Covered Entity solely for purposes of verifying BA's compliance and the Secretary of the Department of Health and Human Services (HHS);
 - vi. not receive remuneration from a third party in exchange for disclosing PHI received from or on behalf of Covered Entity;
 - vii. in accordance with 45 C.F.R. 164.502(e)(1) and 164.308(b), if applicable, require that any Sub-Contractors that create, receive, maintain or transmit PHI on behalf of the Business Associate agree to the same restrictions, conditions, and requirements that apply to the Business Associate with respect to such information; this shall be in the

form of a written HIPAA Business Associate Contract and a fully executed copy will be provided to the Contract Monitor;

- viii. report to Covered Entity in writing any use or disclosure of PHI that is not permitted under this Agreement as soon as reasonably practicable but in no event later than five calendar days from becoming aware of it and mitigate, to the extent practicable and in cooperation with Covered Entity, any harmful effects known to it of a use or disclosure made in violation of this Agreement;
- ix. promptly report to Covered Entity in writing and without unreasonable delay and in no case later than five calendar days any successful Security Incident, as defined in the Security Rule, with respect to Electronic PHI;
- x. with the exception of law enforcement delays that satisfy the requirements of 45 C.F.R. 164.412, notify Covered Entity promptly, in writing and without unreasonable delay and in no case later than five calendar days, upon the discovery of a breach of Unsecured PHI. Such notice shall include, to the extent possible, the name of each individual who's Unsecured PHI has been, or is reasonably believed by Business Associate to have been, accessed, acquired, or disclosed during such Breach. Business Associate shall also, to the extent possible, furnish Covered Entity with any other available information that Covered Entity is required to include in its notification to Individuals under 45 C.F.R. § 164.404(c) at the time of Business Associate's notification to Covered Entity or promptly thereafter as such information becomes available. As used in this Section, "breach" shall have the meaning given such term at 45 C.F.R. 164.402;
- xi. to the extent allowed by law, indemnify and hold Covered Entity harmless from all claims, liabilities costs, and damages arising out of or in any manner related to the unauthorized disclosure by Business Associate of any PHI resulting from the negligent acts or omissions of Business Associate or to the breach by Business Associate of any applicable obligation related to PHI;
- xii. provide access to PHI it maintains in a Designated Record Set to Covered Entity, or if directed by Covered Entity to an Individual in order to meet the requirements of 45 C.F.R. 164.524. In the event that any Individual requests access to PHI directly from Business Associate, Business Associate shall forward such request to Covered Entity within five working days of receiving a request. This shall be in the form of a written HIPAA Business Associate Contract and a fully executed copy will be provided to the Contract Monitor. Any denials of access to the PHI requested shall be the responsibility of Covered Entity;
- xiii. make PHI it maintains in a Designated Record Set available to Covered Entity for amendment and incorporate any amendments to PHI in accordance with 45 C.F.R. 164.526;
- xiv. document disclosure of PHI it maintains in a Designated Record Set and information related to such disclosure as would be required for Covered Entity to

- respond to a request by an Individual for an accounting of disclosures of PHI, in accordance with 45 C.F.R. 164.528, and within five working days of receiving a request from Covered Entity, make such disclosure documentation and information available to Covered Entity. In the event the request for an accounting is delivered directly to Business Associate, Business Associate shall forward within five working days of receiving a request such request to Covered Entity;
- xv. make its internal practices, books, and records related to the use and disclosure of PHI received from or created or received by Business Associate on behalf of Covered Entity available to the Secretary of the Department of HHS, authorized governmental officials, and Covered entity for the purpose of determining Business Associate's compliance with the Privacy Rule. Business Associate shall give Covered Entity advance written notice of requests from HHS or government officials and provide Covered Entity with a copy of all documents made available; and
 - xvi. require that all of its Sub-Contractors, vendors, and agents to whom it provides PHI or who create, receive, use, disclose, maintain, or have access to Covered Entity's PHI shall agree in writing to requirements, restrictions, and conditions at least as stringent as those that apply to Business Associate under this Agreement, including but not limited to implementing reasonable and appropriate safeguards to protect PHI, and shall require that its Sub-Contractors, vendors, and agents agree to indemnify and hold harmless Covered Entity for their failure to comply with each of the provisions of this Agreement.
- e. Permitted Uses and Disclosures of PHI by Business Associate: Except as otherwise provided in this Agreement, Business Associate may use or disclose PHI on behalf of or to provide services to Covered Entity for the purposes specified in this Agreement, if such use or disclosure of PHI would not violate the Privacy Rule if done by Covered Entity. Unless otherwise limited herein, Business Associate may:
- i. use PHI for its proper management and administration or to fulfill any present or future legal responsibilities of Business Associate;
 - ii. disclose PHI for its proper management and administration or to fulfill any present or future legal responsibilities of Business Associate, provided that; (i) the disclosures required by law; or (ii) Business Associate obtains reasonable assurances from any person to whom the PHI is disclosed that such PHI will be kept confidential and will be used or further disclosed only as Required by Law or for the purpose(s) for which it was disclosed to the person, and the person commits to notifying Business Associate of any instances of which it is aware in which the confidentiality of the PHI has been breached;
 - iii. disclose PHI to report violations of law to appropriate federal and state authorities; or
 - iv. aggregate the PHI with other data in its possession for purposes of Covered Entity's Health Care Operations;

- v. make uses and disclosures and requests for protected health information consistent with Covered Entity's minimum necessary policies and procedures;
 - vi. de-identify any and all PHI obtained by Business Associate under this BAA, and use such de-identified data, all in accordance with the de-identification requirements of the Privacy Rule [45 C.F.R. § (d)(1)].
- f. Obligations of Covered Entity
- i. Covered Entity shall notify Business Associate of any changes in, or revocation of, the permission by an individual to use or disclose his or her PHI, to the extent that such changes may affect Business Associate's use or disclosure of PHI.
 - ii. Covered Entity shall notify Business Associate of any restriction on the use or disclosure of PHI that Covered Entity has agreed to or is required to abide by under 45 C.F.R. 164.522, to the extent that such restriction may affect Business Associate's use or disclosure of protected health information.
 - iii. Covered Entity shall not request Business Associate use or disclose PHI in any manner that would violate the Privacy Rule if done by Covered Entity.
 - iv. Covered Entity agrees to timely notify Business Associate, in writing, of any arrangements between Covered Entity and the Individual that is the subject of PHI that may impact in any manner the use and/or disclosure of the PHI by Business Associate under this BAA.
 - v. Covered Entity shall provide the minimum necessary PHI to Business Associate.
- g. Term and Termination:
- i. Obligations of Business Associate upon Termination. Upon termination of this Agreement for any reason, Business Associate, with respect to PHI received from Covered Entity, or created, maintained, or received by Business Associate on behalf of Covered Entity, shall as applicable:
 - (1) retain only that PHI that is necessary for Business Associate to continue its proper management and administration or to carry out its legal responsibilities;
 - (2) return to Covered Entity (or, if agreed to by Covered Entity, destroy) the remaining PHI that the Business Associate still maintains in any form;
 - (3) continue to use appropriate safeguards and comply with Subpart C of 45 C.F.R. Part 164 with respect to PHI to prevent use or disclosure of the PHI, other than as provided for in this Section, for as long as Business Associate retains the PHI;
 - (4) not use or disclose the PHI retained by Business Associate other than for the purposes for which such PHI was retained and subject to the same conditions set out at above under "Permitted Uses and Disclosures By Business Associate" that applied prior to termination; and
 - (5) return to Covered Entity (or, if agreed to by Covered Entity, destroy) the PHI retained by Business Associate when it is no longer needed by Business Associate for its proper management and administration or to carry out its legal responsibilities.

- ii. All other applicable obligations of Business Associate under this Agreement shall survive termination.
 - iii. Should the applicable State of Oklahoma agency become aware of a pattern of activity or practice that constitutes a material breach of a material term of this BAA by Business Associate, the agency shall provide Business Associate with written notice of such a breach in sufficient detail to enable Contractor to understand the specific nature of the breach. The Client shall be entitled to terminate the Underlying Contract associated with such breach if, after the applicable State of Oklahoma agency provides the notice to Business Associate, Business Associate fails to cure the breach within a reasonable time period not less than thirty (30) days specified in such notice; provided, however, that such time period specified shall be based on the nature of the breach involved per 45 C.F.R. §§ 164.504(e)(1)(ii)(A),(B) & 164.314 (a)(2)(i)(D).
- h. Miscellaneous Provisions:
- i. No Third Party Beneficiaries: Nothing in this Agreement shall confer upon any person other than the parties and their respective successors or assigns, any rights, remedies, obligations, or liabilities whatsoever.
 - ii. Business Associate recognizes that any material breach of this Business Associate Terms section or breach of confidentiality or misuse of PHI may result in the termination of this Agreement and/or legal action. Said termination may be immediate and need not comply with any termination provision in the parties' underlying agreement, if any.
 - iii. The parties agree to amend this Agreement from time to time as is necessary for Covered Entity or Business Associate to comply with the requirements of the Privacy Rule and related laws and regulations.
 - iv. The applicable State of Oklahoma agency shall make available its Notice of Privacy Practices.
 - v. Any ambiguity in this Agreement shall be resolved in a manner that causes this Agreement to comply with HIPAA.
 - vi. If Business Associate maintains a designated record set in an electronic format on behalf of Covered Entity, then Business Associate agrees that within 30 calendar days of expiration or termination of the parties' agreement, Business Associate shall provide to Covered Entity a complete report of all disclosures of and access to the designated record set covering the three years immediately preceding the termination or expiration. The report shall include patient name, date and time of disclosures/access, description of what was disclosed/accessed, purpose of disclosure/access, name of individual who received or accessed the information, and, if available, what action was taken within the designated record set.
 - vii. Amendment: To the extent that any relevant provision of the HIPAA Regulations is materially amended in a manner that changes the obligations of Business Associates or Covered Entities, the Parties agree to negotiate in good faith appropriate amendment(s)

to this Agreement to give effect to these revised obligations. The parties agree to amend this Agreement from time to time as is necessary for Covered Entity or to comply with the requirements of the Privacy Rule and related laws and regulations.

3. 42 C.F.R. Part 2 Related Provisions

- a. Confidentiality of Information. Contractor's employees and agents shall have access to private data to the extent necessary to carry out the responsibilities, limited by the terms of this Agreement. Contractor accepts the responsibilities for providing adequate administrative supervision and training to their employees and agents to ensure compliance with relevant confidentiality, privacy laws, regulations and contractual provisions. No private or confidential data collected, maintained, or used shall be disseminated except as authorized by statute and by terms of this Agreement, whether during the period of the Agreement or thereafter. Furthermore, Contractor:
 - i. Acknowledges that in receiving, transmitting, transporting, storing, processing, or otherwise dealing with any information received pursuant to this agreement that identifies or otherwise relates to the individuals under the care of or in the custody of a State of Oklahoma agency, it is fully bound by the provisions of the federal regulations governing the confidentiality of Alcohol and Drug Abuse Patient Records, 42 C.F.R. Part 2 and the HIPAA, 45 C.F.R. 45 Parts 142, 160, and 164, Title 43 A § 1-109 of Oklahoma Statutes, and may not use or disclose the information except as permitted or required by this Agreement or by law;
 - ii. Acknowledges that pursuant to 43A O.S. §1-109, all mental health and drug or alcohol treatment information and all communications between physician or psychotherapist and patient are both privileged and confidential and that such information is available only to persons actively engaged in treatment of the client or consumer or in related administrative work. Contractor agrees that such protected information shall not be available or accessible to staff in general and shall not be used for punishment or prosecution of any kind;
 - iii. Agrees to resist any efforts in judicial proceedings to obtain access to the protected information except as expressly provided for in the regulations governing the Confidentiality of Alcohol and Drug Abuse Patient Records, 42 C.F.R. Part 2;
 - iv. Agrees to, when applicable and to the extent within Contractor's control, use appropriate administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of the electronic protected health information that it creates, receives, maintains, or transmits on behalf of the State of Oklahoma agency and to use appropriate safeguards to prevent the unauthorized use or disclosure of the protected health information, and agrees that protected information will not be placed in the Child Protective Services (CPS) record of any individual involved with the Oklahoma Department of Human Services (DHS).

- v. Agrees to report to the State of Oklahoma agency any use or disclosure or any security incident involving protected information not provided for by this Agreement. Such a report shall be made immediately when an employee becomes aware of such a disclosure, use, or security incident.
 - vi. Agrees to provide access to the protected information at the request of the State of Oklahoma agency or to an authorized individual as directed by the State of Oklahoma agency, in order to meet the requirement of 45 C.F.R. §164.524 which provides clients with the right to access and copy their own protected information;
 - vii. Agrees to make any amendments to the protected information as directed or agreed to by the State of Oklahoma agency, pursuant to 45 C.F.R. §164.526;
 - viii. Agrees to make available its internal practices, books, and records, including policies and procedures, relating to the use and disclosure of protected information received from the State of Oklahoma agency or created or received by the Contractor on behalf of the State of Oklahoma agency, to the State of Oklahoma agency and to the Secretary of the Department of Health and Human Services for purpose of the Secretary determining the giving party's compliance with HIPAA;
 - ix. Agrees to provide the State of Oklahoma agency, or an authorized individual, information to permit the State of Oklahoma agency to respond to a request by an individual for an accounting of disclosures in accordance with 45 C.F.R. §164.528.
- b. Data Security. The Contractor agrees to, when applicable and to the extent within Contractor's control, maintain the data in a secure manner compatible with the content and use. The Contractor will, when applicable to the extent within Contractor's control, control access to the data in Contractor's possession or control compliance with the terms of this Agreement. Only the Contractor's personnel whose duties require the use of such information, will have regular access to the data. The Contractor's employees will be allowed access to the data only for the purpose set forth in this Agreement.
- c. Data Destruction. Contractor agrees to, when applicable and to the extent within Contractor's control, follow State of Oklahoma agency policies regarding secure data destruction.
- d. Use of Information. Contractor agrees that the information received or accessed through this Agreement shall not be used to the detriment of any individual nor for any purpose other than those stated in this Agreement.
- e. Redisclosure of Data. The Contractor agrees not to redisclose any information to a third party not covered by the Agreement unless written permission by the State of Oklahoma agency is received and redisclosure is permitted under applicable law.

4. Federal Tax Information Requirements IRS Publication 1075 (If Applicable)

- a. **PERFORMANCE:** If Contractor takes possession or control of Federal Tax Information in performance of this contract, the Contractor agrees to, when applicable and to the extent

within Contractor's control, comply with and assume responsibility for compliance by officers or employees with the following requirements:

- i. All work will be performed under the supervision of the State of Oklahoma.
- ii. The contractor and contractor's officers or employees to be authorized access to FTI must meet background check requirements defined in IRS Publication 1075. The contractor will maintain a list of officers or employees authorized access to FTI. Such list will be provided to the agency and, upon request, to the IRS.
- iii. FTI in hardcopy or electronic format shall be used only for the purpose of carrying out the provisions of this contract. FTI in any format shall be treated as confidential and shall not be divulged or made known in any manner to any person except as may be necessary in the performance of this contract. Inspection or disclosure of FTI to anyone other than the contractor or the contractor's officers or employees authorized is prohibited.
- iv. FTI will be accounted for upon receipt and properly stored before, during, and after processing. In addition, any related output and products require the same level of protection as required for the source material.
- v. The contractor will certify that FTI processed during the performance of this contract will be completely purged from all physical and electronic data storage with no output to be retained by the contractor at the time the work is completed. If immediate purging of physical and electronic data storage is not possible, the contractor will certify that any FTI in physical or electronic storage will remain safeguarded to prevent unauthorized disclosures.
- vi. Any spoilage or any intermediate hard copy printout that may result during the processing of FTI will be given to the agency. When this is not possible, the contractor will be responsible for the destruction of the spoilage or any intermediate hard copy printouts and will provide the agency with a statement containing the date of destruction, description of material destroyed, and the destruction method.
- vii. All Contractor computer systems receiving, processing, storing, or transmitting FTI must meet the requirements in IRS Publication 1075. To meet functional and assurance requirements, the security features of the environment must provide for the managerial, operational, and technical controls. All security features must be available and activated to protect against unauthorized use of and access to FTI.
- viii. No work involving FTI furnished under this contract will be subcontracted without the prior written approval of the IRS.
- ix. Contractor will ensure that the terms of FTI safeguards described herein are included, without modification, in any approved subcontract for work involving FTI.
- x. To the extent the terms, provisions, duties, requirements, and obligations of this contract apply to performing services with FTI, the contractor shall assume toward the subcontractor all obligations, duties and responsibilities that the agency under this contract assumes toward the contractor, and the subcontractor shall assume toward the contractor all the same obligations, duties and responsibilities which the contractor assumes toward the agency under this contract.

- xi. In addition to the subcontractor's obligations and duties under an approved subcontract, the terms and conditions of this contract apply to the subcontractor, and the subcontractor is bound and obligated to the contractor hereunder by the same terms and conditions by which the contractor is bound and obligated to the agency under this contract.
- xii. For purposes of this contract, the term "contractor" includes any officer or employee of the contractor with access to or who uses FTI, and the term "subcontractor" includes any officer or employee of the subcontractor with access to or who uses FTI.
- xiii. The agency will have the right to void the contract if the contractor fails to meet the terms of FTI safeguards described herein.

b. CRIMINAL/CIVIL SANCTIONS

- i. Each officer or employee of a contractor to whom FTI is or may be disclosed shall be notified in writing that FTI disclosed to such officer or employee can be used only for a purpose and to the extent authorized herein, and that further disclosure of any FTI for a purpose not authorized herein constitutes a felony punishable upon conviction by a fine of as much as \$5,000 or imprisonment for as long as 5 years, or both, together with the costs of prosecution.
- ii. Each officer or employee of a contractor to whom FTI is or may be accessible shall be notified in writing that FTI accessible to such officer or employee may be accessed only for a purpose and to the extent authorized herein, and that access/inspection of FTI without an official need-to-know for a purpose not authorized herein constitutes a criminal misdemeanor punishable upon conviction by a fine of as much as \$1,000 or imprisonment for as long as 1 year, or both, together with the costs of prosecution.
- iii. Each officer or employee of a contractor to whom FTI is or may be disclosed shall be notified in writing that any such unauthorized access, inspection or disclosure of FTI may also result in an award of civil damages against the officer or employee in an amount equal to the sum of the greater of \$1,000 for each unauthorized access, inspection, or disclosure, or the sum of actual damages sustained as a result of such unauthorized access, inspection, or disclosure, plus in the case of a willful unauthorized access, inspection, or disclosure or an unauthorized access/inspection or disclosure which is the result of gross negligence, punitive damages, plus the cost of the action. These penalties are prescribed by IRC sections 7213, 7213A and 7431 and set forth at 26 CFR 301.6103(n)-1.
- iv. Additionally, it is incumbent upon the contractor to inform its officers and employees of the penalties for improper disclosure imposed by the Privacy Act of 1974, 5 U.S.C. 552a. Specifically, 5 U.S.C. 552a(i)(1), which is made applicable to contractors by 5 U.S.C. 552a(m)(1), provides that any officer or employee of a contractor, who by virtue of his/her employment or official position, has possession of or access to agency records which contain individually identifiable information, the disclosure of which is prohibited by the Privacy Act or regulations established thereunder, and who knowing that disclosure of the specific material is so prohibited, willfully discloses the material

in any manner to any person or agency not entitled to receive it, shall be guilty of a misdemeanor and fined not more than \$5,000.

- v. Granting a contractor access to FTI must be preceded by certifying that each officer or employee understands the agency's security policy and procedures for safeguarding FTI. A contractor and each officer or employee must maintain their authorization to access FTI through annual recertification of their understanding of the agency's security policy and procedures for safeguarding FTI. The initial certification and recertifications must be documented and placed in the agency's files for review. As part of the certification and at least annually afterwards, a contractor and each officer or employee must be advised of the provisions of IRC sections 7213, 7213A, and 7431 (see IRS Publication 1075, Exhibit 4, Sanctions for Unauthorized Disclosure, and IRS Publication 1075, Exhibit 5, Civil Damages for Unauthorized Disclosure). The training on the agency's security policy and procedures provided before the initial certification and annually thereafter must also cover the incident response policy and procedure for reporting unauthorized disclosures and data breaches. For the initial certification and the annual recertifications, the contractor and each officer or employee must sign, either with ink or electronic signature, a confidentiality statement certifying their understanding of the security requirements.

c. INSPECTION: The IRS and the Agency, with 24 hour notice, shall have the right to send its inspectors into the offices and plants of the contractor to inspect facilities and operations performing any work with FTI under this contract for compliance with requirements defined in IRS Publication 1075. The IRS' right of inspection shall include the use of manual and/or automated scanning tools to perform compliance and vulnerability assessments of information technology (IT) assets that access, store, process or transmit FTI. Based on the inspection, corrective actions may be required in cases where the contractor is found to be noncompliant with FTI safeguard requirements.

5. SSA Requirements (If applicable)

- a. PERFORMANCE: If Contractor takes possession or control of in SSA provided information in the performance of this contract, the contractor agrees to, where applicable and to the extent within Contractor's control comply with and assume responsibility for compliance by his or her employees with the following requirements:
 - i. All work will be done under the supervision of the State of Oklahoma.
 - ii. Any SSA provided information made available shall be used only for carrying out the provisions of this Agreement. Information contained in such material shall be treated as confidential and shall not be divulged or made known in any manner to any person except as may be necessary in the performance of this contract. Inspection by or disclosure to anyone other than an officer or employee of the Contractor is prohibited.
 - iii. All SSA provided information shall be accounted for upon receipt and properly stored before, during, and after processing. In addition, all related output and products will be given the same level of protection as required for the source material.

- iv. No work involving SSA provided information furnished under this contract shall be subcontracted without prior written approval by the applicable State of Oklahoma agency and the SSA.
- v. The Contractor shall maintain a list of employees authorized access. Such list shall be provided upon request to the applicable State of Oklahoma agency or the SSA.
- vi. Contractor or agents may not legally process, transmit, or store SSA-provided information in a cloud environment without explicit permission from SSA's Chief Information Officer. Proof of this authorization shall be provided to the Contractor by the applicable State of Oklahoma agency prior to accessing SSA provided information.
- vii. Contractor shall provide security awareness training to all employees, contractors, and agents who access SSA-provided information. The training should be annual, mandatory, and certified by the personnel who receive the training. Contractor is also required to certify that each employee, contractor, and agent who views SSA-provided information certify that they understand the potential criminal, civil, and administrative sanctions or penalties for unlawful assess and/or disclosure.
- viii. Contractor shall require employees, contractors, and agents to sign a non-disclosure agreement, attest to their receipt of Security Awareness Training, and acknowledge the rules of behavior concerning proper use and security in systems that process SSA-provided information. Contractor shall retain non-disclosure attestations for at least five (5) to seven (7) years for each employee who processes, views, or encounters SSA-provided information as part of their duties.
- ix. The applicable State of Oklahoma agency shall provide the Contractor a copy of the SSA exchange agreement and all related attachments before initial disclosure of SSA data. Contractor is required to follow the terms of the applicable State of Oklahoma agency's data exchange agreement with the SSA. Prior to signing this Agreement, and thereafter at SSA's request, the applicable State of Oklahoma agency shall obtain from the Contractor a current list of the employees of such Contractor with access to SSA data and provide such list to the SSA.
- x. Where the Contractor processes, handles, or transmits information provided to the applicable State of Oklahoma agency by SSA or has authority to perform on the agency's behalf, the applicable State of Oklahoma agency shall clearly state the specific roles and functions of the Contractor within the Agreement.
- xi. SSA requires all parties subject to this Agreement to exercise due diligence to avoid hindering legal actions, warrants, subpoenas, court actions, court judgments, state or Federal investigations, and SSA special inquiries for matters pertaining to SSA-provided information.
- xii. SSA requires all parties subject to this Agreement to agree that any Client-owned or subcontracted facility involved in the receipt, processing, storage, or disposal of SSA-provided information operate as a "de facto" extension of the Client and is subject to onsite inspection and review by the Client or SSA with prior notice.

- xiii. If the Contractor must send a Contractor computer, hard drive, or other computing or storage device offsite for repair, the Contractor must have a non-disclosure clause in their contract with the vendor. If the Contractor used the item in a business process that involved SSA-provided information and the vendor will retrieve or may view SSA-provided information during servicing, SSA reserves the right to inspect the Contractor's vendor contract. The Contractor must remove SSA-provided information from electronic devices before sending it to an external vendor for service. SSA expects the Contractor to render SSA-provided information unrecoverable or destroy the electronic device if they do not need to recover the information. The same applies to excessed, donated, or sold equipment placed into the custody of another organization.
 - xiv. In the event of a suspected or verified data breach involving SSA provided information, the Contractor shall notify the Client immediately.
 - xv. The Client shall have the right to void the contract if the contractor fails to provide the safeguards described above.
- b. **CRIMINAL/CIVIL SANCTIONS:** The Act specifically provides civil remedies, 5 U.S.C. Sec. 552a(g), including damages, and criminal penalties, 5 U.S.C. Sec. 552a(i), for violations of the Act. The civil action provisions are premised violations of the Act committed by parties subject to this Agreement or regulations promulgated thereunder. An individual claiming such a violation by parties subject to this Agreement may bring civil action in a federal district court. If the individual substantially prevails, the court may assess reasonable attorney fees and other litigation costs. In addition, the court may direct the parties subject to this Agreement to grant the plaintiff access to his/her records, and when appropriate direct an amendment or correction of records subject to the Act. Actual damages may be awarded to the plaintiff for intentional or willful refusal by parties subject to this Agreement to comply with the Act.
- i. **Civil Remedies.**
 - (1) In any suit brought under the provisions of 5 U.S.C. § 552a(g)(1)(C) or (D) in which the court determines that the parties subject to this Agreement acted in a manner which was intentional or willful, shall be liable in an amount equal to the sum of —
 - (a) actual damages sustained by the individual because of the refusal or failure, but in no case, shall a person entitled to recovery receive less than the sum of \$1,000; and
 - (b) the costs of the action together with reasonable attorney fees as determined by the court.
 - (2) An action to enforce any liability created under 5 U.S.C. § 552a may be brought in the district court of the United States in the district in which the complainant resides, or has his principal place of business, or in which the records are situated, or in the District of Columbia, without regard to the amount in controversy, within two years from the date on which the cause of action arises, except that where

parties subject to this Agreement have materially and willfully misrepresented any information required under this section to be disclosed to an individual and the information so misrepresented is material to establishment of the liability of the agency to the individual under 5 U.S.C. § 552a, the action may be brought at any time within two years after discovery by the individual of the misrepresentation. Nothing in this section shall be construed to authorize any civil action because of any injury sustained as the result of a disclosure of a record prior to September 27, 1975.

ii. Criminal Penalties

- (1) Any officer or employee of an agency, who by virtue of his employment or official position, has possession of, or access to, agency records which contain individually identifiable information the disclosure of which is prohibited by this section or by rules or regulations established thereunder, and who knowing that disclosure of the specific material is so prohibited, willfully discloses the material in any manner to any person or agency not entitled to receive it, shall be guilty of a misdemeanor and fined not more than \$5,000. See 5 U.S.C. § 552a(i)(1).
- (2) Any officer or employee of any agency who willfully maintains a system of records without meeting the notice requirements of subsection (e)(4) of this section shall be guilty of a misdemeanor and fined not more than \$5,000. See 5 U.S.C. § 552a(i)(2).
- (3) Any person who knowingly and willfully requests or obtains any record concerning an individual from an agency under false pretenses shall be guilty of a misdemeanor and fined not more than \$5,000. See 5 U.S.C. § 552a(i)(3).

6. Child Support FPLS Requirements (If applicable)

- a. Contractor, when applicable and to the extent within Contractor's control, and the applicable State of Oklahoma agency must comply with the security requirements established by the Social Security Act, the Privacy Act of 1974, the Federal Information Security Management Act of 2002 (FISMA), 42 United States Code (USC) 654(26), 42 UCS 654a(d)(1)-(5), the U.S. Department of Health and Human Services (HHS), the U.S. Department of Health and Human Services Administration of Children and Families Office of Child Support Enforcement Security Agreement and the Automated Systems for Child Support Enforcement: A Guide for States Section H Security and Privacy. Contractor and applicable State of Oklahoma agency also agree to use Federal Parent Locator Service (FPLS) information and Child Support (CS) program information solely for the authorized purposes in accordance with the terms in this agreement. The information exchanged between state Child Support agencies and all other state program information must be used for authorized purposes and protected against unauthorized access to reduce fraudulent activities and protect the privacy rights of individuals against unauthorized disclosure of confidential information.

- i. This is applicable to the personnel, facilities, documentation, data, electronic and physical records and other machine-readable information systems of the applicable State of Oklahoma agency and Contractor, including, but not limited to, state employees and contractors working with FPLS information and CS program information and state CS agency data centers, statewide centralized data centers, contractor data centers, state Health and Human Services' data centers, comprehensive tribal agencies, data centers serving comprehensive tribes, and any other individual or entity collecting, storing, transmitting or processing FPLS information and CS program information. This is applicable to all FPLS information, which consists of the National Directory of New Hires (NDNH), Debtor File, and the Federal Case Registry (FCR). The NDNH, Debtor File and FCR are components of an automated national information system.
- ii. This is also applicable to all CS program information, which includes the state CS program information, other state and tribal program information, and confidential information. Confidential information means any information relating to a specified individual or an individual who can be identified by reference to one or more factors specific to him or her, including but not limited to the individual's Social Security number, residential and mailing addresses, employment information, and financial information. Ref. 45 Code of Federal Regulations (CFR) 303.21(a).

7. FERPA Requirements (If applicable)

- a. If Contractor takes possession or control of Information covered by FERPA in performance of this Agreement, Contractor agrees to, when applicable and to the extent within Contractor's control comply with and assume responsibility for compliance by its employees with the Family Educational Rights and Privacy Act; (20 U.S.C. § 1232g; 34 CFR Part 99) ("FERPA") and the Oklahoma Student Data Accessibility, Transparency, and Accountability Act of 2013; (70 O.S. § 3-168), where personally identifiable student education data is exchanged.

8. CJIS Requirements (If applicable)

a. INTRODUCTION

This section shall be applicable to the extent that Contractor takes possession or control of CJIS data. The use and maintenance of all items of software or equipment offered for purchase herein must be in compliance with the most current version of the U.S. Department of Justice, Federal Bureau of Investigation ("FBI"), Criminal Justice Information Services (CJIS) Division's CJIS Security Policy ("CJIS Security Policy" or "Security Policy" herein).

The Entity or Affiliate acquiring the data or system is hereby ultimately responsible for compliance with the CJIS Security Policy and will be subject to an audit by the State of Oklahoma CJIS Systems Officer ("CSO") and the FBI CJIS Division's Audit Staff.

b. CJIS SECURITY POLICY REQUIREMENTS GENERALLY

The CJIS Security Policy outlines a number of administrative, procedural, and technical controls agencies must have in place to protect Criminal Justice Information (“CJI”). Our experience is that agencies will generally have many of the administrative and procedural controls in place but will need to implement additional technical safeguards in order to be in complete compliance with the mandate. A Criminal Justice Agency (“CJA”) and certain other governmental agencies procuring technology equipment and services that could be used in hosting or connecting or transmitting or receiving CJI data may need to use the check list herein to make sure that the software, equipment, location, security, and persons having the ability to access CJI will meet the CJIS requirements per the then current CJIS Security Policy. A completed Appendix H to said Security Policy will need to be signed by Vendor or a 3rd party if it has access to CJI, such as incident to the maintenance or support of the purchased hardware or software within which resides CJI. Per Appendix “A” to said Security Policy, “access to CJI is the physical or logical (electronic) ability, right or privilege to view, modify or make use of CJI.”

c. DIRECTIVE CONCERNING ACCESS TO CRIMINAL JUSTICE INFORMATION AND TO HARDWARE OR SOFTWARE WHICH INTERACTS WITH CJI AND CERTIFICATION

The FBI CJIS Division provides state-of-the-art identification and information services to the local, state, tribal, federal, and international criminal justice communities for criminal justice purposes, as well as the noncriminal justice communities for noncriminal justice purposes.

This Directive primarily concerns access to CJI and access to hardware and software in the use, retention, transmission, reception, and hosting of CJI for criminal justice purposes and not for noncriminal justice purposes. In that regard, this Directive is not only applicable to such data, but also to the hardware and software interacting with such data, their location(s), and persons having the ability to access such data. The CJIS data applicable to the Security Policy is the data described as such in said Policy plus all data transmitted over the Oklahoma Law Enforcement Telecommunications System (“OLETS”) which is operated by DPS.

In order to have access to CJI or to the aforesaid hardware or software, the vendor must be familiar with the FBI CJIS Security Policy, including but not limited to the following portions of said Security Policy:

1. the Definitions and Acronyms in §3 & Appendices “A” & “B”;

2. the general policies in §4;
3. the Policies in §5;
4. the appropriate forms in Appendices “D”, “E”, “F” & “H”; and
5. the Supplemental Guidance in Appendices “J” & “K”.

This FBI Security Policy is located and may be downloaded at:
<https://www.fbi.gov/services/cjis/cjissecurity-policy-resource-center>.

By executing the Contract to which this Directive is attached, the vendor hereby CERTIFIES that the foregoing directive has and will be followed, including but not limited to full compliance with the FBI CJIS Security Policy, as amended and as applicable.

ATTACHMENT E1

ADDITIONAL TERMS

Intentionally left blank.

ATTACHMENT E2

MASTER TERMS

Intentionally left blank.

ATTACHMENT E3

PRICING

Exhibit 1**Rattan Consulting Pricing for Bid 0900000556 due 12OCT22**

Rattan Professional Services - Hourly Not-to-Exceed Rates		Rate
Title	Description	
Automation Developer	A member of the Centers of Excellence Team that uses the development tools to turn automation ideas into reality.	\$150.00
Solutions Architect	Translates the requirements captured by the analyst, creating the architecture and design artifacts, and overseeing the development.	\$230.00
Business Analyst	Responsible for mapping the AS IS and proposed TO BE business processes.	\$150.00
Project Manager	Sets up and manages the team working on an automation initiative.	\$175.00
Infrastructure Engineer	Responsible for setting up and maintaining the hardware and software resources for the automation development, deployment, and maintenance.	\$155.00
RPA Developer	Professionally trained to code and create automations that distributed throughout the organization.	\$150.00

Software Publishers		
Product Name	Description	Cost
Standard (FLEX)		
UIPath - Flex - Action Center - Named User	Action Center enables efficient process handoff between robots and humans. The Flex Action Center offering includes delivery of Action Center and Apps from Automation Cloud (SaaS), Automation Suite or Standalone Orchestrator (availability and configuration may vary by service). It also includes one locally-installed Task Capture license, a tool that enables employees to quickly document step-by-step processes and provides 3,000 Integration Service API calls/month from Automation Cloud (SaaS). Licenses one named user.	\$440
UIPath - Flex - Attended - Named User	This offering includes an Attended Robot, locally-installed, with orchestration from Automation Cloud (SaaS), Automation Suite or Standalone Orchestrator. The Attended Robot allows a user to access, manage, and run automations. It includes the Apps and Action Center services, which may be delivered and orchestrated from Automation Cloud (SaaS), Automation Suite or Standalone Orchestrator (availability and configuration may vary by service). It also includes one locally-installed Task Capture license, a tool that enables employees to quickly document step-by-step processes and provides 3,000 Integration Service API calls/month from Automation Cloud (SaaS). Licenses one named user.	\$1,600
UIPath - Flex - Citizen Developer - Named User	This offering includes one Attended Robot and one StudioX, each locally-installed. These may be orchestrated from Automation Cloud (SaaS), Automation Suite or Standalone Orchestrator. StudioX is an automation design tool that allows the business user to rapidly automate their business apps without the need for developer resources or coding, bringing automation to the masses. It includes the Apps and Action Center services, which may be delivered and orchestrated from Automation Cloud (SaaS), Automation Suite or Standalone Orchestrator (availability and configuration may vary by service). It also includes one locally-installed Task Capture license, a tool that enables employees to quickly document step-by-step processes and provides 3,000 Integration Service API calls/month from Automation Cloud (SaaS). Finally, it includes the use of a Serverless Automation Cloud Robot for debugging purposes (up to 4 hours execution time per day). Licenses one named user.	\$2,600
UIPath - Flex - Automation Developer - Named User	This offering includes one Attended Robot and one Studio or StudioX, each locally-installed. These may be orchestrated from Automation Cloud (SaaS), Automation Suite or a Standalone Orchestrator. Studio is an automation design tool that allows developers full control over automations with advanced activities, powerful debugging tools, team development support and integrated testing. It includes the following services: Test Management, Apps, and Action Center, which may be delivered and orchestrated from Automation Cloud (SaaS), Automation Suite, or Standalone Orchestrator (availability and configuration may vary by service). It also includes one locally-installed Task Capture license, a tool that enables employees to quickly document step-by-step processes and provides 5,000 Integration Service API calls/month from Automation Cloud (SaaS). Finally, it includes the use of a Serverless Automation Cloud Robot for debugging purposes (up to 4 hours execution time per day). Licenses one named user.	\$4,400
UIPath - Flex - Process Mining Developer - Named User	This offering includes one Attended Robot, one Studio or StudioX license and one Process Mining Developer, each locally installed. These may be orchestrated from Automation Cloud (SaaS), Automation Suite or Standalone Orchestrator. Studio is an automation design tool that allows developers full control over automations with advanced activities, powerful debugging tools, team development support and integrated testing. It includes the following services: Test Management, Apps, and Action Center, which may be delivered and orchestrated from Automation Cloud (SaaS), Automation Suite, or Standalone Orchestrator (availability and configuration may vary by service). It also includes one locally-installed Task Capture license, a tool that enables employees to quickly document step-by-step processes and provides 5,000 Integration Service API calls/month from Automation Cloud (SaaS). Finally, it includes the use of a Serverless Automation Cloud Robot for debugging purposes (up to 4 hours execution time per day). Licenses one named user.	\$6,500
UIPath - Flex - Process Mining Business User - Named User	Process Mining Business User gives users the ability to continuously monitor their end-to-end processes, to discover how to optimize them, and to prioritize their automations based on the impact they will have on their most important KPIs. This offering includes Process Mining view access, delivered via Automation Cloud (SaaS) or Standalone Server. It also includes one locally-installed Task Capture license, a tool that enables employees to quickly document step-by-step processes. The Action Center service is also included, and can be delivered from Automation Cloud (SaaS), Automation Suite or Standalone Orchestrator (availability and configuration may vary by service). Licenses one named user.	\$900
UIPath - Flex - Tester - Named User	This offering provides annual access to comprehensive test management. It includes access to UIPath Test Management, to manage requirements, design test cases and integrate with ALM tooling, which can be delivered and orchestrated from Automaton Cloud (SaaS), Automation Suite or Standalone Orchestrator. Requires UIPath Test Management. It also includes one locally-installed Task Capture license, a tool that enables employees to quickly document step-by-step processes. Licenses one named user.	\$900
UIPath - Flex - Insights - 50 Designer Users Add-on	Insights provides powerful, embedded analytics for measuring and reporting on RPA operations and business definable KPIs. The Flex Insights 50 Designer users add-on provides an additional 50 Designer Users needed to build and customize dashboards. This add-on requires the Flex Insights SKU. This SKU includes Orchestration and delivery from Automation Cloud (SaaS) or Automation Suite, or standalone installation (availability and configuration may vary).	\$9,000
UIPath - Flex - Attended - US Public Sector - Named User	Automation Cloud Public Sector is a secure cloud service for RPA that is currently FedRAMP "In Process" and undergoing FedRAMP assessment. The service is operated by US Persons on US Soil. This offering includes an Attended Robot, locally-installed, with orchestration from Automation Cloud Public Sector (GovCloud), Automation Suite or Standalone Orchestrator. The Attended Robot allows a user to access, manage, and run automations. It includes the Apps and Action Center services, which may be delivered and orchestrated from Automation Cloud Public Sector (GovCloud), Automation Suite or Standalone Orchestrator (availability and configuration may vary by service). It also includes one locally-installed Task Capture license, a tool that enables employees to quickly document step-by-step processes and provides 3,000 Integration Service API calls/month from Automation Cloud Public Sector (GovCloud). Licenses one named user.	\$2,000
UIPath - Flex - Citizen Developer - US Public Sector - Named User	Automation Cloud Public Sector is a secure cloud service for RPA that is currently FedRAMP "In Process" and undergoing FedRAMP assessment. The service is operated by US Persons on US Soil. This offering includes one Attended Robot and one StudioX, each locally-installed. These may be orchestrated from Automation Cloud Public Sector (GovCloud), Automation Suite or Standalone Orchestrator. StudioX is an automation design tool that allows the business user to rapidly automate their business apps without the need for developer resources or coding, bringing automation to the masses. It includes the Apps and Action Center services, which may be delivered and orchestrated from Automation Cloud Public Sector (GovCloud), Automation Suite or Standalone Orchestrator (availability and configuration may vary by service). It also includes one locally-installed Task Capture license, a tool that enables employees to quickly document step-by-step processes and provides 3,000 Integration Service API calls/month from Automation Cloud Public Sector (GovCloud). Licenses one named user.	\$3,300
UIPath - Flex - Automation Developer - US Public Sector - Named User	Automation Cloud Public Sector is a secure cloud service for RPA that is currently FedRAMP "In Process" and undergoing FedRAMP assessment. The service is operated by US Persons on US Soil. This offering includes one Attended Robot and one Studio or StudioX, each locally-installed. These may be orchestrated from Automation Cloud Public Sector (GovCloud), Automation Suite or a Standalone Orchestrator. Studio is an automation design tool that allows developers full control over automations with advanced activities, powerful debugging tools, team development support and integrated testing. It includes the following services: Test Management, Apps, and Action Center, which may be delivered and orchestrated from Automation Cloud Public Sector (GovCloud), Automation Suite, or Standalone Orchestrator (availability and configuration may vary by service). It also includes one locally-installed Task Capture license, a tool that enables employees to quickly document step-by-step processes and provides 5,000 Integration Service API calls/month from Automation Cloud Public Sector (GovCloud). Licenses one named user.	\$5,500

UiPath - Flex - Unattended Robot	This offering includes one customer-hosted Unattended Robot that independently executes automations. It can be orchestrated from Automation Cloud (SaaS), Automation Suite, or Standalone Orchestrator. The Unattended Robot runs on a virtual desktop, in a secure session, end-to-end, without human intervention. It performs the process end to end, 'lights out' - working business transactions with the help of an RPA work queue. It also includes 5,000 Integration Service API calls/month from Automation Cloud (SaaS). Licenses one robot.	\$10,000
UiPath - Flex - Unattended Robot - Test	This offering includes a customer-hosted Test Robot which can be orchestrated from Automation Cloud (SaaS), Automation Suite or Standalone Orchestrator. It also includes 3,000 Integration Service API calls/month from Automation Cloud (SaaS). Licenses one robot.	\$2,000
UiPath - Flex - Unattended Robot - Non-Production	This offering includes one customer-hosted Unattended Robot that independently executes automations. It can be orchestrated from Automation Cloud (SaaS), Automation Suite, or Standalone Orchestrator. The Unattended Robot runs on a virtual desktop, in a secure session, end-to-end, without human intervention. It performs the process end to end, 'lights out' - working business transactions with the help of an RPA work queue. It also includes 3,000 Integration Service API calls/month from Automation Cloud (SaaS). Licenses one robot. Limited to non-production use.	\$550
UiPath - Flex - Unattended Robot - US Public Sector	Automation Cloud Public Sector is a secure cloud service for RPA that is currently FedRAMP "In Process" and undergoing FedRAMP assessment. The service is operated by US Persons on US Soil. This offering includes one customer-hosted Unattended Robot that independently executes automations. It can be orchestrated from Automation Cloud Public Sector (GovCloud), Automation Suite, or Standalone Orchestrator. The Unattended Robot runs on a virtual desktop, in a secure session, end-to-end, without human intervention. It performs the process end to end, 'lights out' - working business transactions with the help of an RPA work queue. It also includes 5,000 Integration Service API calls/month from Automation Cloud Public Sector (GovCloud). Licenses one robot.	\$12,000
UiPath - Flex - Unattended Robot - Non-Production - US Public Sector	Automation Cloud Public Sector is a secure cloud service for RPA that is currently FedRAMP "In Process" and undergoing FedRAMP assessment. The service is operated by US Persons on US Soil. This offering includes one customer-hosted Unattended Robot that independently executes automations. It can be orchestrated from Automation Cloud Public Sector (GovCloud), Automation Suite, or Standalone Orchestrator. The Unattended Robot runs on a virtual desktop, in a secure session, end-to-end, without human intervention. It performs the process end to end, 'lights out' - working business transactions with the help of an RPA work queue. It also includes 3,000 Integration Service API calls/month from Automation Cloud Public Sector (GovCloud). Licenses one robot. Limited to non-production use.	\$700
UiPath - Flex - Automation Hub	Automation Hub enables organizations to manage the entire automation lifecycle with instant transparency and control. With Automation Hub, organizations can discover, prioritize, and track automation ideas in one place, and easily scale their automation programs. An unlimited number of users is included for every Automation Hub instance. It also includes unlimited enterprise production licenses of Task Capture, a separately downloaded tool that enables employees to quickly document step-by-step processes. This SKU allows delivery from Automation Cloud (SaaS) or Automation Suite. Includes additional use of up to 3 non-production instances for Customer-hosted Automation Suite or standalone installation.	\$9,000
UiPath - Flex - AI Unit Bundle - 60K	AI Center is a machine learning platform and enables customers to deploy, manage and train Machine Learning (ML) models, including Task Mining, Document Understanding, Computer Vision, out-of-the-box (OOTB) models provided by UiPath/UiPath Marketplace, and customer's own ML models. This SKU contains a bundle of 60,000 AI Units to be used within AI Center either hosted by UiPath in Automation Cloud or hosted by the customer in Automation Suite.	\$12,000
UiPath - Flex - AI Unit Bundle - 1M	AI Center is a machine learning platform and enables customers to deploy, manage and train Machine Learning (ML) models, including Task Mining, Document Understanding, Computer Vision, out-of-the-box (OOTB) models provided by UiPath/UiPath Marketplace, and customer's own ML models. This SKU contains a bundle of 1,000,000 AI Units to be used within AI Center either hosted by UiPath in Automation Cloud or hosted by Customer in Automation Suite.	\$150,000
UiPath - Flex - AI Unit Bundle - 10M	AI Center is a machine learning platform and enables customers to deploy, manage and train Machine Learning (ML) models, including Task Mining, Document Understanding, Computer Vision, out-of-the-box (OOTB) models provided by UiPath/UiPath Marketplace, and customer's own ML models. This SKU contains a bundle of 10,000,000 AI Units to be used within AI Center either hosted by UiPath in Automation Cloud or hosted by the customer in Automation Suite.	\$1,000,000
UiPath - Flex - Insights	Insights provides powerful, embedded analytics for measuring and reporting on RPA operations and business definable KPIs. Flex Insights is licensed per Automation Cloud or Automation Suite organization. It includes 10 Designer Users and unlimited Viewer Users. Includes additional use of up to 3 non-production instances for Customer-hosted Automation Suite or standalone installation. This SKU allows delivery from Automation Cloud (SaaS), Automation Suite or Standalone Orchestrator.	\$15,000
UiPath - Flex - Integration Service API Calls Bundle - 6M	The UiPath Integration Service delivers the tools and flexibility to solve any automation challenge, faster and at scale allowing developers to seamlessly use UIs and APIs in a single automation. This SKU contains a bundle of 6,000,000 API calls from Automation Cloud (SaaS).	\$20,000
UiPath - Flex - Integration Service API Calls Bundle - 3M	The UiPath Integration Service delivers the tools and flexibility to solve any automation challenge, faster and at scale allowing developers to seamlessly use UIs and APIs in a single automation. This SKU contains a bundle of 3,000,000 API calls from Automation Cloud (SaaS).	\$12,000
UiPath - Flex - Test Management	This offering provides access to UiPath Test Management - a central service that supports requirements management, test case design and integration with ALM tooling. User access to this capability is entitled via either the Flex - Automation Developer or Flex - Tester offerings. This SKU allows delivery from Automation Cloud (SaaS), Automation Suite or standalone Orchestrator.	\$9,000
UiPath - Flex - Computer Vision	Computer Vision is a machine-learning based method used to locate screen elements and operate user interfaces. Technically, it's a class of "surface automation" tools, because it doesn't require or use the underlying properties of applications, but only the aspect and relationship of various screen elements. CV is a set of Studio activities, that require a ML server. By default our UiPath cloud server is used. This SKU includes flexible delivery via Automation Cloud (SaaS), Automation Suite, or standalone installation (availability and configuration may vary by service).	\$0
UiPath - Flex - Process Mining Rows Bundle - 20M	The Process Mining offering includes access to Process Mining capabilities and entitles up to 20,000,000 Rows of Process Mining Capacity in cloud, or a standalone Process Mining server (availability and configuration may vary by service). Process Mining gives users the ability to continuously monitor their end-to-end processes, to discover how to optimize them, and to prioritize automation opportunities based on the impact they will have on their most important KPIs. Includes additional use of up to 3 non-production instances for standalone installation upon request.	\$30,000
UiPath - High Availability Add-On	For each deployment of the UiPath Platform that requires Multi-Node, High Availability, Disaster Recovery or Active-Active scenarios for Standalone Orchestrator or Automation Suite the High Availability Add-on is required. It offers enterprise grade security, professional grade caching and UiPath support. Includes additional use of up to 3 non-production instances for Customer-hosted Automation Suite or standalone installation.	\$25,000
UiPath - Flex - Test Suite Starter Pack	The Test Suite Starter Pack offering includes 1 x Flex - Test Management, 3 x Flex - Automation Developer, 5 x Flex - Tester and 5 x Flex - Unattended Robot - Test. These can be orchestrated and delivered from Automation Cloud (SaaS), Automation Suite or Standalone Orchestrator (availability and configuration may vary by service). It delivers a test solution combining the world's leading automation technology with best-of-breed testing capabilities to ensure application and automation quality across an enterprise. Robots are for test purposes only. Each Automation Developer and Tester is a single named user.	\$29,000
UiPath - Flex - App Testing Starter Pack	The App Testing Starter Pack offering includes 1 x Flex - Test Management and 5 x Flex - Testers. These may be orchestrated from Automation Cloud (SaaS), Automation Suite or Standalone Orchestrator (availability and configuration may vary by service). It delivers a test solution combining the world's leading automation technology with best-of-breed testing capabilities to ensure application and automation quality across an enterprise. Each Tester is a single named user.	\$11,000
UiPath - Flex - Starter Pack - Standard	The Starter Pack - Standard offering includes 1 x Flex - Automation Hub, 1 x Flex - Test Management, 4 x Flex - Automation Developer, 4 x Flex - Unattended Robot - Test. It also includes Flex - Citizen Developer (0-20), Flex - Attended (0-32), and Flex - Unattended Robot (0-5) which are configurable based on standard options as required. These can be orchestrated and delivered from Automation Cloud (SaaS), Automation Suite or Standalone Orchestrator (availability and configuration may vary by service). This pack offers everything needed to automate and test with the UiPath Platform. Each Automation Developer, Citizen Developer and Attended is a single named user.	\$77,000

UiPath - Flex - Starter Pack - Advanced	The Starter Pack - Advanced includes 1 x Flex - Test Management, 1 x Flex - Automation Hub, 8 x Flex - Automation Developers, 8 x Flex - Unattended Robot - Test, 1 x Flex - Insights. It also includes Flex - Citizen Developer (0-40), Flex - Attended (0-67), and Flex - Unattended Robot (0-10) are configurable based on standard options as required. These can be orchestrated and delivered from Automation Cloud (SaaS), Automation Suite or Standalone Orchestrator (availability and configuration may vary by service). This pack contains everything needed to automate and measure with the UiPath Platform at scale. Each Automation Developer, Citizen Developer and Attended is a single named user.	\$147,000
UiPath - Flex - Starter Pack - Basic	The Starter Pack - Basic includes 2 x Flex - Automation Developers, 2 x Flex - Unattended Robot - Non-Production. It also includes Flex - Citizen Developer (0-14), Flex - Attended (0-19), and Flex - Unattended Robots (0-3) which are configurable based on standard options as required. These can be orchestrated and delivered from Automation Cloud (SaaS), Automation Suite or Standalone Orchestrator (availability and configuration may vary by service). This pack contains all the essentials needed to start automating with the UiPath Platform. Each Automation Developer, Citizen Developer and Attended is a single named user.	\$37,000
UiPath - Flex - Enterprise Foundation Pack	The Enterprise Foundation Pack includes 1 x Flex - Automation Hub, 1 x Flex - Test Management, 1 x Flex - Process Mining Rows Bundle - 20M, 1 x Flex - Insights, 2 x Flex - AI Unit Bundle - 60K. This pack contains products and services needed to start automating at enterprise scale and it can be delivered from Automation Cloud (SaaS), Automation Suite or Standalone Orchestrator (availability and configuration may vary by service).	\$77,000
UiPath - Flex - Process Mining Starter Pack	The Process Mining Starter Pack includes 5 x Flex - Process Mining Rows Bundle - 20M, 2x Flex - Process Mining Developer, 20x Flex - Process Mining Business User. This pack contains products and services needed to start automating at enterprise scale and it can be delivered from Automation Cloud (SaaS), Automation Suite or Standalone Orchestrator (availability and configuration may vary by service).	\$150,000
UiPath - Flex - Hyperautomation Bundle - 250 Users	Access to the UiPath Platform for 250 users within the following limits: up to 250 total of any flex - user type; up to 50 locally-installed Flex - Unattended Robot; up to 50 locally installed of any of the Flex - Unattended Robot - Test or Flex - Unattended Robot - Non-Production; up to 10 Flex - AI Unit Bundle - 60K; 1 x Flex - Integration Service API Calls Bundle - 6M and 1 x Flex - Process Mining Rows Bundle - 20M as well as Unlimited Flex - Insights, Flex - Test Management, Flex - Automation Hub, High Availability Add-On. This SKU includes orchestration and delivery from Automation Cloud (SaaS), Automation Suite, or Standalone Orchestrator (availability and configuration may vary by service).	\$800,000
UiPath - Flex - Hyperautomation Bundle - 500 Users	Access to the UiPath Platform for 500 users within the following limits: up to 500 total of any flex - user type; up to 100 locally-installed Flex - Unattended Robot; up to 100 locally installed of any of the Flex - Unattended Robot - Test or Flex - Unattended Robot - Non-Production; up to 15 Flex - AI Unit Bundle - 60K; 1 x Flex - Integration Service API Calls Bundle - 6M and 1 x Flex - Process Mining Rows Bundle - 20M as well as Unlimited Flex - Insights, Flex - Test Management, Flex - Automation Hub, High Availability Add-On. This SKU includes orchestration and delivery from Automation Cloud (SaaS), Automation Suite, or Standalone Orchestrator (availability and configuration may vary by service).	\$1,350,000
UiPath - Flex - Platform Bundle - NFR	Not for Resale (NFR) UiPath Platform offered for channel partners ONLY. To be used for Partners' own demo environments, PoC labs, and training purposes. Production usage prohibited. Not for Resale/ only 1 YR Term. NFR proposal based benefit, based on approvals for UiPath Business Partners. Products included under this offering as well as services may be orchestrated and delivered from Automation Cloud (SaaS), Automation Suite, or Standalone Orchestrator (availability and configuration may vary by service).	\$0
UiPath - Flex - Task Mining AI Unit Pack	UiPath Task Mining automatically identifies and aggregates employee desktop activities, then applies AI to identify repetitive tasks for process improvements and automation opportunities. Task Mining consumes 5,000 AI Units per analysis. This SKU includes 2x 60k AI Unit Bundles, enough to run 24 analyses. The recording of desktop activities and recomputes do not consume AI Units.	\$24,000
UiPath - Cloud - Robot Units Bundle - 72K	This bundle includes 6,000 Robot Units per month for one year (unused Robot Units do not carry over to the following month). Robot Units purchase Robot capacity on VM or Serverless Automation Cloud Robots hosted by UiPath in Automation Cloud. A VM Cloud Robot is a Windows-based Virtual Machine with an unattended robot, and the number of Robot Units required to reserve a VM Cloud Robot per year varies by configuration. Serverless Cloud Robots are non-persistent Linux-based Robots that run in the UiPath Automation Cloud and accept "cross-platform automation" (Web and API-based) jobs on-demand. Serverless Cloud Robot capacity is purchased per minute of execution time.	\$14,400
UiPath - Flex - Starter Pack - Basic - US Public Sector	Automation Cloud Public Sector is a secure cloud service for RPA that is currently FedRAMP "In Process" and undergoing FedRAMP assessment. The service is operated by US Persons on US Soil. The Starter Pack - Basic includes 2 x Flex - Automation Developers, 2 x Flex - Unattended Robot - Non-Production. It also includes Flex - Citizen Developer (0-14), Flex - Attended (0-19), and Flex - Unattended Robots (0-3) which are configurable based on standard options as required. These can be orchestrated and delivered from Automation Cloud Public Sector (GovCloud), Automation Suite or Standalone Orchestrator (availability and configuration may vary by service). This pack contains all the essentials needed to start automating with the UiPath Platform. Each Automation Developer, Citizen Developer and Attended is a single named user.	\$46,000
UiPath Professional Services & Support		
UiPath Professional Services	UiPath Professional Services	Price on request
UiPath - Premium Support	Customers receive access to 24/7 support, accelerated support SLAs, call center support, root cause analysis for high-impact issues, and preventative care encompassing infrastructure analysis, installation assistance and upgrade assistance.	9.5% of license Net ACV: Minimum \$9.5K
UiPath Premium Plus	Dedicated Technical Support Manager: Customers will receive a dedicated, named engineer to provide guidance and hands-on support through the RPA program lifecycle. Success planning support: UiPath Technical Support Manager will work with customers on a technical and business execution strategy to help ensure the successful deployment and end-user adoption of the RPA Application. 24/7 accelerated technical support availability, helping in faster issue resolutions without adding to co Access to Customer Support Portal as a single interface digital platform for case management self-service, e-resource repository for education, training technical support and interaction with relevant expert.	22% of license Net ACV: Minimum \$55K
UiPath - Learning Partnership	-	Price on request
UiPath - STAR Support Add-on	Designated or dedicated Strategic Advisor will guide the customers on how to scale and operationalize automation adoption to drive measurable business value. This subscription-based service is meant to be fluid to respond to changing priorities and program challenges that arise throughout the course of the automation journey. The Strategic Advisor will assess existing challenges, operational practices, organization's strategic imperatives that can be addressed through automation and highlight key areas for improvement as the program evolves.	19% of license Net ACV: Minimum \$110K
UiPath Training	UiPath Training	Price on request
Cloud		
UiPath - Cloud Orchestrated Action Center - Named User	The Action Center offering includes Task Capture, Action Center and 3000 Integration Service API calls/month. Action Center is a central portal allowing humans and unattended robots to seamlessly collaborate on a process. Licensed per Named User with a minimum sale of 5 users. Orchestrated from the UiPath Automation Cloud, it also includes Includes Automation Suite usage rights for non-SaaS orchestration.	\$440
UiPath - Cloud Orchestrated Action Center - Multiuser	The Action Center offering includes Task Capture, Action Center and 3000 Integration Service API calls/month. Action Center is a central portal allowing humans and unattended robots to seamlessly collaborate on a process. License per Named User with a minimum sale of 5 users. Each Multiuser license adds 3 authorized users. Requires UiPath Multiuser Add-On. Orchestrated from the UiPath Automation Cloud, it also includes Includes Automation Suite usage rights for non-SaaS orchestration.	\$880
UiPath - Cloud Orchestrated Attended - Named User	The Attended offering includes Task Capture, Action Center, an Attended Robot and 3000 Integration Service API calls/month. The Attended Robot is deployed on a desktop and allows a user to access, manage, and run automations. Each Multiuser license adds 3 authorized users. Requires UiPath Multiuser Add-On. Orchestrated from the UiPath Automation Cloud, it also includes Includes Automation Suite usage rights for non-SaaS orchestration.	\$1,600
UiPath - Cloud Orchestrated Attended - Multiuser	The Attended offering includes Task Capture, Action Center, an Attended Robot and 3000 Integration Service API calls/month. The Attended Robot is deployed on a desktop and allows a user to access, manage, and run automations. Each Multiuser license adds 3 authorized users. Requires UiPath Multiuser Add-On. Orchestrated from the UiPath Automation Cloud, it also includes Includes Automation Suite usage rights for non-SaaS orchestration.	\$3,200
UiPath - Cloud Orchestrated Citizen Developer - Named User	The Citizen Developer offering includes Task Capture, Action Center, an Attended Robot, StudioX and 3000 Integration Service API calls/month. StudioX is an automation design tool that allows the business user to rapidly automate their business processes without the need for developer resources or coding, bringing automation to the masses. Licenses a single named user. Orchestrated from the UiPath Automation Cloud, it also includes Includes Automation Suite usage rights for non-SaaS orchestration.	\$2,600

UIPath - Cloud Orchestrated Citizen Developer - Multiuser	The Citizen Developer offering includes Task Capture, Action Center, an Attended Robot, StudioX and 3000 Integration Service API calls/month. StudioX is an automation design tool that allows the business user to rapidly automate their business apps without the need for developer resources or coding, bringing automation to the masses. Each Multiuser license adds 3 authorized users. Requires UIPath Multiuser Add-On. Orchestrated from the UIPath Automation Cloud, it also includes Includes Automation Suite usage rights for non-SaaS orchestration.	
		\$5,200
UIPath - Cloud Automation Developer - Named User	The Automation Developer User includes Task Capture, Action Center, Attended Robot, StudioX, Studio, Test Manager access and 5000 Integration Service API calls/month. Studio is an automation design tool that allows developers full control over automations with advanced activities, powerful debugging tools, team development support and integrated testing. Intended for a single named user. Orchestrated from the UIPath Automation Cloud, it also includes Includes Automation Suite usage rights for non-SaaS orchestration.	
		\$4,400
UIPath - Cloud Automation Developer - Multiuser	The Automation Developer User includes Task Capture, Action Center, Attended Robot, StudioX, Studio, Test Manager access and 5000 Integration Service API calls/month. Studio is an automation design tool that allows developers full control over automations with advanced activities, powerful debugging tools, team development support and integrated testing. Orchestrated from the UIPath Automation Cloud, it also includes Includes Automation Suite usage rights for non-SaaS orchestration. Each Multiuser license adds 3 authorized users. Requires UIPath Multiuser Add-On.	
		\$8,800
UIPath - Cloud Process Mining Business User	The Cloud Process Mining Business User offering includes Action Center, Task Capture and Process Mining access. As a Cloud Process Mining Business User, you gain full transparency into your processes, the ability to customize your Process Mining experience and the power to take actions and identify the most powerful automation opportunities. Cloud Process Mining gives users the ability to continuously monitor their end-to-end processes, to discover how to optimize them, and to prioritize their automations based on the impact they will have on their most important KPIs. Licenses a single named user. Delivered from the UIPath Automation Cloud.	
		\$900
UIPath - Cloud Orchestrated Process Mining Developer - Named User	The Process Mining Developer offering includes Task Capture, Action Center, Attended Robot, StudioX, Studio, Process Mining Development and 5000 Integration Service API calls/month. As a Developer User, you can fully access the design and development functionality of Process Mining, to develop, customize and administer platform apps. Orchestrated from the UIPath Automation Cloud, it also includes Includes Automation Suite usage rights for non-SaaS orchestration.	
		\$6,500
UIPath - Cloud Tester - Named User	UIPath Cloud Tester provides annual access to comprehensive test management. It includes access to UIPath Cloud Test Manager, to manage requirements, design test cases and integrate with ALM tooling. Requires UIPath Cloud Test Manager.	
		\$900
UIPath - Cloud Insights - 50 Designer Users Add-on	Cloud Insights provides powerful, embedded analytics for measuring and reporting on RPA operations and business definable KPIs. This add-on provides an additional 50 Designer Users needed to build and customize dashboards. This add-on requires the Cloud Insights SKU.	
		\$9,000
UIPath - Cloud Orchestrated RPA Developer - Named User	The RPA Developer offering includes Task Capture, Action Center, Attended Robot, StudioX and Studio. Studio is an automation design tool that allows developers full control over automations with advanced activities, powerful debugging tools and team development support. Intended for a single named user. Orchestrated from the UIPath Automation Cloud.	
		\$4,400
UIPath - Cloud Orchestrated RPA Developer - Multiuser	The RPA Developer offering includes Task Capture, Action Center, Attended Robot, StudioX and Studio. Studio is an automation design tool that allows developers full control over automations with advanced activities, powerful debugging tools and team development support. Each Multiuser license adds 3 authorized users. Requires UIPath Multiuser Add-On. Orchestrated from the UIPath Automation Cloud.	
		\$8,800
UIPath - Cloud - AI Robot	An AI Robot is the runtime for serving ML Skills (i.e. making machine learning models available for Robots to make prediction requests to) and for run ML Training Jobs (i.e. training a new model version of new data to improve its accuracy). One AI Robot can serve 2 ML Skills concurrently or run one ML training job concurrently. Delivered from the UIPath Automation Cloud.	
		\$11,000
UIPath - Cloud - AI Robot Pro	An AI Robot Pro is a commercial SKU that includes an AI Robot and an attachable GPU. So if you have made a GPU available in your machine/cluster that AI Fabric is running in, you will be able to utilize that GPU for serving ML Skills or running ML Training jobs. Delivered from the UIPath Automation Cloud.	
		\$23,000
UIPath - Cloud Document Understanding Page Bundle - 10M	Document Understanding enables UIPath robots to digitize, classify, and extract information from forms, documents, and unstructured text using a combination of OCR, template, and machine learning approaches. This offering is priced per page for each extraction method. This SKU contains a bundle of 10M pages, but certain features and models may be metered at different rates. For greater volumes, simply order as many as needed to meet required customer volumes.	
		\$1,000,000
UIPath - Cloud Document Understanding Page Bundle - 1M	Document Understanding enables UIPath robots to digitize, classify, and extract information from forms, documents, and unstructured text using a combination of OCR, template, and machine learning approaches. This offering is priced per page for each extraction method. This SKU contains a bundle of 1M pages, but certain features and models may be metered at different rates. For greater volumes, simply order as many as needed to meet required customer volumes.	
		\$150,000
UIPath - Cloud Document Understanding Page Bundle - 40K	Document Understanding enables UIPath robots to digitize, classify, and extract information from forms, documents, and unstructured text using a combination of OCR, template, and machine learning approaches. This offering is priced per page for each extraction method. This SKU contains a bundle of 40K pages, but certain features and models may be metered at different rates. For greater volumes, simply order as many as needed to meet required customer volumes.	
		\$8,000
UIPath - Cloud Orchestrated Robot - Non-Production	The Unattended Non-Production Robot offering contains an Unattended Robot and 3000 Integration Service API calls/month. Limited to non-production use. Orchestrated from the UIPath Automation Cloud, it also includes Automation Suite usage rights for non-SaaS orchestration.	
		\$1,100
UIPath - Cloud Orchestrated Unattended Robot	The Unattended Robot offering includes an Unattended Robot, that independently executes automations, and 3000 Integration Service API calls/month. It runs on a virtual desktop, in a secure session, end-to-end, without human intervention. It performs the process end to end, 'lights out' - working business transactions with the help of an RPA work queue. Licenses a single robot. Orchestrated from the UIPath Automation Cloud, it also includes Includes Automation Suite usage rights for non-SaaS orchestration	
		\$10,000
UIPath - Cloud Orchestrated Unattended Robot - Test	The Unattended Test Robot offering includes a Test Robot and 3000 Integration Service API calls/month. It provides the ability to execute automated tests orchestrated from the UIPath Automation Cloud and it also includes Automation Suite usage rights for non-SaaS orchestration.	
		\$2,000
UIPath - Integration Service API calls bundle - 3M	The UIPath Integration Service delivers the tools and flexibility to solve any automation challenge, faster and at scale allowing developers to seamlessly use UIs and APIs in a single automation. This offering is priced per API call. This SKU contains a bundle of 6M API calls.	
		\$12,000
UIPath - Integration Service API calls bundle - 6M	The UIPath Integration Service delivers the tools and flexibility to solve any automation challenge, faster and at scale allowing developers to seamlessly use UIs and APIs in a single automation. This offering is priced per API call. This SKU contains a bundle of 6M API calls.	
		\$20,000

UiPath - Cloud Test Management	The UiPath Cloud Test Management offering provides access to UiPath Cloud Test Manager - a central service that supports requirements management, test case design and integration with ALM tooling. User access to this capability is entitled via either the Cloud Orchestrated Automation Developer or Cloud Tester offerings. Delivered from the UiPath Automation Cloud.	
		\$9,000
UiPath - Cloud Process Mining 20M Rows Bundle	The Cloud Process Mining offering includes access to Cloud Process Mining capabilities and entitles up to 20M Rows of Process Mining Capacity. Cloud Process Mining gives users the ability to continuously monitor their end-to-end processes, to discover how to optimize them, and to prioritize automation opportunities based on the impact they will have on their most important KPIs. Delivered from the UiPath Automation Cloud.	
		\$30,000
UiPath - Cloud Automation Hub - Standard	Automation Hub enables organizations to manage the entire automation lifecycle with instant transparency and control. With Automation Hub, organizations can discover, prioritize, and track automation ideas in one place, and more easily scale their automation programs. An unlimited number of users is included for every Automation Hub instance. This SKU also includes enterprise production licenses of Task Capture, a separately downloaded tool that enables employees to quickly document step-by-step processes.	
		\$9,000
UiPath - Cloud Insights	Cloud Insights provides powerful, embedded analytics for measuring and reporting on RPA operations and business definable KPIs. Cloud Insights is licensed per Automation Cloud organization; Includes 10 Designer Users and unlimited Viewer Users.	
		\$15,000
UiPath - Cloud Task Mining	Task Mining automatically identifies and aggregates employee desktop activities, then applies AI to map tasks to automation opportunities. Delivered from the UiPath Automation Cloud. This licensing SKU covers unlimited users. Compute required to process the data is purchased separately using the Compute Unit SKUs.	
		\$20,000
UiPath - Computer Vision - On Cloud	ComputerVision is a new, machine-learning based method used to locate screen elements and operate user interfaces. Because it's a class of "surface automation" tools, it doesn't require or use the underlying properties of applications, so it can operate a large array of previously inaccessible technologies: virtual machines, other operating systems (Linux, MacOS, Android, IOS), Silverlight, Flash, etc. This CLOUD deployment option uses UiPath server, eliminating infrastructure requirements for customers.	
		\$0
UiPath - Enterprise Foundation Pack - Cloud	All the foundation services required by an organization to run a highly available scalable enterprise-wide automation program in the Automation Cloud. Includes: 1 Cloud Automation Hub, 1 Cloud Test Manager, 1 Process Mining Server, 1 Process Mining Server - Nonproduction, 1 Cloud Task Mining, 1 Cloud Insights - Orchestrator Add-On. Automation users, automation developers and robots purchased separately as required.	
		\$67,000
UiPath - Starter Pack - Standard - Cloud	Everything needed to automate with the UiPath Platform in the Automation Cloud. Includes: 1 Cloud Test Management, 1 Cloud Automation Hub, 4 Automation Developers, 4 Unattended Test Robots, Citizen Developer (0-16), Attended User (0-25), and Unattended Robots (0-4) are configurable based on standard options as required. Users and Robots orchestrated from the Automation Cloud.	
		\$77,000
UiPath - Starter Pack - Advanced - Cloud	Everything needed to automate and measure with the UiPath Platform at scale in the Automation Cloud. Includes: 1 Cloud Test Management, 1 Cloud Automation Hub, 8 Automation Developers, 8 Unattended Test Robots, 1 Cloud Insights - Orchestrator Add-On. Citizen Developer (0-40), Attended User (0-67), and Unattended Robots (0-10) are configurable based on standard options as required. Users and Robots orchestrated from the Automation Cloud.	
		\$147,000
UiPath - Starter Pack - Advanced - Cloud (No Test Manager)	Everything needed to automate and measure with the UiPath Platform at scale in the Automation Cloud. Includes: 1 Cloud Test Management, 1 Cloud Automation Hub, 8 Automation Developers, 8 Unattended Test Robots, 1 Cloud Insights - Orchestrator Add-On. Citizen Developer (0-40), Attended User (0-67), and Unattended Robots (0-10) are configurable based on standard options as required. Users and Robots orchestrated from the Automation Cloud.	
		\$147,000
UiPath - Starter Pack - Basic - Cloud	All the essentials needed to start automating with the UiPath Platform in the Automation Cloud. Includes: 2 Automation Developers, 2 Nonproduction Robots. Citizen Developer (0-14), Attended User (0-19), and Unattended Robots (0-3) are configurable based on standard options as required. Users and Robots orchestrated from the Automation Cloud.	
		\$37,000
UiPath - Cloud Hyperautomation Bundle - 250 Users	Access to the UiPath Platform in the Automation Cloud for 250 users within the following limits: Up to 250 total of any cloud orchestrated user type; Up to 50 Cloud Orchestrated Unattended Robots or Automation Cloud Robots; Up to 10AI Robot + AI Robot Pros and up to 50 Non-Production Robots.	
		\$800,000
UiPath - Cloud Hyperautomation Bundle - 500 Users	Access to the UiPath Platform in the Automation Cloud for 500 users within the following limits: Up to 500 total of any cloud orchestrated user type; Up to 100 Cloud Orchestrated Unattended Robots or Automation Cloud Robots; Up to 15 AI Robot + AI Robot Pros and up to 100 Non-Production Robots.	
		\$1,350,000
UiPath - Cloud Process Mining Starter Pack	The Cloud Process Mining Starter Pack includes the capacity to mine up to 100M rows of data, 2 Cloud Orchestrated Process Mining Developer Users, and 20 Cloud Process Mining Business Users. Delivered from the UiPath Automation Cloud.	
		\$150,000
UiPath - Cloud RPA Platform - NFR - Bundle	Not for Resale (NFR) Cloud RPA Platform offered for channel partners ONLY. To be used for Partners own demo environments, PoC labs, and training purposes. Production usage prohibited. Not for Resale/ only 1 YR Term. NFR proposal based benefit, based on approvals for UiPath Business Partners.	
		\$0
UiPath - Test Suite Starter Pack - Cloud	The Test Suite Starter Pack - Cloud offering includes UiPath Cloud Test Management, 3 Cloud Orchestrated Automation Developers, 5 Cloud Testers and 5 Cloud Orchestrated Unattended Robots. It delivers a test solution combining the world's leading automation technology with best-of-breed testing capabilities to ensure application and automation quality across an enterprise. Robots are for test purposes only. Each Automation Developer and Tester is a single named user. Delivered and orchestrated from the UiPath Automation Cloud.	
		\$29,000
UiPath - App Testing Starter Pack - Cloud	The App Testing Starter Pack - Cloud offering includes UiPath Cloud Test Management and 5 Cloud Testers. It delivers a test solution combining the world's leading automation technology with best-of-breed testing capabilities to ensure application and automation quality across an enterprise. Each Tester is a single named user. Delivered from the UiPath Automation Cloud.	
		\$11,000
OnPrem		
UiPath - Action Center - Named User	The Action Center offering includes Task Capture and Action Center. Action Center is a central portal allowing humans and unattended robots to seamlessly collaborate on a process. License per Named User with a minimum sale of 5 users.	
		\$440
UiPath - Action Center - Multiuser	The Action Center offering includes Task Capture and Action Center. Action Center is a central portal allowing humans and unattended robots to seamlessly collaborate on a process. License per Named User with a minimum sale of 5 users. Each Multiuser license adds 3 authorized users. Requires UiPath Multiuser Add-On.	
		\$880

UiPath - Attended - Named User	The Attended offering includes Task Capture, Action Center and an Attended Robot. The Attended Robot is deployed on a desktop and allows a user to access, manage, and run automations. Licenses a single named user.	\$1,200
UiPath - Attended - Multiuser	The Attended offering includes Task Capture, Action Center and an Attended Robot. The Attended Robot is deployed on a desktop and allows a user to access, manage, and run automations. Each Multiuser license adds 3 authorized users. Requires UiPath Multiuser Add-On.	\$2,400
UiPath - Citizen Developer - Named User	The Citizen Developer offering includes Task Capture, Action Center, an Attended Robot and StudioX. StudioX is an automation design tool that allows the business user to rapidly automate their business apps without the need for developer resources or coding, bringing automation to the masses. Intended for a single named user.	\$2,000
UiPath - Citizen Developer - Multiuser	The Citizen Developer offering includes Task Capture, Action Center, an Attended Robot and StudioX. StudioX is an automation design tool that allows the business user to rapidly automate their business apps without the need for developer resources or coding, bringing automation to the masses. Each Multiuser license adds 3 authorized users. Requires UiPath Multiuser Add-On.	\$4,000
UiPath - Automation Developer - Named User	The Automation Developer User includes Task Capture, Action Center, Attended Robot, StudioX, Studio and Test Manager access. Studio is an automation design tool that allows developers full control over automations with advanced activities, powerful debugging tools, team development support and integrated testing. Intended for a single named user.	\$3,400
UiPath - Automation Developer - Multiuser	The Automation Developer User includes Task Capture, Action Center, Attended Robot, StudioX, Studio and Test Manager access. Studio is an automation design tool that allows developers full control over automations with advanced activities, powerful debugging tools, team development support and integrated testing. Each Multiuser license adds 3 authorized users. Requires UiPath Multiuser Add-On.	\$6,800
UiPath - Process Mining Business User - Named User	The Process Mining Business User offering includes Action Center, Task Capture and Process Mining access. As a Process Mining Business User, you gain full transparency into your processes. Process Mining gives users the ability to reveal inefficient processes, discover automation opportunities, and continuously enhance and monitor end-to-end processes. Licenses a single named user.	\$900
UiPath - Process Mining Developer - Named User	The Process Mining Developer offering includes Task Capture, Action Center, an Attended Robot, StudioX, Studio and Process Mining Development. As a Developer User, you can fully access the design and development functionality of Process Mining, to develop, customize and administer platform apps.	\$5,500
UiPath - RPA Developer - Named User	The RPA Developer offering includes Task Capture, Action Center, Attended Robot, StudioX and Studio. Studio is an automation design tool that allows developers full control over automations with advanced activities, powerful debugging tools and team development support. Intended for a single named user.	\$3,400
UiPath - RPA Developer - Multiuser	The RPA Developer offering includes Task Capture, Action Center, Attended Robot, StudioX and Studio. Studio is an automation design tool that allows developers full control over automations with advanced activities, powerful debugging tools and team development support. Each Multiuser license adds 3 authorized users. Requires UiPath Multiuser Add-On.	\$6,800
UiPath - Tester - Named User	UiPath Tester provides annual access to comprehensive test management. It includes access to UiPath Test Manager, to manage requirements, design test cases and integrate with ALM tooling.	\$900
UiPath - Multiuser Add-On	Required to enable the use of Multiuser licensing with the UiPath Platform. Multiuser licenses add 3 authorized users for each purchased product. Multiuser Licenses are purchased separately from the Multiuser Add-On.	\$40,000
UiPath - AI Robot	An AI Robot is the runtime for serving ML Skills (i.e. making machine learning models available for Robots to make prediction requests to) and for run ML Training jobs (i.e. training a new model version of new data to improve its accuracy). One AI Robot can serve 2 ML Skills concurrently or run one ML training job concurrently.	\$9,000
UiPath - Document Understanding Page Bundle - 10M	Document Understanding enables UiPath robots to digitize, classify, and extract information from forms, documents, and unstructured text using a combination of OCR, template, and machine learning approaches. This offering is priced per page for each extraction method. This SKU contains a bundle of 10M pages, but certain features and models may be metered at different rates. For greater volumes, simply order as many as needed to meet required customer volumes.	\$1,000,000
UiPath - Document Understanding Page Bundle - 1M	Document Understanding enables UiPath robots to digitize, classify, and extract information from forms, documents, and unstructured text using a combination of OCR, template, and machine learning approaches. This offering is priced per page for each extraction method. This SKU contains a bundle of 1M pages, but certain features and models may be metered at different rates. For greater volumes, simply order as many as needed to meet required customer volumes.	\$150,000
UiPath - Document Understanding Page Bundle - 40K	Document Understanding enables UiPath robots to digitize, classify, and extract information from forms, documents, and unstructured text using a combination of OCR, template, and machine learning approaches. This offering is priced per page for each extraction method. This SKU contains a bundle of 40K pages, but certain features and models may be metered at different rates. For greater volumes, simply order as many as needed to meet required customer volumes.	\$8,000
UiPath - Robot - NonProduction	An Unattended Robot independently executes automations. It runs on a virtual desktop, in a secure session, end-to-end, without human intervention. A nonproduction Robot is used in dev/test to validate correct operation of automations before deployment in production.	\$400
UiPath - Unattended Robot - Concurrent Runtime	Concurrent licenses are available ONLY in the case of Orchestrator scenario. 1 active runtime, unlimited users and workstations defined. Unattended Concurrent Runtime License - the No. of Unattended Concurrent Runtime licenses purchased equals the maximum number of unattended robots that are able to execute back office processes simultaneously, regardless of the number of users and machines defined in Orchestrator.	\$8,000
UiPath - Unattended Robot - Test	UiPath Unattended Test Robot provides the ability to execute automated tests from UiPath Orchestrator.	\$1,600
UiPath - Computer Vision - On-Prem	ComputerVision is a new, machine-learning based method used to locate screen elements and operate user interfaces. Technically, it's a class of "surface automation" tools, because it doesn't require or use the underlying properties of applications, but only the aspect and relationship of various screen elements. CV is a set of Studio activities, that require a ML server. By default our UiPath cloud server is used.	\$0
UiPath - High-Availability Add-On for Orchestrator	For each deployment of the UiPath Platform that requires Multi-Node, High Availability, Disaster Recovery or Active-Active scenarios for UiPath Orchestrator the High Availability Add-on is required. It offers enterprise grade security, professional grade caching and UiPath support.	\$18,000
UiPath - High-Availability Add-On for Orchestrator - NonProduction	For each non-production deployment of the UiPath Platform that has two or more Orchestrators that require High Availability. The SKU enables active-active DR, low latency grade caching.	\$3,600
UiPath - Insights - Orchestrator Add-On	UiPath Insights provides powerful, embedded analytics that measure, report and align RPA Operations with Strategic Business Outcomes. It is licensed per Orchestrator. This add-on covers all connected robots and users on a single production Orchestrator.	\$9,000
UiPath - Insights - Orchestrator Add-On - NonProduction	UiPath Insights provides powerful, embedded analytics that measure, report and align RPA Operations with Strategic Business Outcomes. It is licensed per Orchestrator. This add-on covers all connected robots and users on a single nonproduction Orchestrator.	\$1,800
UiPath - Orchestrator - NonProduction	Orchestrator offered for non-production scope	\$4,000
UiPath - Orchestrator - Basic	A "basic" Orchestrator package limited to a single tenancy, with a maximum of 5 Robots, Attended and/or Unattended, and a maximum of 5 Studios.	\$9,000

UiPath - Orchestrator - Basic Upgrade	Upgrade path from Orchestrator Basic to Orchestrator Standard Edition. Offered for on-premises and 3rd party cloud orchestration (use cloud orchestrated SKU's instead to buy SaaS orchestration)	
		\$12,000
UiPath - Orchestrator - Standard	Robot Management and Control System supporting: release management, centralized logging, reporting, auditing and monitoring tools, remote control, centralized scheduling, queue / robot workload management, assets management. It provides an unlimited amount of tenants (e.g. separate logical environments of robots, processes, users and systems and data). Offered for on-premises and 3rd party cloud orchestration (use cloud orchestrated SKU's instead to buy SaaS orchestration)	
		\$20,000
UiPath - Process Mining Server	Process Mining enables organizations to discover high impact automation opportunities and continuously monitor and improve their operations. With Process Mining, organizations can easily visualize, analyze and monitor key business processes, using the derived insights to introduce process enhancements that maximize the ROI of their RPA programs. Note that a separate Starter Pack is required for Process Mining implementation, which includes UiPath support during the implementation process.	
		\$20,000
UiPath - Process Mining Server - NonProduction	Process Mining enables organizations to discover high impact automation opportunities and continuously monitor and improve their operations. With Process Mining, organizations can easily visualize, analyze and monitor key business processes, using the derived insights to introduce process enhancements that maximize the ROI of their RPA programs. This offering is intended for training, development, acceptance or testing purposes, and can only be sold in combination with a server license. Its usage is limited only to non-production servers.	
		\$4,000
UiPath - Test Manager	UiPath Test Manager is a central service that supports requirements management, test case design and integration with ALM tooling. Test Manager is an add-on to UiPath Orchestrator. User access to Test Manager is entitled via either the Automation Developer or Tester offerings.	
		\$9,000
UiPath - App Testing Starter Pack	The App Testing Starter Pack offering includes UiPath Test Manager and 5 Testers. It delivers a test solution combining the world's leading automation technology with best-of-breed testing capabilities to ensure application and automation quality across an enterprise. Each Tester is a single named user.	
		\$11,000
UiPath - Hyperautomation Bundle - 250 Users	Access to the UiPath platform for 250 users within the following limits: Up to 250 total of any user type; 1 Process Mining Server; Up to 50 Concurrent Unattended Robots; Up to 10 AI Robot + AI Robot Pros and up to 50 Non-Production Robots.	
		\$600,000
UiPath - Hyperautomation Bundle - 500 Users	Access to the UiPath platform for 500 users within the following limits: Up to 500 total of any user type; 2 Process Mining Servers; Up to 100 Concurrent Unattended Robots; Up to 15 AI Robot + AI Robot Pros and up to 100 Non-Production Robots.	
		\$1,000,000
UiPath - Process Mining Starter Bundle	Process Mining allows you to visualize, analyze and continuously monitor end-to-end process data from source systems to identify optimization opportunities. The Starter Bundle includes 1 Process Mining Server, 20 Process Mining Business Users and 2 Process Mining Developer Users.	
		\$45,000
UiPath - RPA Platform - NFR - Bundle	Not for Resale (NFR) On-Prem RPA Platform offered for channel partners ONLY. To be used for Partners own demo environments, PoC labs, and training purposes. Production usage prohibited. Not for Resale/ only 1 YR Term. NFR proposal based benefit, based on approvals for UiPath Business Partners.	
		\$0

ATTACHMENT E4

VALUE ADD SERVICES

Intentionally left blank.

ATTACHMENT E5

THIRD PARTY TERMS

Intentionally left blank.

ATTACHMENT F

EXCEPTIONS

Intentionally left blank.

ATTACHMENT F1

STATE OF OKLAHOMA CONTRACT WITH RATTAN CONSULTING, INC.

RESULTING FROM SOLICITATION NO. 0900000556

Template for Contract Modifications for Quotes, Statements of
Work, or other Ordering Documents

The parties agree to use this template as the process to formally approve any terms, conditions or clauses that are to supersede the terms and Conditions in the Contract for purposes of the applicable quote, statement of work or other ordering document.

Contract Modifications for Quote, Statement of Work, or other Ordering Document

Solely for purposes of this ordering document, the terms and conditions of the Contract are hereby amended as set forth below. This amendment is considered an Addendum.

RFP Section	Exception/Additional Terms

STATE OF OKLAHOMA
by and through the
OFFICE OF MANAGEMENT AND
ENTERPRISE SERVICES

RATTAN CONSULTING, INC.

By: _____

By: _____

Name: _____

Name: _____

Title: _____

Title: _____

Date: _____

Date: _____

The [INSERT AGENCY NAME] is additionally executing this document to memorialize its involvement in negotiation of and its agreement with the terms of this document.

By: _____

Name: _____

Title: _____

Date: _____









Execution Version Statewide Contract 1041 Rattan Consulting

Final Audit Report

2023-12-13

Created:	2023-12-13
By:	Courtney Templeton (courtney.templeton@omes.ok.gov)
Status:	Signed
Transaction ID:	CBJCHBCAABAA14RrcgxAomXkJRCieVmzLv-NXcswifBW

"Execution Version Statewide Contract 1041 Rattan Consulting" History

-  Document created by Courtney Templeton (courtney.templeton@omes.ok.gov)
2023-12-13 - 3:53:45 PM GMT
-  Document emailed to Travis Rattan (trattan@rattanconsulting.com) for signature
2023-12-13 - 3:55:35 PM GMT
-  Email viewed by Travis Rattan (trattan@rattanconsulting.com)
2023-12-13 - 9:51:20 PM GMT
-  Document e-signed by Travis Rattan (trattan@rattanconsulting.com)
Signature Date: 2023-12-13 - 9:51:45 PM GMT - Time Source: server
-  Document emailed to Joe McIntosh (joe.mcintosh@omes.ok.gov) for signature
2023-12-13 - 9:51:47 PM GMT
-  Email viewed by Joe McIntosh (joe.mcintosh@omes.ok.gov)
2023-12-13 - 10:37:12 PM GMT
-  Document e-signed by Joe McIntosh (joe.mcintosh@omes.ok.gov)
Signature Date: 2023-12-13 - 10:37:45 PM GMT - Time Source: server
-  Agreement completed.
2023-12-13 - 10:37:45 PM GMT