

Statewide Contract Summary

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

Contract title: Software Value Added Reseller

Contract Number: SW1041AWS

Date of Contract issuance: 6/04/2024

Contract period: 6/04/2024 through 6/03/2025

Agreement period: 6/03/2024 through 6/03/2029

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: Amazon Web Services

Supplier ID #: 0000415602

Contract ID #: 7409

Supplier Point of Contact: Brad Stone

Supplier address: 410 Terry Avenue North

City: Seattle

State: WA

Zip Code: 98109 - 5210

Phone #: 1 - 916 - 467 - 6610

Email: aws-oklahoma-contract@amazon.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:



OKLAHOMA
Office of Management
& Enterprise Services

State of Oklahoma

Office of Management and Enterprise Services

STATE OF OKLAHOMA STATEWIDE CONTRACT WITH AMAZON WEB SERVICES, 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 (“State”) and Amazon Web Services, 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, is one year and there are four (4) one-year options to renew the Contract.

The following paragraph is a disclaimer for customers under this Contract and is not a Contract term. In order to get the benefit of the pre-negotiated terms and conditions of this Contract with Amazon Web Services, Inc., any entity purchasing off this Contract must not create an account outside of the terms of this Contract. Any purchasing entity should make certain that they are properly identifying their accounts as an Enterprise Account. If a purchasing entity under this Contract creates an account not within the parameters of this Contract, by creating something other than an Enterprise Account, the purchasing entity will be bound by the AWS Customer Agreement, and not the terms of this Contract. The AWS Customer Agreement is accessible via <http://aws.amazon.com/agreement>. Further, in order to get the benefit of the pre-negotiated terms and conditions of this Contract with Amazon Web Services, Inc., any purchasing entity must create/configure their Enterprise Account in the United States. If the purchasing entity creates/configures an account outside of the United States, then it will be governed by the AWS Customer Agreement, identified in the hyperlink above, and not by this Contract. Additionally, this Contract does not include the State’s CJIS Security Policy. Customer and Supplier may address the use of criminal justice information through further agreement.

Purpose

The State is awarding this Contract to Supplier for the provision of software and services to support State agencies and other eligible Oklahoma Interlocal Entities, including software, training, pre-sales assistance, documentation, installation, maintenance, support, configuration, customization, and license agreement administration, as more particularly described in certain Contract Documents. 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 offering products and Services under this Contract. For State agencies, boards and commissions issuance of a purchase order is required prior to use of products and Services and payment to Supplier under this Contract.
2. The following are the Contract Documents which are attached hereto:
 - 2.1 Solicitation 0900000556, Attachment A;
 - 2.1. General Terms, Attachment B;
 - 2.2. Oklahoma Statewide Contract terms, Attachment C;
 - 2.3. Information Technology terms, Attachment D;
 - 2.4. Enterprise Agreement, Attachment E-1
 - i. FERPA Appendix to the Enterprise Agreement
 - ii. IRS 1075 Appendix to the Enterprise Agreement
 - iii. Minimum Architecture Requirements Appendix to the Enterprise Agreement, Held as Confidential
 - iv. Pricing Appendix to the Enterprise Agreement
 - v. Statement of Work Template to the Enterprise Agreement
 - vi. Data Processing Appendix to the Enterprise Agreement
 - vii. Business Associate Appendix to the Enterprise Agreement, Confidential
 - 2.5. Negotiated Exceptions, Attachment F; and
 - 2.6. 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 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. No modification or amendment of any portion of this Contract will be effective unless in writing and signed by Supplier and the Chief Information Officer utilizing Attachment F-1. No other terms and conditions or clauses, including via a hyperlink or uniform resource locator that are not already identified in the Contract Documents, 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, unless the Contract is modified or amended pursuant to this Section 3.2.

- 3.3. To the extent any Contract Document, or a hyperlink or uniform resource locator that is identified in the Contract Documents contains a terms or condition that directly conflicts with an applicable Oklahoma and/or United States law or regulation, such term or condition is void and unenforceable.
4. Any reference to a Contract Document refers to such Contract Document as it may have been amended.

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

Amazon Web Services, Inc.

By:

DocuSigned by:

Joe McIntosh

1C5419931B80453...

By:

DocuSigned by:

Steve Boyce

07E36C4BC587455...

Name: Joe McIntosh

Name: Steve Boyce

Title: CIO

Title: Authorized Signatory

Date: June 4, 2024

Date: June 3, 2024



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.

09/01/2020



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

09/01/2020



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.

**ATTACHMENT E-1 to
STATE OF OKLAHOMA CONTRACT WITH
AMAZON WEB SERVICES, INC.
RESULTING FROM SOLICITATION NO. 0900000556**

The Enterprise Agreement is hereby amended to include the terms as set forth below and supersedes all prior Enterprise Agreements submitted by Amazon Web Services Inc. or discussed by the parties.

1. Use of the Service Offerings.

1.1 Generally. Customer may access and use the Services in accordance with this Contract. Service Level Agreements apply to certain Services. Customer's use of the Service Offerings will comply with the terms of Statewide 1041 (the "Contract".)

1.2 AWS Account. To access the Services, Customer must create one or more AWS Enterprise Accounts. Unless explicitly permitted by the Service Terms, Customer will only create one AWS Enterprise Account per email address. All AWS Enterprise Accounts will be covered by the Contract. For all AWS Enterprise Accounts, the Contract supersedes any acceptance of the AWS Customer Agreement ("Agreement") by Customer or any of its employees acting on behalf of Customer. If any of Customer's AWS accounts do not meet the definition of an "AWS Enterprise Account," those accounts will be governed by the AWS Customer Agreement.

1.3 Third-Party Content. Third-Party Content may be used by Customer at Customer's election. Third-Party Content is governed by the Contract unless accompanied by separate terms and conditions, which may include separate fees and charges.

2. Changes.

2.1 To the Service Offerings. AWS may change or discontinue any of the Service Offerings, from time to time. For any AWS Enterprise Accounts enrolled in AWS Support at the Developer-level tier or above (or any successor service providing such communications alerts), AWS will provide at least 12 months' prior Notice to Customer if AWS decides to discontinue a Service that it makes generally available to its customers and that Customer is using. AWS will not be obligated to provide Notice under this Section 2.1 if the discontinuation is necessary to address an emergency or threat to the security or integrity of AWS, respond to claims, litigation, or loss of license rights related to third-party intellectual property rights, or comply with the law or requests of a government entity.

2.2 To the Service Level Agreements. AWS may change Service Level Agreements from time to time, but will provide 90 days' prior Notice to Customer before materially reducing the benefits offered to Customer under any Service Level Agreement(s) that are available as of the Effective Date.

3. Privacy and Security.

3.1 AWS Security. AWS will implement reasonable and appropriate measures for the AWS Network (as determined by AWS) designed to help Customer secure Customer Data against accidental or unlawful loss, access or disclosure (the "**Security Objectives**") in accordance with the AWS Security Standards. AWS may modify the AWS Security Standards from time to time, but will continue to provide at least the same level of security as is described in the AWS Security Standards on the Effective Date.

3.2 Data Privacy. Customer may specify the AWS regions in which Customer Data will be stored. Customer consents to the storage of Customer Data in, and transfer of Customer Data into, the AWS regions Customer selects. AWS will not access or use Customer Data except as necessary to



maintain or provide the Service Offerings, or as necessary to comply with the law or a binding order of a governmental body. AWS will not (a) disclose Customer Data to any government or third party, or (b) subject to Section 3.3, move Customer Data from the AWS regions selected by Customer; except in each case as necessary to comply with the law or a binding order of a governmental body (such as a subpoena or court order). Unless it would be in violation of a court order or other legal requirement, AWS will give Customer reasonable Notice of any legal requirement or order referred to in this Section 3.2, to enable Customer to seek a protective order or other appropriate remedy. AWS will only use Account Information in accordance with the Privacy Notice, and Customer consents to such usage. The Privacy Notice does not apply to Customer Data.

3.3 Service Attributes. To provide billing and administration services, AWS may process Service Attributes in the AWS region(s) where Customer uses the Service Offerings and the AWS regions in the United States. Consistent with Section 3.2, to provide Customer with support services initiated by Customer and investigate fraud, abuse or violations of the Contract, AWS may process Service Attributes where AWS maintains its support and investigation personnel.

3.4 AWS Information Security Program. As of the Effective Date, the AWS Information Security Management System (ISMS) is ISO 27001 certified. AWS will maintain an information security program designed to provide at least the same level of protection as evidenced by that certification on the Effective Date.

3.5 Audits of Technical and Organizational Measures. Upon Customer's request, and provided that the parties have an applicable NDA in place, AWS will provide to Customer a copy of the AWS System and Organization Controls 1, Type 2 report or such alternative industry standard reports or certifications that are substantially equivalent as reasonably determined by AWS. AWS will make this documentation available to Customer via AWS Artifact (or an alternative means accessible via the AWS Site) and this documentation will be treated as Confidential Information of AWS.

4. Customer Responsibilities.

4.1 Customer Data. Customer is solely responsible for the development, content, operation, maintenance, and use of Customer Data. Customer agrees that Customer Data will not violate any of the Policies or any applicable law.

4.2 Customer's Security and Redundancy. Customers have a variety of options to choose from when configuring their accounts, and for all sensitive or otherwise valuable content AWS recommends that Customer uses strong security and redundancy features, such as access controls, encryption, and backup. Customer is responsible for properly configuring and using the Service Offerings in a manner that provides security and redundancy of its AWS Enterprise Accounts and Customer Data, such as, for example, using enhanced access controls to prevent unauthorized access to AWS Enterprise Accounts and Customer Data, using encryption technology to prevent unauthorized access to Customer Data, and ensuring the appropriate level of backup to prevent loss of Customer Data.

4.3 Log-In Credentials and Account Keys. AWS log-in credentials and private keys generated by the Services are for Customer's internal use only and Customer may not sell, transfer or sublicense them to any other entity or person, except that Customer may disclose its private key to its agents and subcontractors (including any of its Affiliates who are acting as an agent or subcontractor of Customer) performing work on behalf of Customer. Except to the extent caused by AWS's breach of the Contract, as between the parties, Customer is responsible for all activities that occur under its AWS Enterprise Accounts.

4.4 End Users. If Customer uses the Services to provide services to, or otherwise interact with, End Users, then Customer, and not AWS, will have the relationships (e.g., via executed contracts between Customer and End Users or via online terms of service) with End Users. Therefore Customer, and not AWS, is responsible for End Users' use of Customer Data and the Service Offerings. To the extent that Customer enables End Users to access the Services or Customer Data, Customer will ensure that all End Users comply with any applicable obligations of Customer under the Contract and that any terms of any agreement with each End User are not inconsistent with the Contract. AWS does not provide any support or services to End Users unless AWS has a separate agreement with Customer or an End User obligating AWS to provide support or services to End Users. Customer is responsible for providing customer service (if any) to End Users.

5. Fees and Payment.

5.1 Service Fees. Unless otherwise stated on the AWS Site, AWS will invoice Customer at the end of each month for all applicable fees and charges accrued for use of the Service Offerings, as described on the AWS Site, during the month. Customer will pay AWS all invoiced amounts within 45 days of the date of the invoice (other than Disputed Amounts). For any Disputed Amounts, Customer will provide Notice to AWS, including the basis for the dispute (including any supporting documentation), and the parties will meet within 30 days of the date of the Notice to resolve the dispute. If the parties fail to resolve the dispute within such 30-day period, AWS may, at its option, limit (in full or in part) Customer's or any End User's right to access or use the Service Offerings until the dispute is resolved. All amounts payable by Customer under the Contract will be paid to AWS without setoff or counterclaim and without deduction or withholding, provided that Disputed Amounts will be handled as set forth above. Fees and charges for any new Service or new feature of a Service will be effective when AWS posts updated fees and charges on the AWS Site, unless expressly stated otherwise in a Notice. AWS may increase or add new fees and charges for any existing Service by giving Customer at least 60 days' prior Notice. AWS may charge Customer interest at the rate of 1.5% per month (or the highest rate permitted by law, whichever is less) on all late payments.

5.2 Taxes. Each party will be responsible, as required under applicable law, for identifying and paying all taxes and other governmental fees and charges (and any penalties, interest, and other additions thereto) that are imposed on that party upon or with respect to the transactions and payments under the Contract. All fees payable by Customer are exclusive of Indirect Taxes, except where applicable law requires otherwise. AWS may charge and Customer will pay applicable Indirect Taxes that AWS is legally obligated or authorized to collect from Customer. Customer will provide such information to AWS as reasonably required to determine whether AWS is obligated to collect Indirect Taxes from Customer. AWS will not collect, and Customer will not pay, any Indirect Tax for which Customer furnishes AWS a properly completed exemption certificate or a direct payment permit certificate for which AWS may claim an available exemption from such Indirect Tax. All payments made by Customer to AWS under the Contract will be made free and clear of any deduction or withholding, as may be required by law. If any such deduction or withholding (including but not limited to cross-border withholding taxes) is required on any payment, Customer will pay such additional amounts as are necessary so that the net amount received by AWS is equal to the amount then due and payable under the Contract. AWS will provide Customer with such tax forms as are reasonably requested in order to reduce or eliminate the amount of any withholding or deduction for taxes in respect of payments made under the Contract.

6. Temporary Limitation of Access and Use Rights. AWS may temporarily limit (in full or in part, as set forth in this Section 6) Customer's or any End User's right to access or use the Service Offerings upon Notice to Customer (which will be reasonable prior notice unless AWS reasonably

believes immediate limitation is necessary) if AWS reasonably determines that Customer's or an End User's use of the Service Offerings poses a security risk or threat to the function of the Service Offerings, or poses a security or liability risk or threat of harm to AWS, its Affiliates or any third party. AWS will only limit Customer's right to access or use the instances, data or portions of the Service Offerings that caused the security or liability risk or threat. AWS will restore Customer's access and use rights promptly after Customer has resolved the issue giving rise to the limitation. Customer remains responsible for all fees and charges for the Service Offerings during the period of limitation.

7. Term; Termination.

7.1 Term. Reserved.

7.2 Termination of a Purchase Order (or other similar ordering document) or Customer's agreement to purchase under the Contract.

(a) **Termination for Convenience.** Between Customer and AWS, Customer may terminate any purchase order (or other similar ordering document) or Customer's agreement to purchase under the Contract for any reason by providing AWS Notice. Between Customer and AWS, AWS may terminate any purchase order (or other similar ordering document) or Customer's agreement to purchase under the Contract for any reason by providing Customer at least two years' Notice.

(b) Termination for Cause.

(i) **By Customer or AWS.** Between Customer and AWS, either Customer or AWS may terminate any purchase order (or other similar ordering document) or Customer's agreement to purchase under the Contract for cause if the other is in material breach and the material breach remains uncured for a period of 30 days from receipt of Notice by the breaching party.

(ii) **By AWS.** Between Customer and AWS, AWS may terminate any purchase order (or other similar ordering document) or Customer's agreement to purchase under the Contract for cause (a) upon 90 days' Notice to Customer if AWS has the right to limit Customer's or any End User's right to access or use the Service Offerings under Section 6 and Customer has not cured the condition giving rise to that right to limit within such 90 day period, or (b) upon 30 days' Notice to Customer in order to comply with applicable law or requirements of governmental entities.

(c) For clarification, Section 7.2 does not govern termination of Statewide 1041 between the State, through OMES, and AWS. For termination of the Statewide 1041 Contract, see Attachment B, Sections 17-19.

7.3 Effect of Termination of a Purchase Order (or other similar ordering document) or Customer's agreement to purchase under the Contract.

(a) Generally. Upon the Termination Date:

(i) except as provided in this Section 7.3, all of Customer's rights under the Contract immediately terminate;

(ii) Customer remains responsible for all fees and charges Customer has incurred through the Termination Date; and

(iii) Sections 4, 5, 7.3, 8.1, 8.3, 8.4, 9, 10.3, 11, 12 and 13 of the Enterprise Agreement and Attachment B, Section 16.5 (Limitation of Liability) will continue to apply in accordance with their terms.

(b) **Post-Termination Retrieval of Customer Data.** During the 180 days following the Termination Date, AWS will not take action to remove any Customer Data as a result of the termination from any

open AWS Enterprise Account. In addition, during such period, Customer may retrieve any remaining Customer Data from the Services, unless (i) prohibited by law or the order of a governmental or regulatory body or it could subject AWS or its Affiliates to liability, or (ii) Customer has not paid all amounts due under the Contract, other than Disputed Amounts. For purposes of this language, Customer is intended and understood to mean the purchasing entity and not the State of Oklahoma as a whole. For any use of the Services during such period, all terms of the Contract will continue to apply and Customer will pay the applicable fees at the rates under Section 5. No later than the end of this 180-day period, Customer will close all AWS Enterprise Accounts and return or, if instructed by AWS, destroy all AWS Content in Customer's possession (except for AWS Content that is publicly available on the AWS Site).

8. Proprietary Rights.

8.1 Customer Data. As between Customer and AWS, Customer (or Customer's licensors) own all right, title, and interest in and to Customer Data. Except as provided in the Contract, AWS obtains no rights under the Contract from Customer (or Customer's licensors) to Customer Data.

8.2 Intellectual Property License. The Intellectual Property License applies to the use of AWS Content and the Services.

8.3 Restrictions. Neither Customer nor any End User may use the Service Offerings in any manner or for any purpose other than as expressly permitted by the Contract. Neither Customer nor any End User may, or may attempt to (a) reverse engineer, disassemble, or decompile the Services or AWS Content or apply any other process or procedure to derive the source code of any software included in the Services or AWS Content, (b) access or use the Services or AWS Content in a way intended to avoid incurring fees or exceeding usage limits or quotas, or (c) resell the Services or AWS Content. The AWS Trademark Guidelines apply to the use of AWS Marks. Customer will not misrepresent or embellish the relationship between AWS and Customer (including by expressing or implying that AWS supports, sponsors, endorses, or contributes to Customer or Customer's business endeavors). Customer will not imply any relationship or affiliation between AWS and Customer except as expressly permitted by the Contract.

8.4 Suggestions. If Customer elects to provide any Suggestions to AWS or its Affiliates, AWS and its Affiliates will be entitled to use the Suggestions without restriction.

9. Third-Party Claims.

9.1 Policies and End User Disputes. Customer represents and warrants that Customer's and its End Users' access and use of the Services and AWS Content will not violate the Policies.

9.2 Intellectual Property.

(a) Reserved.

(b) Customer represents and warrants that Customer Data will not infringe or misappropriate any third party's intellectual property rights.

(c) Reserved.

(d) Reserved.

10. AWS Warranties and Warranty Disclaimers.

10.1 AWS Warranties. AWS represents and warrants to Customer that (a) the Services will perform substantially in accordance with the Documentation and (b) AWS will use commercially

reasonable efforts to prevent the introduction or proliferation of any viruses or other malicious code into the Services.

10.2 Mutual Warranties. Customer and AWS each represents and warrants to the other that (a) it has full power and authority to enter into and perform the Contract, (b) the execution and delivery of the Contract has been duly authorized, (c) it will comply with all applicable laws, rules, regulations and ordinances in the performance of the Contract (and, in the case of Customer, the use of the Service Offerings), and (d) its performance hereunder does not breach any other agreement to which it is bound.

10.3 Warranty Disclaimers. EXCEPT AS EXPRESSLY SET FORTH IN SECTION 10.1 AND SECTION 10.2, AND EXCEPT TO THE EXTENT PROHIBITED BY LAW, AWS, ITS AFFILIATES AND ITS LICENSORS MAKE NO REPRESENTATIONS OR WARRANTIES OF ANY KIND, WHETHER EXPRESS, IMPLIED, STATUTORY OR OTHERWISE, REGARDING THE SERVICE OFFERINGS OR THE THIRD-PARTY CONTENT, AND DISCLAIM ALL OTHER WARRANTIES, INCLUDING ANY IMPLIED OR EXPRESS WARRANTIES (A) OF MERCHANTABILITY, SATISFACTORY QUALITY, FITNESS FOR A PARTICULAR PURPOSE, NON-INFRINGEMENT, OR QUIET ENJOYMENT, (B) ARISING OUT OF ANY COURSE OF DEALING OR USAGE OF TRADE, (C) THAT THE SERVICE OFFERINGS OR THIRD-PARTY CONTENT WILL BE UNINTERRUPTED, ERROR FREE, OR FREE OF HARMFUL COMPONENTS, AND (D) THAT ANY CONTENT, INCLUDING CUSTOMER DATA OR THIRD-PARTY CONTENT, WILL BE SECURE OR NOT OTHERWISE LOST OR DAMAGED.

11. Limitations of Liability.

11.1 Reserved.

12. Miscellaneous.

12.1 Assignment. As between Customer and AWS, neither Customer nor AWS may assign or otherwise transfer the Customer's agreement under the Contract or any of its rights and obligations under the Customer's agreement under the Contract without the prior written approval of the other; except that either Customer or AWS may assign or otherwise transfer the Customer's agreement under the Contract without the consent of the other (a) in connection with a merger, acquisition or sale of all or substantially all of its assets, or (b) to any Affiliate or as part of a corporate reorganization, or (c) in the case of AWS, with respect to specific AWS Enterprise Accounts, to an Affiliate; provided that the assigning party provides notice to the other upon completion of such assignment. Effective upon such assignment or transfer, subject to the assignee/transferee's consent, the assignee/transferee is deemed substituted for the assignor/transferor as a party to the Customer's agreement under the Contract. Subject to the foregoing, this Customer's agreement under the Contract will be binding upon, and inure to the benefit of the parties and their respective permitted successors and assigns.

For clarification, Section 12.1 is not applicable to the assignment of Statewide 1041 between the State, through OMES, and AWS. For assignment of Statewide 1041 between State, through OMES, and AWS, see Attachment B, Section 13.1.

12.2 Counterparts; Facsimile. The Contract may be executed by facsimile or by electronic signature in a format approved by AWS, and in counterparts, each of which (including signature pages) will be deemed an original, but all of which together will constitute one and the same instrument.

12.3 This Enterprise Agreement incorporates the Policies. If any of Customer's AWS accounts do not meet the definition of an "AWS Enterprise Account," then those AWS accounts will be governed by the AWS Customer Agreement. AWS will not be bound by any term, condition or other provision which is different from or in addition to the provisions of the Contract (whether or not it would materially alter

this Contract) including for example, any term, condition or other provision (a) submitted by Customer in any order, receipt, acceptance, confirmation, correspondence or other document, (b) related to any online registration, response to any Request for Bid, Request for Proposal, Request for Information, or other questionnaire, or (c) related to any invoicing process that Customer submits or requires AWS to complete. If the terms of this document are inconsistent with the terms contained in any Policy, the terms contained in this document will control, except that the Service Terms will control over this document. No modification or amendment of any portion of this Agreement will be effective unless in writing and signed by the parties to this Agreement.

12.4 Force Majeure. Reserved.

12.5 Governing Law; Venue. The laws of the State of Oklahoma, without reference to conflict of law rules, govern this Contract and any dispute of any sort that might arise between the parties. Any dispute relating in any way to the Service Offerings or the Contract will only be adjudicated in a state or federal court located in Oklahoma City, Oklahoma. Each party consents to exclusive jurisdiction and venue in these courts. Notwithstanding the foregoing and to the extent permitted by Oklahoma law, AWS may seek injunctive relief in any state, federal, or national court of competent jurisdiction for any actual or alleged infringement of such party's, its Affiliates' or any third party's intellectual property or other proprietary rights to the extent the State of Oklahoma is not involved. The United Nations Convention for the International Sale of Goods does not apply to this Contract.

12.6 Trade Compliance. In connection with the Contract, each party will comply with all applicable import, re-import, sanctions, anti-boycott, export, and re-export control laws and regulations, including all such laws and regulations that apply to a U.S. company, such as the Export Administration Regulations, the International Traffic in Arms Regulations, and economic sanctions programs implemented by the Office of Foreign Assets Control. Customer is solely responsible for compliance with applicable laws related to the manner in which Customer chooses to use the Service Offerings, including (i) Customer's transfer and processing of Customer Data, (ii) the provision of Customer Data to End Users, and (iii) specifying the AWS region in which any of the foregoing occur. Customer represents that Customer and the entities that own or control Customer, and the financial institutions used to pay AWS under the Contract, are not subject to sanctions or otherwise designated on any list of prohibited or restricted parties, including but not limited to the lists maintained by the United Nations Security Council, the U.S. Government (e.g., the U.S. Department of Treasury's Specially Designated Nationals list and Foreign Sanctions Evaders list, and the U.S. Department of Commerce's Entity List), the European Union or its member states, or other applicable government authority.

12.7 Independent Contractors. AWS and Customer are independent contractors, and the Contract will not be construed to create a partnership, joint venture, agency, or employment relationship. Neither Customer nor AWS, nor any of their respective Affiliates, is an agent of the other for any purpose or has the authority to bind the other.

12.8 Language. All communications and Notices made or given pursuant to the Contract must be in the English language. If AWS provides a translation of the English language version of the Contract, the English language version of the Contract will control if there is any conflict.

12.9 Nondisclosure; Publicity: Except to the extent permitted by applicable law, neither Customer nor AWS will issue any press release or make any other public communication with respect to the Contract or Customer's use of the Service Offerings. AWS and Customer agree that some portions, of the Contract as approved by the Oklahoma State Purchasing Director, are not publicly known and will not be disclosed by them.



12.10 Notice.

(a) **General.** Except as otherwise set forth in Section 12.10(b), to give notice to a party under the Contract, each party must contact that other party by personal delivery, overnight courier or registered or certified mail. Notices must be sent to addressed to the address of the other party listed on the Cover Page to this Contract (or such other address as a party may subsequently provide in writing to the other party. Notices provided by personal delivery will be effective immediately. Notices provided by overnight courier will be effective one business day after they are sent. Notices provided by registered or certified mail will be effective three business days after they are sent.

(b) **Notice for purposes of this Contract:**

If sent to AWS:

410 Terry Avenue North
Seattle, WA 98109-5210
Attention: AWS General Counsel

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

(c) **Electronic Notice.** AWS may provide notice to Customer (i) under Sections 2.2 or 5.1 by (A) sending a message to the email address then associated with at least one of Customer's AWS Enterprise Accounts, or (B) posting a notice on the AWS Site, (ii) under Section 6 or Appendix A by sending a message to the email address then associated with Customer's applicable AWS Enterprise Account, and (iii) under Section 2.1 by sending a message to the email address then associated with at least one of Customer's AWS Enterprise Accounts (or such other email address as agreed upon by the parties) or via a support case. Any notices provided by posting on the AWS Site will be effective upon posting and notices provided by email will be effective when AWS sends the email.

12.11 No Third-Party Beneficiaries. Except as set forth in Section 9, the Contract does not create any third-party beneficiary rights in any individual or entity that is not a party to the Contract.

12.12 No Waivers. The failure by a party to enforce any provision of the Contract will not constitute a present or future waiver of such provision nor limit such party's right to enforce such provision at a later time. All waivers by a party must be provided in a Notice to be effective.

12.13 Reserved.

13. Definitions. Defined terms used in this Contract with initial letters capitalized have the meanings given below, unless the Definition has been otherwise modified by the parties in Attachment F:

"Acceptable Use Policy" means the policy located at <http://aws.amazon.com/aup> (and any successor or related locations designated by AWS), as it may be updated by AWS from time to time.



“Account Information” means information about Customer that Customer provides to AWS in the creation or administration of an AWS Enterprise Account. For example, Account Information includes names, usernames, phone numbers, email addresses and billing information associated with an AWS Enterprise Account.

“Affiliate” means any entity that directly or indirectly controls, is controlled by or is under common control with that party.

“API” means an application program interface.

“AWS Content” means Content that AWS or any of its Affiliates makes available related to the Services or on the AWS Site to allow access to and use of the Services, including APIs; WSDLs; sample code; software libraries; command line tools; proofs of concept, templates, and other related technology (including but not limited to any of the foregoing that are provided by any AWS personnel). AWS Content does not include the Services or Third-Party Content.

“AWS Contracting Party Site” means <https://aws.amazon.com/legal/aws-contracting-party> (and any successor or related locations designated by AWS), as may be updated by AWS from time to time.

“AWS Customer Agreement” means AWS’s standard user agreement located on the AWS Site at <http://aws.amazon.com/agreement> (and any successor or related locations designated by AWS), as may be updated by AWS from time to time.

“AWS Enterprise Account” means any AWS account that (a) is listed on Appendix A, as that list may be updated from time to time as described in Appendix A, (b) is opened by Customer using a Customer-issued email address (with an email domain name that is owned by Customer), (c) includes Customer’s full legal name in the “Company Name” field associated with the AWS account, and (d) is associated with a geographic location in the United States AWS determines the location associated with each AWS Enterprise Account in the manner described on the AWS Contracting Party Site.

“AWS Marks” means any trademarks, service marks, service or trade names, logos, and other designations of AWS and its Affiliates that AWS may make available to Customer in connection with this Contract.

“AWS Network” means AWS’s data center facilities, servers, networking equipment, storage media, and host software systems (e.g., virtual firewalls) that are within AWS’s control and are used to provide the Services.

“AWS Security Standards” means the security standards attached to this as Appendix B.

“AWS Site” means <http://aws.amazon.com> (and any successor or related locations designated by AWS), as may be updated by AWS from time to time.

“AWS Trademark Guidelines” means the guidelines and trademark license located at <http://aws.amazon.com/trademark-guidelines> (and any successor or related locations designated by AWS), as may be updated by AWS from time to time.

“Content” means software (including machine images), data, text, audio, video, or images.

“Customer Data” As defined in Attachment F, Information Technology Terms, Definitions (Section 1.2, pg. 1).

“Disputed Amounts” means amounts disputed by Customer in a Notice and in good faith as billing errors.

“Documentation” means the user guides and admin guides (in each case exclusive of content referenced via hyperlink) for the Services located at <http://aws.amazon.com/documentation> (and any successor or related locations designated by AWS), as such user guides and admin guides may be updated by AWS from time to time.

“End User” means any individual or entity that directly or indirectly through another user (a) accesses or uses Customer Data, or (b) otherwise accesses or uses the Service Offerings under an AWS Enterprise Account. The term “End User” does not include individuals or entities when they are accessing or using the Services or any Content under their own AWS account, rather than under an AWS Enterprise Account.

“Indirect Taxes” means applicable taxes and duties, including, without limitation, VAT, GST, excise taxes, sales and transactions taxes, and gross receipts tax.

“Intellectual Property License” means the separate license terms that apply to Customer’s access to and use of AWS Content and Services located at <https://aws.amazon.com/legal/aws-ip-license-terms> (and any successor or related locations), as may be updated from time to time.

“Losses” means any damages, losses, liabilities, costs and expenses (including reasonable attorneys’ fees).

“Notice” means any notice provided in accordance with Section 12.10.

“Policies” means the Acceptable Use Policy, Privacy Notice, and the Service Terms.

“Privacy Notice” means the privacy notice located at <http://aws.amazon.com/privacy> (and any successor or related locations designated by AWS), as may be updated by AWS from time to time.

“Service” means each of the services made available by AWS or its Affiliates for which Customer registers via the AWS Site (or by such other means made available by AWS), including those web services described in the Service Terms. Services do not include Third-Party Content.

“Service Attributes” means Service usage data related to an AWS Enterprise Account, such as resource identifiers, metadata tags, security and access roles, rules, usage policies, permissions, usage statistics and analytics.

“Service Level Agreement” means all service level agreements that AWS offers with respect to the Services and post on the AWS Site, as they may be updated by AWS from time to time. The service level agreements that AWS offers with respect to the Services are located at <https://aws.amazon.com/legal/service-level-agreements> (and any successor or related locations designated by AWS), as may be updated by AWS from time to time.

“Service Offerings” means the Services, the AWS Content, the AWS Marks, and any other product or service provided by AWS under the Contract. Service Offerings do not include Third-Party Content.

“Service Terms” means the rights and restrictions for particular Services located at <http://aws.amazon.com/serviceterms> (and any successor or related locations designated by AWS), as may be updated by AWS from time to time.

“Suggestions” means all suggested improvements to the Service Offerings that Customer provides to AWS.

“Third-Party Content” means Content of a third party made available on the AWS Marketplace or on developer forums, sample code repositories, public data repositories, community-focused areas of



the AWS Site, or any other part of the AWS Site that allows third parties to make available software, products, or data.

Appendix A

AWS Account ID(s):

The list above includes any Management Account or Member Accounts joined to such accounts via AWS Organizations, as described in the Service Terms.

Customer may add AWS accounts to the list above or remove AWS accounts from the list above by providing notice to AWS via email to aws-oklahoma-contract@amazon.com, that includes (1) Customer’s full name, (2) the Enterprise Agreement number (which begins with “CC” and is found on the upper right corner of each page of this Agreement), and (3) the AWS Account ID of each added or removed AWS account. Upon Notice, AWS may replace the notification process or make available another means of adding and removing AWS accounts to the list above.

Appendix B

AWS Security Standards

Capitalized terms not otherwise defined in this document have the meanings assigned to them in the applicable AWS Enterprise Agreement.

1. Information Security Program. AWS will maintain an information security program (including the adoption and enforcement of internal policies and procedures) designed to (a) satisfy the Security Objectives, (b) identify reasonably foreseeable and internal risks to security and unauthorized access to the AWS Network, and (c) minimize security risks, including through risk assessment and regular testing. AWS will designate one or more employees to coordinate and be accountable for the information security program. The information security program will include the following measures:

1.1 Network Security. The AWS Network will be electronically accessible to employees, contractors and any other person as necessary to provide the Services. AWS will maintain access controls and policies to manage what access is allowed to the AWS Network from each network connection and user, including the use of firewalls or functionally equivalent technology and authentication controls. AWS will maintain corrective action and incident response plans to respond to potential security threats.

1.2 Physical Security

1.2.1 Physical Access Controls. Physical components of the AWS Network are housed in nondescript facilities (the “**Facilities**”). Physical barrier controls are used to prevent unauthorized entrance to the Facilities both at the perimeter and at building access points. Passage through the physical barriers at the Facilities requires either electronic access control validation (e.g., card access systems, etc.) or validation by human security personnel (e.g., contract or in-house security guard service, receptionist, etc.). Employees and certain contractors are assigned photo-ID badges that must be worn while the employees and contractors are at any of the Facilities. Visitors and any other contractors are required to sign-in with designated personnel, must show appropriate identification, are assigned a visitor ID badge that must be worn while the visitor or contractor is at any of the Facilities, and are continually escorted by authorized employees or contractors while visiting the Facilities.

1.2.2 Limited Employee and Contractor Access. AWS provides access to the Facilities to those employees and contractors who have a legitimate business need for such access privileges. When an employee or contractor no longer has a business need for the access privileges assigned to him/her, the access privileges are promptly revoked, even if the employee or contractor continues to be an employee of AWS or its affiliates.

1.2.3 Physical Security Protections. All access points (other than main entry doors) are maintained in a secured (locked) state. Access points to the Facilities are monitored by video surveillance cameras designed to record all individuals accessing the Facilities. AWS also maintains electronic intrusion detection systems designed to detect unauthorized access to the Facilities, including monitoring points of vulnerability (e.g., primary entry doors, emergency egress doors, roof hatches, dock bay doors, etc.) with door contacts, glass breakage devices, interior motion-detection, or other devices designed to detect individuals attempting to gain access to the Facilities. All physical access to the Facilities by employees and contractors is logged and routinely audited.

2. Continued Evaluation. AWS will conduct periodic reviews of the security of its AWS Network and adequacy of its information security program as measured against industry security standards and its policies and procedures. AWS will continually evaluate the security of its AWS Network and associated Services to determine whether additional or different security measures are required to respond to new security risks or findings generated by the periodic reviews.

**Attachment E-1 to
STATE OF OKLAHOMA CONTRACT WITH AMAZON WEB SERVICES, INC.
RESULTING FROM SOLICITATION NO. 0900000556**

The FERPA requirements are hereby amended as set forth below and supersedes all prior
versions of this document

FERPA REQUIREMENTS

Data Privacy of Education Records. The parties acknowledge that the Family Educational Right and Privacy Act applies to education records included in Customer Data ("**FERPA Data**"). With respect to FERPA Data, Supplier, on behalf of itself and its employees, agrees to (a) be considered a "school official" with "legitimate educational interests" as those terms are used in 34 C.F.R. 99.31(a)(1), and (b) comply with the applicable requirements imposed by 34 C.F.R. 99.33(a) on school officials in effect as of the Effective Date and (c) and comply with the Oklahoma Student Data Accessibility, Transparency, and Accountability Act of 2013 (70 O.S. § 3-168) to the extent it is consistent with the Supplier's obligations under the Contract.

**Attachment E-1 to
STATE OF OKLAHOMA CONTRACT WITH AMAZON WEB SERVICES, INC.
RESULTING FROM SOLICITATION NO. 0900000556**

The IRS Publication 1075 Customer Appendix is hereby amended as set forth below and supersedes all prior documents submitted by **Amazon Web Services, Inc.** or discussed by the parties.

IRS Publication 1075 Customer Appendix

This IRS 1075 Appendix (this “**Appendix**”) is entered into by Amazon Web Services Inc. (“**AWS**”) and **Customer**. This Appendix supplements the AWS Enterprise Agreement under the Contract No. 1041 between Customer and AWS (the “**Contract**”). Unless otherwise defined in this Appendix, all capitalized terms in this Appendix have the meanings set forth in the Contract. The parties agree as follows.

1. General

1.1 Customer agrees that this Appendix only applies to Customer Data subject to IRS Publication 1075 and Services listed as those that can be configured to meet IRS Publication 1075 requirements at <https://aws.amazon.com/compliance/irs-1075/>, or its successor site.

1.2 AWS and Customer agrees that IRS Publication 1075 and Exhibit 7 - Safeguarding Contract Language will be satisfied as set forth in this Appendix.

2. Customer Responsibilities

2.1 Customer is solely responsible for ensuring that IRS Publication 1075 requirements are fulfilled prior to introducing Customer Data that includes Federal Tax Information (“FTI”), as defined under IRS Publication 1075, into the Service or Service Offerings. Customer agrees to configure the Services in such a manner that it prevents AWS from having logical access to Customer’s FTI.

2.2 Customers have a variety of options to choose from when configuring their accounts for all sensitive or otherwise valuable Customer Data including FTI. AWS recommends that Customer uses strong security and redundancy features, such as access controls, encryption, and backup. Customer is responsible for properly configuring and using the Service Offerings as Customer determines is appropriate, in order for Customer to comply with IRS Publication 1075 or other legal or regulatory requirements applicable to Customer.

2.3 Customer understands that AWS Services operate under a shared security model where security and compliance is a shared responsibility between AWS and the customer. Customers are responsible for security in the cloud and must configure the Services as part of its security responsibilities. Customer agrees that its compliance with IRS Publication 1075 is dependent upon on Customer’s configuration of the Services and adoption and implementation of policies and practices. Documentation for the Services includes information that may help the Customer comply with IRS Publication 1075 requirements.

3. Customer Inspection Rights

3.1 Provided that the Customer and AWS have a NDA in place, Customer will be provided (i) through AWS Artifact, access to information generated by AWS’s regular monitoring of security, privacy,



and operational controls in place to afford you an ongoing view into the effectiveness of such controls; and (ii) upon request, be afforded the opportunity to communicate with AWS's subject matter experts for clarification of the reports identified above.

3.2 Notwithstanding anything to the contrary in Attachment A, Customer will use the information from Section 3.1 herein to satisfy any inspection requirements under IRS Publication 1075. Customer agrees that the audit rights described in this section are the sole rights to be provided in full satisfaction of any audit that may otherwise be requested by the IRS or Customer. Notwithstanding anything to the contrary in Attachment A, AWS will not grant any inspection rights to Customer or access to data centers or other facilities that may cause AWS to be non-compliant with its contractual obligations under FedRAMP, ISO 27001/27018, other US Government security related operations, or its security policies.

3.3 Information provided by AWS is confidential and subject to the NDA. Upon request and pursuant to appropriate confidentiality protections, Customer shall be permitted to provide information described in Section 3.1 to the IRS to satisfy the IRS inspection requirements under IRS Publication 1075.

Attachment A**(IRS Publication 1075, Exhibit 7)****I. PERFORMANCE**

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

- (1) All work will be performed under the supervision of the contractor.
- (2) 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.
- (3) 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.
- (4) 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.
- (5) 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.
- (6) 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.
- (7) All 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.
- (8) No work involving FTI furnished under this contract will be subcontracted without the prior written approval of the IRS.

- (9) Contractor will ensure that the terms of FTI safeguards described herein are included, without modification, in any approved subcontract for work involving FTI.
- (10) 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.
- (11) 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.
- (12) 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.
- (13) The agency will have the right to void the contract if the contractor fails to meet the terms of FTI safeguards described herein.

II. CRIMINAL/CIVIL SANCTIONS

- (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.
- (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.
- (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.
- (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.

- (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 Exhibit 4, Sanctions for Unauthorized Disclosure](#), and [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. (See Section 10) 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.

III. 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.

**Attachment E-1 to
STATE OF OKLAHOMA CONTRACT WITH AMAZON WEB SERVICES, INC.
RESULTING FROM SOLICITATION NO. 0900000556**

Minimum Architecture Requirements

Held as Confidential

The Pricing is hereby amended as set forth below and supersedes all prior versions of this document

Amazon Web Services, Inc. Response to OK OMES RFP Solicitation No. 0900000556

Section 9: Pricing

Table of Contents

Tab	Description
<u>Exhibit 1 Price Template</u>	Provided pricing template from the State of Oklahoma Office of Management and Enterprise Services (OK OMES). Contains Amazon Web Services (AWS) manufacturer’s suggested retail price (MSRP) or standard commercial rate for AWS Cloud Services, AWS Marketplace, and AWS Professional Services.
<u>AWS Pricing Index</u>	AWS provides commercial off-the-shelf (COTS) cloud services, and we provide our pricing in our MSRP format in the tab AWS Pricing Index for AWS Support and AWS Training services.
<u>Complementary Services</u>	Free service list which details Complementary Management, Monitoring and Support Services as described in Section 10.6 , as well as Cost Savings and Optimizations as detailed in Section 8.4.7 .

Please Note:

1. As discussed in Section 8.4.7 Cost Savings and Optimizations, AWS has multiple mechanisms and frameworks that enable customers to take advantage of pricing incentives and volumes discounts.
2. Since AWS provides commercial off-the-shelf (COTS) cloud services, we provide our pricing in our MSRP format. While AWS does not provide a per line item discount, we will not charge the contract management fee. Therefore, OK OMES customers will receive an effective discount of 1.00% for the offerings set forth in our bid response.
3. AWS retains the right to change its prices.

This document is provided for informational purposes only. It represents AWS’s current product offerings and practices as of the date of issue of this document and is subject to change. The responsibilities and liabilities of AWS to its customers are controlled by AWS agreements, and this document is not part of, nor does it modify, any agreement between AWS and its customers. For current services and prices for AWS Services, please refer to the AWS website at www.aws.amazon.com or contact your AWS Sales Representative.



Amazon Web Services, Inc. Response to OK OMES RFP Solicitation No. 0900000556

Section 9: Pricing

Exhibit I Price Template

SW1041 Software

Software Publishers		
Description	Maximum Cost + % Markup	% off List Price
Cloud Services - Amazon Web Services (AWS) provides commercial off-the-shelf (COTS) cloud services provided at our commercial manufacturer's suggested retail price (MSRP). AWS offers over 200 fully featured global services related to compute, storage, databases, analytics, networking, machine learning, mobile, developer tools, management and governance, IoT, security, enterprise applications, and more.	MSRP, Please refer to aws.amazon.com/pricing/ for current AWS Service prices. Configure unique cost estimates using the AWS Pricing Calculator at https://calculator.aws/#/?ch=cta&cta=lower-pricing-calc	0.00%
AWS Marketplace - AWS Marketplace is a curated digital catalog with thousands of software listings from independent software venders (ISV) making it easy to find, test, buy, and deploy software, professional services, and data listings. AWS Marketplace is a sell through channel for ISVs as well as an AWS Service. Buyers establish pricing and license terms directly with ISVs, and these transactions are made through the buyer's AWS bill. ISVs define pricing and licensing terms. As illustrated in Section 10.2.1 Value Added Products and Services, Streamlined and Flexible Procurement, customers can negotiate additional savings directly with ISVs though the use of Private Offers.	MSRP, Please refer to https://aws.amazon.com/marketplace for current AWS Marketplace prices	0.00%

Other Value Add Products and Services		
Description	Maximum Cost + % Markup	% off List Price
AWS Basic Support	Please refer to AWS Pricing Index Tab inserted into this file	0.00%
AWS Developer Support	Please refer to AWS Pricing Index Tab inserted into this file	0.00%
AWS Business Support	Please refer to AWS Pricing Index Tab inserted into this file	0.00%
AWS Enterprise On-Ramp	Please refer to AWS Pricing Index Tab inserted into this file	0.00%
AWS Enterprise Support	Please refer to AWS Pricing Index Tab inserted into this file	0.00%
Instructor Led Training Per Day (Maximum of 25 Students Per Day)	Please refer to AWS Pricing Index Tab inserted into this file	0.00%
AWS Skill Builder Team Subscription Cost Per Person Per Year	Please refer to AWS Pricing Index Tab inserted into this file	0.00%
AWS Foundational Certification	Please refer to AWS Pricing Index Tab inserted into this file	0.00%
AWS Associate Certification	Please refer to AWS Pricing Index Tab inserted into this file	0.00%
AWS Professional Certification	Please refer to AWS Pricing Index Tab inserted into this file	0.00%
AWS Specialty Certification	Please refer to AWS Pricing Index Tab inserted into this file	0.00%

Professional Services		
Description	List Price	Discounted Hourly Rates
AWS Professional Services provides consulting and advisory services to help accelerate our customers' enterprise cloud adoption by delivering business and technology outcomes. We deliver focused guidance through our global specialty practices, which cover a variety of solutions, technologies, and industries/verticals (i.e., Application Migration, Modernization & Management, Data & Analytics, Emerging Technologies & Intelligence, Security & Infrastructure, etc.). We also provide assistance through a portfolio of pre-packaged offerings which help you achieve specific outcomes. AWS offers AWS Professional Services on a firm fixed price (FFP) 40 hour (per unit) basis, based on our standard commercial rate. For clarification purposes, a single AWS Professional Service unit is not less than 40-hours. Any "unit" of services provided by AWS Professional Services can involve support from a variety of AWS Professional Services resources with background/skills relevant to a customer's specific goals. Rather than providing a single labor category in any "unit" of AWS Professional Services, we offer a blend of categories based on the scope of required services.	[TBD upon scope of AWS Professional Services]	N/A

*AWS Professional Services is delivered and invoiced on a per FFP unit basis and prices may increase over time. An FFP "Unit" comprises approximately 40 labor hours. Customers will only be billed for actual Units worked and only after the Unit is fully expended. Customers can pause or stop the engagement at any time for any reason and will not be billed on any unused AWS Professional Services Units.

Please Note:
Use or disclosure of data contained on this sheet is subject to the restriction on the title page of this document

Amazon Web Services, Inc. Response to OK OMES RFP Solicitation No. 0900000556

Section 9: Pricing

AWS Pricing Index

Use or disclosure of data contained on this sheet is subject to the restriction on the title page of this document.

Service*	Current List Price
AWS Basic Support	Included with all AWS Services
AWS Developer Support	For current prices, please refer to the AWS website at www.aws.amazon.com or contact your AWS Sales Representative.
AWS Business Support	
AWS Enterprise On-Ramp	
AWS Enterprise Support	

*Purchase of AWS Support is not required for the purchase of AWS Services.

Service	Service Description (provide detailed service features)	Current List Price	Unit of Measure
AWS Training	Instructor Led Training Per Day (Maximum of 25 Students Per Day)	For current services and prices for AWS Services, please refer to the AWS website at www.aws.amazon.com or contact your AWS Sales Representative.	Per Day
AWS Training	AWS Skill Builder Team Subscription Cost Per Person Per Year		Per Person
AWS Certification	AWS Foundational Certification		Per Person
AWS Certification	AWS Associate Certification		Per Person
AWS Certification	AWS Professional Certification		Per Person
AWS Certification	AWS Specialty Certification		Per Person
AWS Training	AWS Training - On-Site AWS Instructor Lead Private Training Pricing - Instructor Travel Fee - 1 Day		Per Instructor
AWS Training	AWS Training - On-Site AWS Instructor Lead Private Training Pricing - Instructor Travel Fee - 2 Days		Per Instructor
AWS Training	AWS Training - On-Site AWS Instructor Lead Private Training Pricing - Instructor Travel Fee - 3 Days		Per Instructor
AWS Training	AWS Training - On-Site AWS Instructor Lead Private Training Pricing - Instructor Travel Fee - 4 Days		Per Instructor
AWS Training	AWS Training - On-Site AWS Instructor Lead Private Training Pricing - Instructor Travel Fee - 5 Days		Per Instructor



Amazon Web Services, Inc. Response to OK OMES RFP Solicitation No. 090000556		
Section 9: Pricing		
Complementary AWS Services		
Note: AWS offers a suite of supporting tools and features provided at no additional cost to facilitate optimized and secure cloud operations and achieve cost efficiencies. This list is subject to change. For additional information, please refer to the AWS website at www.aws.amazon.com or contact your AWS Sales Representative:		
Service	Description of Service	Value to OK OMES Mission
Amazon EC2 Auto Scaling	Automatically adds or removes Amazon EC2 instances according to user-defined conditions	<ul style="list-style-type: none">• Improve fault tolerance• Increase application availability• Lower costs
AWS Auto Scaling	Monitors applications and automatically adjusts capacity to maintain steady, predictable performance at the lowest possible cost	<ul style="list-style-type: none">• Set up scaling quickly• Make smart scaling decisions• Automatically maintain performance• Pay only for what is needed
AWS CloudFormation	Accelerates cloud provisioning with infrastructure as code	<ul style="list-style-type: none">• Automate best practices• Scale infrastructure• Integrate with other AWS Cloud services• Manage third-party and private resources• Use for free for specified namespaces here
AWS Command Line Interface (AWS CLI)	Manages AWS Cloud services through a unified tool	<ul style="list-style-type: none">• Manage resources from the command line• Produce repeatable scripts and documentation
AWS Elastic Beanstalk	Deploys and scales web applications and services developed with Java, .NET, PHP, Node.js, Python, Ruby, Go, and Docker on familiar servers such as Apache, Nginx, Passenger, and IIS	<ul style="list-style-type: none">• Automatically handle the deployment details of capacity provisioning, load balancing, automatic scaling, and application health monitoring• Save valuable developer time• Handle peaks in workload or traffic while minimizing cost and maintaining resource control
IAM	Securely manages access to AWS Cloud services and resources	<ul style="list-style-type: none">• Maintain fine-grained access control to AWS resources• Implement multi-factor authentication for highly privileged users• Analyze access• Integrate with existing directories
AWS License Manager	Sets rules to manage, discover, and report software license usage	<ul style="list-style-type: none">• Gain control over license usage• Get a centralized view of license usage so that administrators can determine the right number of licenses to purchase• Give administrators the ability to set limits for license usage
AWS Management Console	Allows access and management of the AWS Cloud in one web interface	<ul style="list-style-type: none">• Securely log in using AWS or IAM account credentials• Offer browser and mobile application• Provide easy search and navigation• Gain access to tutorials, documentation, on-demand webinars, and more
AWS Marketplace	Offers thousands of software listings in a digital catalog from independent software vendors that make it easy to find, test, purchase, and deploy software that runs on AWS	<ul style="list-style-type: none">• Provide flexibility and additional opportunities to purchase software to enable innovation
AWS Organizations	Centrally manages and governs environments as AWS resources scale	<ul style="list-style-type: none">• Manage costs and optimize usage• Quickly scale workloads• Provide custom environments for different workloads• Centrally secure and audit environments across accounts• Gain simple permission management and access control• Efficiently provision resources across accounts
AWS Private Marketplace	Creates a customized, private catalog of pre-approved products from AWS Marketplace	<ul style="list-style-type: none">• Govern which products users can run on AWS by making it possible to see only products that comply with [Customer] policies
AWS STS	Requests temporary, limited-privilege credentials for AWS IAM users or for users that [Customer] authenticates (federated users)	<ul style="list-style-type: none">• Provide additional flexibility in user management
AWS Pricing Calculator	Estimates monthly AWS bill more efficiently through a web tool	<ul style="list-style-type: none">• Gain additional options for cost management
AWS Cost Explorer Application Programming Interface (AWS Cost Explorer API)	Programmatically queries cost and usage data	<ul style="list-style-type: none">• Use a simple tool for cost management and optimization
AWS Price List API	Queries for the prices of AWS Cloud services using either JSON (with the Price List Service API) or HTML (with the AWS Price List API)	<ul style="list-style-type: none">• Easily obtain prices of AWS Cloud services
AWS Resource Access Manager (RAM)	Securely shares AWS resources with any AWS account or within your AWS Organization including AWS Transit Gateways, subnets, AWS License Manager configurations, and Amazon Route 53 Resolver rules resources	<ul style="list-style-type: none">• Allow for reduction of operational overhead, improved security and visibility, and cost optimization
AWS Cloud Economics Support	Provides complementary support for customers with greater than \$1M in annual spend; an expert will assist with assessing cost optimization opportunities, performing value realization studies, and recommending financial management activities	<ul style="list-style-type: none">• Discuss current and future cloud optimization based on specific customer needs and plans with a cloud economics expert
AWS Cloud9	Lets you write, run, debug your code with just a browser through a cloud-based integrated development environment (IDE)	<ul style="list-style-type: none">• Enable real time collaborative coding to launch projects quickly
AWS Software Development Kits (SDKs)	Uses SDKs to take the complexity out of coding by providing language-specific APIs for AWS services	<ul style="list-style-type: none">• Expedite application development
AWS Cloud Development Kit (CDK)	Defines your cloud application resources using familiar programming languages with an open source software development framework	<ul style="list-style-type: none">• Provide high-level constructs that preconfigure cloud resources with proven defaults, so customers can build cloud applications without needing to be an expert
AWS Deep Learning Amazon Machine Image (AMI)	Provides infrastructure and tools to accelerate deep learning in the cloud at any scale	<ul style="list-style-type: none">• Quickly define models and train them at scale
AWS Shield Standard	Provides a managed distributed denial of service (DDoS) protection service	<ul style="list-style-type: none">• Defend against most common, frequently occurring network and transport layer DDoS attacks that target your web site or applications, minimizing down time and latency
AWS Personal Health Dashboard	Provides a personalized view into the performance and availability of the AWS Cloud services underlying your AWS resources	<ul style="list-style-type: none">• Receive alerts and remediation guidance to minimize the impact of service events
AWS Service Health Dashboard	Shows up-to-the-minute information on availability of all AWS Cloud services	<ul style="list-style-type: none">• Receive real time notifications of any service interruption to expedite mitigation activities

Additional Opportunities for Cost Savings with AWS	
Opportunity for Saving	Description
Reserved Instances	Reserved Instances (RI) provide customers with significant savings (up to 75%) compared to On-Demand EC2 Instance pricing. Customers have the option to commit to a one or three-year term with three payment options—No Upfront, Partial Upfront, and All Upfront—enabling them to balance the amount they pay upfront with their effective hourly price.
Savings Plan	Savings Plans offer a flexible pricing model that provide savings on AWS usage beyond On-Demand rates in exchange for a commitment of using a specified amount of compute power (measured per hour) for a one or three year period. You can save up to 72 percent on your AWS compute workloads. Compute Savings Plans provide lower prices on Amazon EC2 instance usage regardless of instance family, size, OS, tenancy, or AWS Region. This also applies to AWS Fargate and AWS Lambda usage. SageMaker Savings Plans provide you with lower prices for your Amazon SageMaker instance usage, regardless of your instance family, size, component, or AWS Region. EC2 Instance Savings Plans provide the same level of discount as an RI (up to 75%) but allow for greater flexibility. You can manage your plans by using recommendations, performance reporting, and budget alerts in the AWS Cost Explorer.



Storage Tier Discounts	AWS provides three tiers of pricing for Amazon Simple Storage Service (Amazon S3) based on the total amount of data stored. The more data stored, the lower the rate. If data access patterns fluctuate over time, then customers can leverage Amazon S3 Intelligent-Tiering to systematically move data between frequent access and infrequent access storage tiers to deliver automatic cost optimization.
------------------------	--

Use or disclosure of data contained on this sheet is subject to the restriction on the title page of this document





**Attachment E-1 to
STATE OF OKLAHOMA CONTRACT WITH AMAZON WEB SERVICES, INC.
RESULTING FROM SOLICITATION NO. 0900000556**

The AWS Professional Services- Statement of Work template is hereby amended as set forth below and supersedes all prior versions of this document. The parties agree to use this document or a similar version of this document.

AWS Professional Services – Statement of Work

"Customer"	
"AWS"	
Project Name	
"Project Location"	
Customer's Engagement Contact Name and Email Address	
Customer's Accounts Payable / Bill To / Name and Email Address	
Customer's Bill-To Mailing Address	
Customer's Bill-To Phone Number	
Customer's AWS Billing Account ID	
Currency	

This Statement of Work for AWS Professional Services (this **"SOW"**) is entered into between AWS and Customer. This SOW is made a part of the Enterprise Agreement, by and between Customer and Amazon Web Services Inc. (the **"Agreement"**). This SOW is effective as of the date the last party signs this SOW (the **"SOW Effective Date"**). Capitalized terms not defined in this SOW may be defined in the Contract.





Scope of the AWS Professional Services

{To be Determined}

Customer Responsibilities

{Customer responsibilities to be determined upon the scope of AWS Professional Services}

Schedule of Rates

{Schedule of Rates to be determined upon the scope of AWS Professional Services}

Engagement Related Expenses

{Engagement Related Expenses to be determined upon the scope of AWS Professional Services}

Additional Terms

{Additional Terms to be determined upon the scope of AWS Professional Services}



Acceptance and authorization

IN WITNESS WHEREOF, the parties below have executed this SOW as of the SOW Effective Date.

AWS:

CUSTOMER:

Amazon Web Services, Inc.

DRAFT – NOT FOR SIGNATURE	DRAFT – NOT FOR SIGNATURE
Signature	Signature
Full name	Full name
Title	Title
Date	Date



**Attachment E-1 to
STATE OF OKLAHOMA CONTRACT WITH AMAZON WEB SERVICES, INC.
RESULTING FROM SOLICITATION NO. 0900000556**

The DPA is hereby amended as set forth below and supersedes all prior versions of this document

DATA PROCESSING APPENDIX TO THE AWS ENTERPRISE AGREEMENT

This Data Processing Appendix supplements the AWS Enterprise Agreement under the Contract (the “**Agreement**”) and shall not diminish each party’s rights and responsibilities under the Contract. Unless otherwise defined in this Appendix or in the Agreement, all capitalized terms used in this Appendix will have the meanings given to them in Section 17 of this Appendix.

1. Data Processing.

- 1.1 **Scope and Roles.** This Appendix applies when Customer Personal Data is processed by AWS. In this context, AWS will act as processor to Customer, who can act either as controller or processor of Customer Personal Data.
- 1.2 **Customer Controls.** Customer can use the Service Controls to assist it with its obligations under Applicable Data Protection Law, including its obligations to respond to requests from data subjects. Taking into account the nature of the processing, Customer agrees that it is unlikely that AWS would become aware that Customer Personal Data transferred under the Standard Contractual Clauses is inaccurate or outdated. Nonetheless, if AWS becomes aware that Customer Personal Data transferred under the Standard Contractual Clauses is inaccurate or outdated, it will inform Customer without undue delay. AWS will cooperate with Customer to erase or rectify inaccurate or outdated Customer Personal Data transferred under the Standard Contractual Clauses by providing the Service Controls that Customer can use to erase or rectify Customer Personal Data.
- 1.3 **Details of Data Processing.**
 - 1.3.1 **Subject matter.** The subject matter of the data processing under this Appendix is Customer Personal Data.
 - 1.3.2 **Duration.** As between AWS and Customer, the duration of the data processing under this Appendix is determined by Customer.
 - 1.3.3 **Purpose.** The purpose of the data processing under this Appendix is the provision of the Services initiated by Customer from time to time.
 - 1.3.4 **Nature of the processing.** Compute, storage and such other Services as described in the Documentation and initiated by Customer from time to time.
 - 1.3.5 **Type of Customer Personal Data.** Customer Personal Data uploaded to the Services under Customer’s AWS accounts.

- 1.3.6 **Categories of data subjects.** The data subjects could include Customer's customers, employees, suppliers and End Users.
- 1.4 **Compliance with Laws.** Each party will comply with all laws, rules and regulations applicable to it and binding on it in the performance of this Appendix, including Applicable Data Protection Law.
2. **Customer Instructions.** The parties agree that this Appendix and the Agreement (including Customer providing instructions via configuration tools such as the AWS management console and APIs made available by AWS for the Services) constitute Customer's documented instructions regarding AWS's processing of Customer Personal Data ("**Documented Instructions**"). AWS will process Customer Personal Data only in accordance with Documented Instructions (which if Customer is acting as a processor, could be based on the instructions of its controllers). Additional instructions outside the scope of the Documented Instructions (if any) require prior written agreement between AWS and Customer, including agreement on any additional fees payable by Customer to AWS for carrying out such instructions. Customer is entitled to terminate this Appendix and the Agreement if AWS declines to follow instructions requested by Customer that are outside the scope of, or changed from, those given or agreed to be given in this Appendix. Taking into account the nature of the processing, Customer agrees that it is unlikely AWS can form an opinion on whether Documented Instructions infringe Applicable Data Protection Law. If AWS forms such an opinion, it will immediately inform Customer, in which case, Customer is entitled to withdraw or modify its Documented Instructions.
3. **Confidentiality of Customer Personal Data.** AWS will not access or use, or disclose to any third party, any Customer Personal Data, except, in each case, as necessary to maintain or provide the Services, or as necessary to comply with the law or a valid and binding order of a governmental body (such as a subpoena or court order). If a governmental body sends AWS a demand for Customer Personal Data, AWS will attempt to redirect the governmental body to request that data directly from Customer. As part of this effort, AWS may provide Customer's basic contact information to the governmental body. If compelled to disclose Customer Personal Data to a governmental body, then AWS will give Customer reasonable notice of the demand to allow Customer to seek a protective order or other appropriate remedy unless AWS is legally prohibited from doing so.
4. **Confidentiality Obligations of AWS Personnel.** AWS restricts its personnel from processing Customer Personal Data without authorization by AWS as described in the Security Standards. AWS imposes appropriate contractual obligations upon its personnel, including relevant obligations regarding confidentiality, data protection and data security.
5. **Security of Data Processing**
- 5.1 AWS has implemented and will maintain the technical and organizational measures for the AWS Network as described in the Security Standards and this Section. In particular, AWS has implemented and will maintain the following technical and organizational measures:
- (a) security of the AWS Network as set out in Section 1.1 of the Security Standards;
 - (b) physical security of the facilities as set out in Section 1.2 of the Security Standards;

- (c) measures to control access rights for authorized personnel to the AWS Network as set out in Section 1.3 of the Security Standards; and
 - (d) processes for regularly testing, assessing and evaluating the effectiveness of the technical and organizational measures implemented by AWS as described in Section 2 of the Security Standards.
- 5.2 Customer can elect to implement technical and organizational measures to protect Customer Personal Data. Such technical and organizational measures include the following which can be obtained by Customer from AWS as described in the Documentation, or directly from a third party supplier:
 - (a) pseudonymization and encryption to ensure an appropriate level of security;
 - (b) measures to ensure the ongoing confidentiality, integrity, availability and resilience of the processing systems and services that are operated by Customer;
 - (c) measures to allow Customer to backup and archive appropriately in order to restore availability and access to Customer Personal Data in a timely manner in the event of a physical or technical incident; and
 - (d) processes for regularly testing, assessing and evaluating the effectiveness of the technical and organizational measures implemented by Customer.

6. Sub-processing.

- 6.1 **Authorized Sub-processors.** Customer provides general authorization to AWS's use of sub-processors to provide processing activities on Customer Personal Data on behalf of Customer ("**Sub-processors**") in accordance with this Section. The AWS website (currently posted at <https://aws.amazon.com/compliance/sub-processors/>) lists Sub-processors that are currently engaged by AWS. At least 30 days before AWS engages a Sub-processor, AWS will update the applicable website and provide Customer with a mechanism to obtain notice of that update. To object to a Sub-processor, Customer can:
 - (i) terminate the Agreement pursuant to its terms; (ii) cease using the Service for which AWS has engaged the Sub-processor; or (iii) move the relevant Customer Personal Data to another Region where AWS has not engaged the Sub-processor.
- 6.2 **Sub-processor Obligations.** Where AWS authorizes a Sub-processor as described in Section 6.1:
 - (i) AWS will restrict the Sub-processor's access to Customer Personal Data only to what is necessary to provide or maintain the Services in accordance with the Documentation, and AWS will prohibit the Sub-processor from accessing Customer Personal Data for any other purpose;
 - (ii) AWS will enter into a written agreement with the Sub-processor and, to the extent that the Sub-processor performs the same data processing services provided by AWS under this Appendix, AWS will impose on the Sub-processor the same contractual obligations that AWS has under this Appendix; and
 - (iii) AWS will remain responsible for its compliance with the obligations of this Appendix and for any acts or omissions of the Sub-processor that cause AWS to breach any of AWS's obligations under this Appendix.

7. **AWS Assistance with Data Subject Requests.** Taking into account the nature of the processing, the Service Controls are the technical and organizational measures by which AWS will assist Customer in fulfilling Customer's obligations to respond to data subjects' requests under Applicable Data Protection Law. If a data subject makes a request to AWS, AWS will promptly forward such request to Customer once AWS has identified that the request is from a data subject for whom Customer is responsible. Customer authorizes on its behalf, and on behalf of its controllers when Customer is acting as a processor, AWS to respond to any data subject who makes a request to AWS, to confirm that AWS has forwarded the request to Customer. The parties agree that Customer's use of the Service Controls and AWS forwarding data subjects' requests to Customer in accordance with this Section, represent the scope and extent of Customer's required assistance.
8. **Optional Security Features.** AWS makes available many Service Controls that Customer can elect to use. Customer is responsible for (a) implementing the measures described in Section 5.2, as appropriate, (b) properly configuring the Services, (c) using the Service Controls to allow Customer to restore the availability and access to Customer Personal Data in a timely manner in the event of a physical or technical incident (for example backups and routine archiving of Customer Personal Data), and (d) taking such steps as Customer considers adequate to maintain appropriate security, protection, and deletion of Customer Personal Data, which includes use of encryption technology to protect Customer Personal Data from unauthorized access and measures to control access rights to Customer Personal Data.
9. **DPA Security Incident Notification.**
 - 9.1 **DPA Security Incident.** AWS will (a) notify Customer of a DPA Security Incident without undue delay after becoming aware of the DPA Security Incident, and (b) take appropriate measures to address the DPA Security Incident, including measures to mitigate any adverse effects resulting from the DPA Security Incident.
 - 9.2 **AWS Assistance.** To enable Customer to notify a DPA Security Incident to supervisory authorities or data subjects (as applicable), AWS will cooperate with and assist Customer by including in the notification under Section 9.1(a) such information about the DPA Security Incident as AWS is able to disclose to Customer, taking into account the nature of the processing, the information available to AWS, and any restrictions on disclosing the information, such as confidentiality. Taking into account the nature of the processing, Customer agrees that it is best able to determine the likely consequences of a DPA Security Incident.
 - 9.3 **Unsuccessful DPA Security Incidents.** Customer agrees that:
 - (i) an unsuccessful DPA Security Incident will not be subject to this Section 9. An unsuccessful DPA Security Incident is one that results in no unauthorized access to Customer Personal Data or to any of AWS's equipment or facilities storing Customer Personal Data, and could include, without limitation, pings and other broadcast attacks on firewalls or edge servers, port scans, unsuccessful log-on attempts, denial of service attacks, packet sniffing (or other unauthorized access to traffic data that does not result in access beyond headers) or similar incidents; and

- (ii) AWS's obligation to report or respond to a DPA Security Incident under this Section 9 is not and will not be construed as an acknowledgement by AWS of any fault or liability of AWS with respect to the DPA Security Incident.

9.4 **Communication.** Notification(s) of DPA Security Incidents, if any, will be delivered to one or more of Customer's administrators by any means AWS selects, including via email. It is Customer's sole responsibility to ensure Customer's administrators maintain accurate contact information on the AWS management console and secure transmission at all times.

9.5 **Notification Obligations.** If AWS notifies Customer of a DPA Security Incident, or Customer otherwise becomes aware of any accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Customer Personal Data, Customer will be responsible for (a) determining if there is any resulting notification or other obligation under Applicable Data Protection Law and (b) taking necessary action to comply with those obligations. This does not limit AWS's obligations under this Section 9.

10. AWS Certifications and Audits.

10.1 **AWS ISO-Certification and SOC Reports.** In addition to the information contained in this Appendix, upon Customer's request, and provided that the parties have an applicable NDA in place, AWS will make available the following documents and information:

- (i) the certificates issued for the ISO 27001 certification, the ISO 27017 certification, the ISO 27018 certification, and the ISO 27701 certification (or the certifications or other documentation evidencing compliance with such alternative standards as are substantially equivalent to ISO 27001, ISO 27017, ISO 27018, and ISO 27701); and
- (ii) the System and Organization Controls (SOC) 1 Report, the System and Organization Controls (SOC) 2 Report and the System and Organization Controls (SOC) 3 Report (or the reports or other documentation describing the controls implemented by AWS that replace or are substantially equivalent to the SOC 1, SOC 2 and SOC 3).

10.2 **AWS Audits.** AWS uses external auditors to verify the adequacy of its security measures, including the security of the physical data centers from which AWS provides the Services. This audit: (a) will be performed at least annually; (b) will be performed according to ISO 27001 standards or such other alternative standards that are substantially equivalent to ISO 27001; (c) will be performed by independent third party security professionals at AWS's selection and expense; and (d) will result in the generation of an audit report ("**Report**"), which will be AWS's Confidential Information.

10.3 **Audit Reports.** At Customer's written request, and provided that the parties have an applicable NDA in place, AWS will provide Customer with a copy of the Report so that Customer can reasonably verify AWS's compliance with its obligations under this Appendix.

10.4 **Privacy Impact Assessment and Prior Consultation.** Taking into account the nature of the processing and the information available to AWS, AWS will assist Customer in complying with Customer's obligations in respect of data protection impact assessments and prior consultation, by providing the information AWS makes available under this Section 10.

- 11. Customer Audits.** Customer chooses to conduct any audit, including any inspection, it has the right to request or mandate on its own behalf, and on behalf of its controllers when Customer is acting as a processor, under Applicable Data Protection Law or the Standard Contractual Clauses, by instructing AWS to carry out the audit described in Section 10. If Customer wishes to change this instruction regarding the audit, then Customer has the right to request a change to this instruction by sending AWS written notice as provided for in the Agreement. If AWS declines to follow any instruction requested by Customer regarding audits, including inspections, Customer is entitled to terminate the Agreement in accordance with its terms.
- 12. Transfers of Personal Data.**

 - 12.1 Regions.** Customer can specify the location(s) where Customer Personal Data will be processed within the AWS Network (each a “**Region**”), including Regions in the EEA. Once Customer has made its choice, AWS will not transfer Customer Personal Data from Customer’s selected Region(s) except as necessary to provide the Services initiated by Customer, or as necessary to comply with the law or valid and binding order of a governmental body.
 - 12.2 Application of Standard Contractual Clauses.** Subject to Section 12.3, the Standard Contractual Clauses will only apply to Customer Personal Data subject to the GDPR that is transferred, either directly or via onward transfer, to any Third Country (each a “**Data Transfer**”).

 - 12.2.1** When Customer is acting as a controller, the Controller-to-Processor Clauses will apply to a Data Transfer.
 - 12.2.2** When Customer is acting as a processor, the Processor-to-Processor Clauses will apply to a Data Transfer. Taking into account the nature of the processing, Customer agrees that it is unlikely that AWS will know the identity of Customer’s controllers because AWS has no direct relationship with Customer’s controllers and therefore, Customer will fulfil AWS’s obligations to Customer’s controllers under the Processor-to-Processor Clauses.
 - 12.3 Alternative Transfer Mechanism.** The Standard Contractual Clauses will not apply to a Data Transfer if AWS has adopted Binding Corporate Rules for Processors or an alternative recognized compliance standard for lawful Data Transfers.
- 13. Termination of the Appendix.** This Appendix will continue in force until the termination of the Agreement (the “**Termination Date**”).
- 14. Return or Deletion of Customer Personal Data.** At any time up to the Termination Date, and for 90 days following the Termination Date, subject to the terms and conditions of the Agreement, AWS will return or delete Customer Personal Data when Customer uses the Service Controls to request such return or deletion. No later than the end of this 90-day period, Customer will close all AWS accounts containing Customer Personal Data.
- 15. Duties to Inform.** Where Customer Personal Data becomes subject to confiscation during bankruptcy or insolvency proceedings, or similar measures by third parties while being processed by AWS, AWS will inform Customer without undue delay. AWS will, without undue delay, notify all relevant parties in such action (for example creditors, bankruptcy trustee) that any Customer Personal Data subjected to those proceedings is Customer’s property and area of responsibility and that Customer Personal Data is at Customer’s sole disposition.

- 16. Entire Agreement; Conflict.** This Appendix incorporates the Standard Contractual Clauses by reference. This Appendix supersedes and replaces all prior or contemporaneous representations, understandings, agreements, or communications between Customer and AWS, whether written or oral, regarding the subject matter of this Appendix, including any data processing addenda entered into between Amazon Web Services, Inc. and Customer containing terms and conditions about Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data. Nothing in this document varies or modifies the Standard Contractual Clauses.
- 17. Definitions.** Unless otherwise defined in the Agreement, all capitalized terms used in this Appendix will have the meanings given to them below:
- “**API**” means an application program interface.
- “**Applicable Data Protection Law**” means all laws and regulations applicable to and binding on the processing of Customer Personal Data by a party, including, as applicable, the GDPR.
- “**AWS Network**” means the servers, networking equipment, and host software systems (for example, virtual firewalls) that are within AWS’s control and are used to provide the Services.
- “**Binding Corporate Rules**” has the meaning given to it in the GDPR.
- “**controller**” has the meaning given to it in the GDPR.
- “**Controller-to-Processor Clauses**” means the standard contractual clauses between controllers and processors for Data Transfers, as approved by the European Commission Implementing Decision (EU) 2021/914 of 4 June 2021, and currently located at https://d1.awsstatic.com/Controller_to_Processor_SCCs.pdf.
- “**Customer Personal Data**” means the Personal Data that is uploaded to the Services under Customer’s AWS accounts.
- “**Documentation**” means the then-current documentation for the Services located at <http://aws.amazon.com/documentation> (and any successor locations designated by AWS).
- “**EEA**” means the European Economic Area.
- “**GDPR**” means Regulation 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).
- “**NDA**” means the most recent Mutual Nondisclosure Agreement between the parties or their respective Affiliates applicable to the relationship contemplated by this Agreement, if any.
- “**Personal Data**” means personal data, personal information, personally identifiable information or other equivalent term (each as defined in Applicable Data Protection Law).
- “**processing**” has the meaning given to it in the GDPR and “process”, “processes” and “processed” will be interpreted accordingly.
- “**processor**” has the meaning given to it in the GDPR.

“Processor-to-Processor Clauses” means the standard contractual clauses between processors for Data Transfers, as approved by the European Commission Implementing Decision (EU) 2021/914 of 4 June 2021, and currently located at [https://d1.awsstatic.com/Processor to Processor SCCs.pdf](https://d1.awsstatic.com/Processor_to_Processor_SCCs.pdf).

“Region” has the meaning given to it in Section 12.1 of this Appendix.

“DPA Security Incident” means a breach of AWS’s security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Customer Personal Data.

“Security Standards” means the security standards attached to this Appendix as Annex 1.

“Service Controls” means the controls, including security features and functionalities, that the Services provide, as described in the Documentation.

“Standard Contractual Clauses” means (i) the Controller-to-Processor Clauses, or (ii) the Processor-to-Processor Clauses, as applicable in accordance with Sections 12.2.1 and 12.2.2.

“Third Country” means a country outside the EEA not recognized by the European Commission as providing an adequate level of protection for personal data (as described in the GDPR).

Annex 1

Security Standards

Capitalized terms not otherwise defined in this document have the meanings assigned to them in the Agreement.

1. Information Security Program. AWS will maintain an information security program designed to (a) enable Customer to secure Customer Personal Data against accidental or unlawful loss, access, or disclosure, (b) identify reasonably foreseeable risks to the security and availability of the AWS Network, and (c) minimize physical and logical security risks to the AWS Network, including through regular risk assessment and testing. AWS will designate one or more employees to coordinate and be accountable for the information security program. AWS's information security program will include the following measures:

1.1 Logical Security.

1.1.1 Access Controls. AWS will make the AWS Network accessible only to authorized personnel, and only as necessary to maintain and provide the Services. AWS will maintain access controls and policies to manage authorizations for access to the AWS Network from each network connection and user, including through the use of firewalls or functionally equivalent technology and authentication controls. AWS will maintain access controls designed to (i) restrict unauthorized access to data, and (ii) segregate each customer's data from other customers' data.

1.1.2 Restricted User Access. AWS will (i) provision and restrict user access to the AWS Network in accordance with least privilege principles based on personnel job functions, (ii) require review and approval prior to provisioning access to the AWS Network above least privileged principles, including administrator accounts, (iii) require at least quarterly review of AWS Network access privileges and, where necessary, revoke AWS Network access privileges in a timely manner, and (iv) require two-factor authentication for access to the AWS Network from remote locations.

1.1.3 Vulnerability Assessments. AWS will perform regular external vulnerability assessments and penetration testing of the AWS Network, and will investigate identified issues and track them to resolution in a timely manner.

1.1.4 Application Security. Before publicly launching new Services or significant new features of Services, AWS will perform application security reviews designed to identify, mitigate, and remediate security risks.

1.1.5 Change Management. AWS will maintain controls designed to log, authorize, test, approve, and document changes to existing AWS Network resources, and will document change details within its change management or deployment tools. AWS will test changes according to its change management standards prior to migration to production. AWS will maintain processes designed to detect unauthorized changes to the AWS Network and track identified issues to a resolution.

1.1.6 Data Integrity. AWS will maintain controls designed to provide data integrity during transmission, storage, and processing within the AWS Network. AWS will provide Customer the ability to delete Customer Personal Data from the AWS Network.

1.1.7 Business Continuity and Disaster Recovery. AWS will maintain a formal risk management program designed to support the continuity of its critical business functions ("**Business Continuity Program**"). The Business Continuity Program includes processes and procedures for identification of, response to, and recovery from, events that could prevent or materially impair AWS's provision of the Services (a "**BCP Event**"). The Business Continuity Program includes a three-phased approach that AWS will follow to manage BCP Events:

(i) Activation and Notification Phase. As AWS identifies issues likely to result in a BCP Event, AWS will escalate, validate and investigate those issues. During this phase, AWS will analyze the root cause of the BCP Event.

(ii) **Recovery Phase.** AWS assigns responsibility to the appropriate teams to take steps to restore normal system functionality or stabilize the affected Services.

(iii) **Reconstitution Phase.** AWS leadership reviews actions taken and confirms that the recovery effort is complete and the affected portions of the Services and AWS Network have been restored. Following such confirmation, AWS conducts a post-mortem analysis of the BCP Event.

1.1.8 Incident Management. AWS will maintain corrective action plans and incident response plans to respond to potential security threats to the AWS Network. AWS incident response plans will have defined processes to detect, mitigate, investigate, and report security incidents. The AWS incident response plans include incident verification, attack analysis, containment, data collection, and problem remediation. AWS will maintain an AWS Security Bulletin (as of the Effective Date, <http://aws.amazon.com/security/security-bulletins/>) which publishes and communicates security related information that may affect the Services and provides guidance to mitigate the risks identified.

1.1.9 Storage Media Decommissioning. AWS will maintain a media decommissioning process that is conducted prior to final disposal of storage media used to store Customer Personal Data. Prior to final disposal, storage media that was used to store Customer Personal Data will be degaussed, erased, purged, physically destroyed, or otherwise sanitized in accordance with industry standard practices designed to ensure that the Customer Personal Data cannot be retrieved from the applicable type of storage media.

1.2 Physical Security.

1.2.1 Access Controls. AWS will (i) implement and maintain physical safeguards designed to prevent unauthorized physical access, damage, or interference to the AWS Network, (ii) use appropriate control devices to restrict physical access to the AWS Network to only authorized personnel who have a legitimate business need for such access, (iii) monitor physical access to the AWS Network using intrusion detection systems designed to monitor, detect, and alert appropriate personnel of security incidents, (iv) log and regularly audit physical access to the AWS Network, and (v) perform periodic reviews to validate adherence with these standards.

1.2.2 Availability. AWS will (i) implement redundant systems for the AWS Network designed to minimize the effect of a malfunction on the AWS Network, (ii) design the AWS Network to anticipate and tolerate hardware failures, and (iii) implement automated processes designed to move customer data traffic away from the affected area in the case of hardware failure.

1.3 AWS Employees.

1.3.1 Employee Security Training. AWS will implement and maintain employee security training programs regarding AWS information security requirements. The security awareness training programs will be reviewed and updated at least annually.

1.3.2 Background Checks. Where permitted by law, and to the extent available from applicable governmental authorities, AWS will require that each employee undergo a background investigation that is reasonable and appropriate for that employee's position and level of access to the AWS Network.

2. Continued Evaluation. AWS will conduct periodic reviews of the information security program for the AWS Network. AWS will update or alter its information security program as necessary to respond to new security risks and to take advantage of new technologies.

**Attachment E-1 to
STATE OF OKLAHOMA CONTRACT WITH AMAZON WEB SERVICES, INC.
RESULTING FROM SOLICITATION NO. 0900000556**

AWS BUSINESS ASSOCIATE APPENDIX

Held as Confidential

Attachment F to

**STATE OF OKLAHOMA CONTRACT WITH Amazon Web Services, Inc.
 RESULTING FROM SOLICITATION NO. #0900000556
 Negotiated Exceptions to the Solicitation**

The Solicitation is hereby amended as set forth below and supersedes all prior Exceptions submitted by Amazon Web Services, Inc. or discussed by the parties.

ANY REQUESTED EXCEPTIONS NOT APPEARING BELOW HAVE BEEN DECLINED BY THE STATE

Information Technology Terms (Attachment D), Definitions (Section 1.2, pg. 1)	Section 1.2 shall be modified as follows: Customer Data means software (including machine images), data, text, audio, video, or images that Customer or any End User transfers to AWS for processing, storage or hosting by the Services in connection with an AWS Enterprise Account and any computational results that Customer or any End User derive from the foregoing through its use of the Services. Customer Data does not include Account Information.
Information Technology Terms, Definitions (Section 1.3, pg. 1)	Section 1.3 shall be modified as follows: Data Breach means a breach of the security measures described in the AWS Security Standards that resulted in either (a) any unlawful access to any Customer Data stored on AWS's equipment or in AWS facilities, or (b) any unauthorized access to such equipment or facilities, where in each case such access results in the loss, disclosure or alteration of Customer Data
Information Technology Terms, Definitions (Section 1.4, pg. 1)	Section 1.4 shall be modified as follows: Host includes the terms Hosted or Hosting and means the processing or storing of Customer Data.
Information Technology Terms, Definitions (Section 1.7, pg.1)	Section 1.7 is deleted in its entirety.
Information Technology Terms, Definitions (Section 1.8, pg. 2)	Section 1.8 is deleted in its entirety.

Attachment F to

**STATE OF OKLAHOMA CONTRACT WITH Amazon Web Services, Inc.
 RESULTING FROM SOLICITATION NO. #0900000556
 Negotiated Exceptions to the Solicitation**

The Solicitation is hereby amended as set forth below and supersedes all prior Exceptions submitted by Amazon Web Services, Inc. or discussed by the parties.

ANY REQUESTED EXCEPTIONS NOT APPEARING BELOW HAVE BEEN DECLINED BY THE STATE

Information Technology Terms, Definitions (Section 1.9, pg. 2)	<p>Section 1.9 shall be modified as follows:</p> <p>Security Incident means the unauthorized access to Customer Data by a third party caused by a material breach by AWS of its obligations under the AWS Security Standards (Enterprise Agreement, Attachment B), provided that Customer has complied with the Minimum Architecture Requirements of the AWS Enterprise Agreement. For clarity, a Security Incident defined by Section 1.9 is not the same as a Security Incident defined by the Health Insurance Portability and Accountability Act or as used in any Business Associate Addendum.</p>
Information Technology Terms, Termination of Maintenance and Support Services (Section 2, pg. 3)	<p>Section 2 is deleted in its entirety.</p>
Information Technology Terms, Compliance and Electronic and Information Technology Accessibility (Section 3, pg. 3)	<p>Section 3 shall be modified as follows:</p> <p>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/divisions/information-services/about-information-services/policy-and-standards/information-and-communication-technology-accessibility-standards.html . Subject to an executed Non-Disclosure Agreement, Supplier will make available through AWS Artifact or its successor Service, a Voluntary Product Accessibility Template (“VPAT”) describing accessibility compliance.</p> <p>All representations contained in the VPAT provided will be relied upon by the State or a Customer, as applicable, for accessibility compliance purposes.</p>
Information Technology Terms, Media Ownership (Disk drive and/or Memory Chip Ownership) (Section 4, pg. 4)	<p>Section 4 is deleted in its entirety and replaced with the following:</p> <p>Storage Media Decommissioning. Supplier will maintain a media decommissioning process that is conducted prior to final disposal of storage media used to store Customer Data. Prior to final disposal, storage media that was used to store Customer Data will be degaussed, erased, purged, physically destroyed, or otherwise sanitized in accordance with industry standard practices designed to ensure that the Customer Data cannot be retrieved from the applicable type of storage media.</p>

Attachment F to

**STATE OF OKLAHOMA CONTRACT WITH Amazon Web Services, Inc.
 RESULTING FROM SOLICITATION NO. #0900000556
 Negotiated Exceptions to the Solicitation**

The Solicitation is hereby amended as set forth below and supersedes all prior Exceptions submitted by Amazon Web Services, Inc. or discussed by the parties.

ANY REQUESTED EXCEPTIONS NOT APPEARING BELOW HAVE BEEN DECLINED BY THE STATE

Information Technology Terms, Offshore Services (Section 5, pg. 4)	<p>Section 5 is deleted in its entirety and replaced with the following:</p> <p>Customer may specify the AWS regions in which Customer Data will be stored. Customer consents to the storage of Customer Data in, and transfer of Customer Data into, the AWS regions Customer selects. The parties mutually agree that the Customer will intend to store all Customer Data within the continental United States and AWS will comply with Customer's specification.</p>
Information Technology Terms, Compliance with Technology Policies (Section 6, pg. 4)	<p>Section 6 shall be deleted and replaced with the following:</p> <p>To the extent applicable and agreed upon to be the Supplier's responsibility in the terms of this Contract:</p> <p>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</p> <p>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.html.</p> <p>6.2 Supplier may offer Services that will allow Customer to 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. Supplier will offer Services that will allow Customer to protect Customer Data in accordance with these standards as well as other Customer standards. As of the effective date of the Contract, Supplier provides a list of Services in scope by compliance program available on the AWS site at www.aws.amazon.com/compliance/services-in-scope/FedRAMP/.</p>
Information Technology Terms, Emerging Technologies (Section 7, pg. 5)	<p>Section 7 shall be modified as follows:</p> <p>The State of Oklahoma reserves the right to suggest emerging technologies not identified elsewhere in the Contract Documents.</p>

Attachment F to

**STATE OF OKLAHOMA CONTRACT WITH Amazon Web Services, Inc.
 RESULTING FROM SOLICITATION NO. #0900000556
 Negotiated Exceptions to the Solicitation**

The Solicitation is hereby amended as set forth below and supersedes all prior Exceptions submitted by Amazon Web Services, Inc. or discussed by the parties.

ANY REQUESTED EXCEPTIONS NOT APPEARING BELOW HAVE BEEN DECLINED BY THE STATE

Information Technology Terms, Source Code Escrow (Section 9, pg. 5)	<p>Section 9 is deleted in its entirety and replaced with the following:</p> <p>The Contract does not contemplate, authorize, or support acquisition of custom software products or services.</p>
Information Technology Terms, Commercial Off the Shelf Software (Section 10, pg. 6)	<p>Section 10 is deleted in its entirety and replaced with the following:</p> <p>Third Party Content shall be governed by the Contract unless accompanied by a separate electronic license, subscription, maintenance, support or other terms and conditions. Third-Party terms and conditions or clauses in an electronic license, subscription, maintenance, support or other terms and conditions shall be identified (a) on the AWS Marketplace web pages, (b) in the Service Terms, (c) on a software package download page, product detail page, or notice file associated with the software, or (d) on the developer forum pages on the AWS Site; and Customer reserves the right to negotiate Third-Party terms and conditions prior to purchase.</p>
Information Technology Terms, Ownership Rights (Section 11, pg. 6)	<p>Section 11 is deleted in its entirety and replaced with the following:</p> <p>The Contract does not contemplate, authorize, or support the development of software products or services for the sole and exclusive use of the State.</p>
Information Technology Terms, Intellectual Property Ownership (Section 12, pg. 7)	<p>Section 12 is deleted in its entirety and replaced with the following:</p> <p>The Contract does not contemplate, authorize, or support acquisition of custom software products or services.</p>

Attachment F to

STATE OF OKLAHOMA CONTRACT WITH Amazon Web Services, Inc.
RESULTING FROM SOLICITATION NO. #0900000556
Negotiated Exceptions to the Solicitation

The Solicitation is hereby amended as set forth below and supersedes all prior Exceptions submitted by Amazon Web Services, Inc. or discussed by the parties.

ANY REQUESTED EXCEPTIONS NOT APPEARING BELOW HAVE BEEN DECLINED BY THE STATE

Information Technology Terms, Change Management (Section 14, pg. 10)	Section 14 is deleted in its entirety and replaced with the following: Supplier may change or discontinue any of the Service Offerings, as defined by the Enterprise Agreement, from time to time. For any AWS Enterprise Accounts enrolled in AWS Support at the Developer-level tier or above (or any successor service providing such communications alerts), Supplier will provide at least 12 months’ prior Notice to Customer if AWS decides to discontinue a Service that it makes generally available to its customers and that Customer is using. AWS will not be obligated to provide Notice under Enterprise Agreement Section 2.1 if the discontinuation is necessary to address an emergency or threat to the security or integrity of AWS, respond to claims, litigation, or loss of license rights related to third-party intellectual property rights, or comply with the law or requests of a government entity.
Information Technology Terms, Service Level Deficiency (Section 15, pg. 10)	Section 15 shall be modified as follows: 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.



Attachment F to

STATE OF OKLAHOMA CONTRACT WITH Amazon Web Services, Inc.

RESULTING FROM SOLICITATION NO. #0900000556

Negotiated Exceptions to the Solicitation

The Solicitation is hereby amended as set forth below and supersedes all prior Exceptions submitted by Amazon Web Services, Inc. or discussed by the parties.

ANY REQUESTED EXCEPTIONS NOT APPEARING BELOW HAVE BEEN DECLINED BY THE STATE

Information Technology Terms, Notices (Section 16, pg. 10)	<p>Section 16 is deleted and replaced with the following:</p> <p>(a) General. Except as otherwise set forth in Enterprise Agreement Section 12.10(b), to give notice to a party under the Contract, each party must contact that other party as follows: (i) by facsimile transmission; or (ii) by personal delivery, overnight courier or registered or certified mail. Notices must be sent to the fax number of the other party listed on the Cover Page to this Contract or addressed to the address of the other party listed on the Cover Page to this Contract (or in the case of any AWS Contracting Party that is added to the Contract pursuant to Enterprise Agreement Section 12.14, to such fax number or address provided on the AWS Contracting Party Site), or such other fax number or address as a party may subsequently provide in writing to the other party. Notices provided by personal delivery will be effective immediately. Notices provided by facsimile transmission or overnight courier will be effective one business day after they are sent. Notices provided by registered or certified mail will be effective three business days after they are sent.</p> <p>(b) Notice for purposes of this Contract:</p> <p>If sent to the Supplier: 410 Terry Avenue North, Seattle, WA 98109-5210 Attention: AWS General Counsel</p> <p>If sent to the State: State Purchasing Director 2401 North Lincoln Boulevard, Suite 116 Oklahoma City, Oklahoma 73105</p> <p>Chief Information Officer 3115 N. Lincoln Blvd Oklahoma City, OK 73105</p> <p>With a copy, which shall not constitute notice, to: Purchasing Division Deputy General Counsel 2401 North Lincoln Boulevard, Suite 116 Oklahoma City, Oklahoma 73105</p> <p>Information Services Deputy Counsel 3115 North Lincoln Boulevard</p>
--	--



Attachment F to

STATE OF OKLAHOMA CONTRACT WITH Amazon Web Services, Inc.

RESULTING FROM SOLICITATION NO. #0900000556

Negotiated Exceptions to the Solicitation

The Solicitation is hereby amended as set forth below and supersedes all prior Exceptions submitted by Amazon Web Services, Inc. or discussed by the parties.

ANY REQUESTED EXCEPTIONS NOT APPEARING BELOW HAVE BEEN DECLINED BY THE STATE

	<p>Oklahoma City, Oklahoma 73105</p> <p>(c) Electronic Notice. AWS may provide notice to Customer (i) under Enterprise Agreement Sections 2.2 or 5.1 by (A) sending a message to the email address then associated with at least one of Customer’s Enterprise Accounts, or (B) posting a notice on the AWS Site, (ii) under Section 6 or Attachment A of the Enterprise Agreement by sending a message to the email address then associated with Customer’s applicable AWS Enterprise Account, and (iii) under Enterprise Agreement Section 2.1 by sending a message to the email address then associated with at least one of Customer’s AWS Enterprise Accounts (or such other email address as agreed upon by the parties) or via a support case. Any notices provided by posting on the AWS Site will be effective upon posting and notices provided by email will be effective when AWS sends the email.</p>
--	--



Attachment F to

STATE OF OKLAHOMA CONTRACT WITH Amazon Web Services, Inc.

RESULTING FROM SOLICITATION NO. #0900000556

Negotiated Exceptions to the Solicitation

The Solicitation is hereby amended as set forth below and supersedes all prior Exceptions submitted by Amazon Web Services, Inc. or discussed by the parties.

ANY REQUESTED EXCEPTIONS NOT APPEARING BELOW HAVE BEEN DECLINED BY THE STATE

Information Technology Terms, Appendix 1, Customer Data (Section A, pg. 11)	<p>Section A shall be modified as follows:</p> <ol style="list-style-type: none">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. Supplier may temporarily limit (in full or in part, as set forth in Enterprise Agreement Section 6) Customer’s or any End User’s right to access or use the Service Offerings upon Notice to Customer (which will be reasonable prior notice unless Supplier reasonably believes immediate limitation is necessary) if Supplier reasonably determines that Customer’s or an End User’s use of the Service Offerings poses a security risk or threat to the function of the Service Offerings, or poses a security or liability risk or threat of harm to Supplier, its Affiliates or any third party. Supplier will only limit Customer’s right to access or use the instances, data or portions of the Service Offerings that caused the security or liability risk or threat. Supplier will restore Customer’s access and use rights promptly after Customer has resolved the issue giving rise to the limitation. Customer remains responsible for all fees and charges for the Service Offerings during the period of limitation. The parties agree and understand that this section only speaks to limitation of Customer’s access and use due to a security risk or threat but does not mean that the services are still not being used by Customer.Supplier will not (a) disclose Customer Data to any government or third party, or (b) subject to Section 3.3 of the Enterprise Agreement, move Customer Data from the AWS regions selected by Customer; except in each case as necessary to comply with the law or a binding order of a governmental body (such as a subpoena or court order). Unless it would be in violation of a court order or other legal requirement, Supplier will give Customer reasonable Notice of any legal requirement or order referred to in this subsection, to enable Customer to seek a protective order or other appropriate remedy.
---	--



Attachment F to

STATE OF OKLAHOMA CONTRACT WITH Amazon Web Services, Inc.

RESULTING FROM SOLICITATION NO. #0900000556

Negotiated Exceptions to the Solicitation

The Solicitation is hereby amended as set forth below and supersedes all prior Exceptions submitted by Amazon Web Services, Inc. or discussed by the parties.

ANY REQUESTED EXCEPTIONS NOT APPEARING BELOW HAVE BEEN DECLINED BY THE STATE

Information Technology Terms, Appendix 1 (Data Security, Section B, pg. 11)	<p>Section B shall be deleted in its entirety and replaced as follows:</p> <ol style="list-style-type: none">Supplier will use commercially reasonable efforts, consistent with industry standards, to provide security for the AWS Network and to protect against unauthorized access to the AWS Network. Supplier shall implement and maintain appropriate administrative, technical and organizational security measures to safeguard against unauthorized access, to the AWS Network.Supplier shall enable Customer to encrypt Customer Data.Supplier represents and warrants to Customer that Supplier will use commercially reasonable efforts to prevent the introduction and proliferation of any viruses or other malicious code into the Services.Customer may specify the AWS regions in which Customer Data will be stored. Customer consents to the storage of Customer Data in, and transfer of Customer Data into, the AWS regions Customer selects.Upon Customer’s request, and provided that the parties have an applicable NDA in place, AWS will provide to Customer a copy of the AWS System and Organization Controls 1, Type 2 report or such alternative industry standard reports or certifications that are substantially equivalent as reasonably determined by AWS. AWS will make this documentation available to Customer via AWS Artifact (or an alternative means accessible via the AWS Site) and this documentation will be treated as Confidential Information of AWS under the NDA.
Information Technology Terms, Appendix 1, Security Assessment (Section C, pg. 12)	<p>Section C is deleted in its entirety and replaced with the following:</p> <p>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.</p>



Attachment F to

STATE OF OKLAHOMA CONTRACT WITH Amazon Web Services, Inc.

RESULTING FROM SOLICITATION NO. #0900000556

Negotiated Exceptions to the Solicitation

The Solicitation is hereby amended as set forth below and supersedes all prior Exceptions submitted by Amazon Web Services, Inc. or discussed by the parties.

ANY REQUESTED EXCEPTIONS NOT APPEARING BELOW HAVE BEEN DECLINED BY THE STATE

Information Technology Terms, Appendix 1, Security Incident or Data Breach Notification (Section D, pg. 13)	<p>Section D shall be modified as follows:</p> <p>Data Breach Notification: Supplier shall inform Customer of any SecurityIncident or Data Breach.</p> <ol style="list-style-type: none">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.Supplier shall notify Customer of the Data Breach using the email address listed in the Customer’s AWS account within 72 hours after AWS confirms the Data Breach (provided Customer’s AWS account is enrolled in an Enterprise-level AWS Support plan and AWS is not prohibited from providing the notification by a court order or other legal requirement).Supplier shall:<ol style="list-style-type: none">Maintain processes and procedures to identify, respond to and analyze a Data Breach;Make reasonable and appropriate information regarding the cause, nature and Customer impact of the Data Breach available to Customer at Customer’s request, provided that Supplier will not be required to provide information if Customer is not enrolled in AWS Support at an Enterprise level;Mitigate, to the extent reasonable, the harmful effects of the Data Breach that are known to Supplier; andDocument all Data Beaches and their outcomes.
Information Technology Terms, Appendix 1, Breach Responsibilities (Section E, pg. 14)	<p>Section E is deleted in its entirety.</p>



Attachment F to

STATE OF OKLAHOMA CONTRACT WITH Amazon Web Services, Inc.

RESULTING FROM SOLICITATION NO. #0900000556

Negotiated Exceptions to the Solicitation

The Solicitation is hereby amended as set forth below and supersedes all prior Exceptions submitted by Amazon Web Services, Inc. or discussed by the parties.

ANY REQUESTED EXCEPTIONS NOT APPEARING BELOW HAVE BEEN DECLINED BY THE STATE

Information Technology Terms, Appendix 1, Notices (Section F, pg. 14)	<p>Section F is deleted in its entirety and replaced with the following:</p> <p>(a) General. Except as otherwise set forth in Enterprise Agreement Section 12.10(b), to give notice to a party under the Contract, each party must contact that other party as follows: (i) by facsimile transmission; or (ii) by personal delivery, overnight courier or registered or certified mail. Notices must be sent to the fax number of the other party listed on the Cover Page to this Contract or addressed to the address of the other party listed on the Cover Page to this Contract (or in the case of any AWS Contracting Party that is added to the Contract pursuant to Enterprise Agreement Section 12.14, to such fax number or address provided on the AWS Contracting Party Site), or such other fax number or address as a party may subsequently provide in writing to the other party. Notices provided by personal delivery will be effective immediately. Notices provided by facsimile transmission or overnight courier will be effective one business day after they are sent. Notices provided by registered or certified mail will be effective three business days after they are sent.</p> <p>(b) Notice to Supplier for purposes of this Contract:</p> <p>If sent to the Supplier: 410 Terry Avenue North, Seattle, WA 98109-5210 Attention: AWS General Counsel</p> <p>If sent to the State: State Purchasing Director 2401 North Lincoln Boulevard, Suite 116 Oklahoma City, Oklahoma 73105</p> <p>Chief Information Officer 3115 N. Lincoln Blvd Oklahoma City, OK 73105</p> <p>With a copy, which shall not constitute notice, to: Purchasing Division Deputy General Counsel 2401 North Lincoln Boulevard, Suite 116 Oklahoma City, Oklahoma 73105</p> <p>Information Services Deputy Counsel 3115 North Lincoln Boulevard</p>
---	---



Attachment F to

STATE OF OKLAHOMA CONTRACT WITH Amazon Web Services, Inc.

RESULTING FROM SOLICITATION NO. #0900000556

Negotiated Exceptions to the Solicitation

The Solicitation is hereby amended as set forth below and supersedes all prior Exceptions submitted by Amazon Web Services, Inc. or discussed by the parties.

ANY REQUESTED EXCEPTIONS NOT APPEARING BELOW HAVE BEEN DECLINED BY THE STATE

	<p>Oklahoma City, Oklahoma 73105</p> <p>(c) Electronic Notice. AWS may provide notice to Customer (i) under Enterprise Agreement Sections 2.2 or 5.1 by (A) sending a message to the email address then associated with at least one of Customer’s AS Enterprise Accounts, or (B) posting a notice on the AWS Site, (ii) under Section 6 or Attachment A by sending a message to the email address then associated with Customer’s applicable AWS Enterprise Account, and (iii) under Enterprise Agreement Section 2.1 by sending a message to the email address then associated with at least one of Customer’s AWS Enterprise Accounts (or such other email address as agreed upon by the parties) or via a support case. Any notices provided by posting on the AWS Site will be effective upon posting and notices provided by email will be effective when AWS sends the email.</p>
<p>Information Technology Terms, Appendix 1, Supplier Representations and Warranties (Section G, pg. 15)</p>	<p>Section G is deleted in its entirety and replaced with the following:</p> <p>Supplier represents and warrants to Customer that (a) the Services will perform substantially in accordance with the Documentation, as defined by the Enterprise Agreement, and (b) Supplier will use commercially reasonable efforts to prevent the introduction or proliferation of any viruses and other malicious code into the Services.</p>



Attachment F to

STATE OF OKLAHOMA CONTRACT WITH Amazon Web Services, Inc.

RESULTING FROM SOLICITATION NO. #0900000556

Negotiated Exceptions to the Solicitation

The Solicitation is hereby amended as set forth below and supersedes all prior Exceptions submitted by Amazon Web Services, Inc. or discussed by the parties.

ANY REQUESTED EXCEPTIONS NOT APPEARING BELOW HAVE BEEN DECLINED BY THE STATE

Information Technology Terms, Appendix 1, Indemnity (Section H, pg. 15)	<p>Section H shall be modified as follows:</p> <p>(1) Subject to the Limitation of Liability (Attachment B, General Terms, Section 16.5), if a third party claims that any portion of the Services infringes that third-party’s intellectual property rights, Supplier shall defend, indemnify and hold harmless the Customer, its officers, directors and employees, from all liabilities, claims, damages, losses, costs, expenses, demands, suit and action (including reasonable attorneys’ fees and costs required for reasonable attempts to establish the right to indemnification) and, at Supplier’s expense, pay all related costs, damages, and reasonable attorney’s fees incurred by or assessed to Customer. AWS shall not have any obligations or liability under this section arising from infringement by any combination of the Services or Customer Data, as applicable, with any other product, service, software, data, content, or method. AWS will not have obligations or liability arising from Customer’s use of the Services after Supplier has notified Customer to discontinue such use. For any claim covered by this Section H)(1), AWS will, at its election, either: (i) procure the rights to use that portion of the Services alleged to be infringing; (ii) replace the alleged infringing portion of the Services with a non-infringing alternative; (iii) modify the alleged infringing portion of the Services to make it non-infringing; or (iv) terminate the allegedly infringing portion of the Services or the Contract. The remedies provided in this Section (H)(1) are the sole and exclusive remedies for any third-party claims of infringement or misappropriation of intellectual property rights by the Services.</p> <p>(2) Subject to the Limitation of Liability and provided that the Customer has complied with the Minimum Architecture Requirements, Supplier will defend, indemnify, and hold harmless Customer, its employees, officers and directors from any third-party claim demands, suits and actions arising from a Security Incident and a Data Breach, and pay all costs, damages and attorneys’ fees.</p> <p>(3) The obligations under this Section H shall only apply if the Customer promptly notifies Supplier of any third-party claims, the Attorney General of the State of Oklahoma permits Supplier to control the defense and settlement of the claim and reasonably cooperates with Supplier in the defense and settlement of the claim. Supplier will not agree to any settlement of any such claim that involves any commitment, other than the payment of money, without the written consent of the Customer. 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 participate in any proceeding related to this section.</p>
---	--



Attachment F to

**STATE OF OKLAHOMA CONTRACT WITH Amazon Web Services, Inc.
 RESULTING FROM SOLICITATION NO. #0900000556
 Negotiated Exceptions to the Solicitation**

The Solicitation is hereby amended as set forth below and supersedes all prior Exceptions submitted by Amazon Web Services, Inc. or discussed by the parties.

ANY REQUESTED EXCEPTIONS NOT APPEARING BELOW HAVE BEEN DECLINED BY THE STATE

Information Technology Terms, Appendix 1, Termination, Expiration and Suspension of Service (Section I, pg. 16)	<p>Section I is deleted in its entirety and replaced with the following:</p> <ol style="list-style-type: none"> 1. If requested by Customer, Customer will be permitted to retrieve Customer Data from the Services that are subject to limitation under Section 6 of the Enterprise Agreement, but only to the extent that such retrieval is commercially reasonable and technically feasible and would not result in or exacerbate any of the conditions giving rise to Supplier's right to limit access and use identified in Section 6 of the Enterprise Agreement. 2. During the 180 days following the Termination Date, Supplier will not take action to remove any Customer Data as a result of the termination from any open AWS Enterprise Account. In addition, during such period, Customer may retrieve any remaining Customer Data from the Services, unless (i) prohibited by law or the order of a governmental or regulatory body or it could subject Supplier or its Affiliates to liability, or (ii) Customer has not paid all amounts due under this Agreement, other than Disputed Amounts. For any use of the Services during such period, all terms of this Agreement will continue to apply, and Customer will pay the applicable fees at the rates under Enterprise Agreement Section 5. No later than the end of this 180-day period, Customer will close all AWS Enterprise Accounts and return or, if instructed by AWS, destroy all AWS Content in Customer's possession (except for AWS Content that is publicly available on the AWS Site). 3. AWS will maintain a media decommissioning process that is conducted prior to final disposal of storage media used to store Customer Data. Prior to final disposal, storage media that was used to store Customer Data will be degaussed, erased, purged, physically destroyed, or otherwise sanitized in accordance with industry standard practices designed to ensure that the Customer Data cannot be retrieved from the applicable type of storage media.
Information Technology Terms (Appendix 2, pg. 17)	Appendix 2 is deleted in its entirety.
Bidder Instructions, Submission of Bid (Section 9.6, pg. 12)	<p>Section 9.6 shall be modified as follows:</p> <p>The Bidder guarantees unit prices to be correct.</p>

Attachment F to

STATE OF OKLAHOMA CONTRACT WITH Amazon Web Services, Inc.

RESULTING FROM SOLICITATION NO. #0900000556

Negotiated Exceptions to the Solicitation

The Solicitation is hereby amended as set forth below and supersedes all prior Exceptions submitted by Amazon Web Services, Inc. or discussed by the parties.

ANY REQUESTED EXCEPTIONS NOT APPEARING BELOW HAVE BEEN DECLINED BY THE STATE

General Terms (Attachment B), Scope and Contract Renewal (Section 1.1, pg. 1)	Section 1.1 is amended as follows: Supplier may not add products or services to its offerings under the Contract outside the scope of the contract and Customer will not use products and services outside the scope under this Contract.
General Terms, Scope and Contract Renewal (Section 1.2, pg. 1)	Section 1.2 is deleted in its entirety.
General Terms, Scope and Contract Renewal (Section 1.3, pg. 1)	Section 1.3 shall be modified as follows: 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 negotiate such requested changes in a mutually acceptable Addendum.



Attachment F to

**STATE OF OKLAHOMA CONTRACT WITH Amazon Web Services, Inc.
 RESULTING FROM SOLICITATION NO. #0900000556
 Negotiated Exceptions to the Solicitation**

The Solicitation is hereby amended as set forth below and supersedes all prior Exceptions submitted by Amazon Web Services, Inc. or discussed by the parties.

ANY REQUESTED EXCEPTIONS NOT APPEARING BELOW HAVE BEEN DECLINED BY THE STATE

General Terms, Contract Effectiveness and Order of Priority (Section 2.2, pg. 2)	<p>Section 2.2 shall be modified as follows:</p> <p>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:</p> <ul style="list-style-type: none"> A. Any future Addendum or Amendment; B. Terms 1-4 of the Cover Page; C. AWS Enterprise Agreement, Attachment E-1 of this Contract; D. Attachment F, Negotiated Exceptions; E. any terms contained in Attachments B, C, and D, including, without limitation, information technology terms; F. any applicable Solicitation, Attachment A of the Contract; G. 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; H. any purchase order (or other similar ordering document) as applicable; and I. other mutually agreed Contract Documents.
General Terms, Contract Effectiveness and Order of Priority (Section 2.3, pg. 2)	Section 2.3 is deleted in its entirety.
General Terms, Modification of Contract Terms and Contract Documents (Section 3.1, pg. 3)	<p>Section 3.1 shall be modified as follows:</p> <p>The Contract may only be modified, amended, or expanded by an Addendum, agreed to in writing by both parties. No oral statement of any person shall modify or otherwise affect the terms, conditions, or specifications stated in the Contract.</p>

Attachment F to

**STATE OF OKLAHOMA CONTRACT WITH Amazon Web Services, Inc.
 RESULTING FROM SOLICITATION NO. #0900000556
 Negotiated Exceptions to the Solicitation**

The Solicitation is hereby amended as set forth below and supersedes all prior Exceptions submitted by Amazon Web Services, Inc. or discussed by the parties.

ANY REQUESTED EXCEPTIONS NOT APPEARING BELOW HAVE BEEN DECLINED BY THE STATE

General Terms, Definitions, "Customer" (Section 4.8, p. 4)	<p>Section 4.8 shall be modified as follows:</p> <p>Customer means an entity receiving goods or services contemplated by the Contract.</p>
General Terms, Definitions, "Moral Rights" (Section 4.13, pp. 4-5)	Section 4.13 is deleted in its entirety.
General Terms, Pricing (Section 5, pg. 6)	<p>Section 5 shall be deleted and replaced with:</p> <p>a. 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. Supplier will provide and Customer shall complete such tax forms as are reasonably requested in order to reduce or eliminate the amount of any withholding or deduction for taxes in respect of payments made under this Contract. Any taxes of any nature whatsoever payable by the Supplier shall not be reimbursed.</p> <p>b. Pursuant 74 O.S. § 85.40, all travel expenses of Supplier must be included in the total Acquisition price.</p>
General Terms, Ordering, Inspection, and Acceptance (Section 6.1, pg. 6)	<p>Section 6.1 shall be modified as follows:</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 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.</p>
General Terms, Ordering, Inspection, and Acceptance (Section 6.2, pg. 6)	Section 6.2 shall be modified as follows: Services are deemed as accepted upon provision of a Service or Third Party Content. Payment for professional services are due in accordance with the terms of the Contract only after the work has been performed pursuant to the agreed upon statement of work.

Attachment F to

STATE OF OKLAHOMA CONTRACT WITH Amazon Web Services, Inc.
RESULTING FROM SOLICITATION NO. #0900000556
Negotiated Exceptions to the Solicitation

The Solicitation is hereby amended as set forth below and supersedes all prior Exceptions submitted by Amazon Web Services, Inc. or discussed by the parties.

ANY REQUESTED EXCEPTIONS NOT APPEARING BELOW HAVE BEEN DECLINED BY THE STATE

General Terms, Ordering, Inspection, and Acceptance (Section 6.3, pg. 7)	Section 6.3 is deleted in its entirety.
General Terms, Ordering, Inspection, and Acceptance (Section 6.4, pg. 7)	Section 6.4 is deleted in its entirety.



Attachment F to

STATE OF OKLAHOMA CONTRACT WITH Amazon Web Services, Inc.
RESULTING FROM SOLICITATION NO. #0900000556
Negotiated Exceptions to the Solicitation

The Solicitation is hereby amended as set forth below and supersedes all prior Exceptions submitted by Amazon Web Services, Inc. or discussed by the parties.

ANY REQUESTED EXCEPTIONS NOT APPEARING BELOW HAVE BEEN DECLINED BY THE STATE

General Terms, Invoices and Payment (Section 7.1, pg. 8)	<p>Section 7.1 shall be modified as follows:</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.</p> <p>The following terms additionally apply where applicable:</p> <div><div>A.</div><div>An invoice shall contain the purchase order number (upon receipt and acceptance of a valid purchase order from an eligible entity), description of products or services provided and the dates of such provision.</div></div> <div><div>B.</div><div>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.</div></div> <div><div>C.</div><div>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.</div></div> <div><div>D.</div><div>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 or provide an early payment discount.</div></div> <div><div>E.</div><div>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.</div></div> <div><div>F.</div><div>The Supplier shall accept payment by Purchase Card as allowed by Oklahoma law. If an eligible entity utilizes a Purchase Card, then the eligible entity must notify Supplier in writing via email within 2 business days.</div></div>
--	---



Attachment F to

STATE OF OKLAHOMA CONTRACT WITH Amazon Web Services, Inc.
RESULTING FROM SOLICITATION NO. #0900000556
Negotiated Exceptions to the Solicitation

The Solicitation is hereby amended as set forth below and supersedes all prior Exceptions submitted by Amazon Web Services, Inc. or discussed by the parties.

ANY REQUESTED EXCEPTIONS NOT APPEARING BELOW HAVE BEEN DECLINED BY THE STATE

General Terms, Maintenance of Insurance, Payment of Taxes, and Workers' Compensation (Section 8.1, pg.8)	<p>Section 8.1 shall be modified as follows:</p> <p>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. AWS can satisfy the below minimum limits by any combination of primary liability, umbrella excess liability and self-insurance coverage that results in the same protection.</p> <p>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. 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:</p> <p>A. Workers' Compensation and Employer's Liability Insurance in accordance with and to the extent required by applicable law;</p> <p>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 \$1,000,000 per occurrence;</p> <p>C. Automobile Liability Insurance with limits of liability of not less than \$1,000,000 combined single limit each accident;</p> <p>D. Cyber Liability and Technology Errors & Omissions 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</p> <p>E. Additional coverage required in writing in connection with a particular Acquisition after review and acceptance by Supplier.</p>
--	--



Attachment F to

STATE OF OKLAHOMA CONTRACT WITH Amazon Web Services, Inc.

RESULTING FROM SOLICITATION NO. #0900000556

Negotiated Exceptions to the Solicitation

The Solicitation is hereby amended as set forth below and supersedes all prior Exceptions submitted by Amazon Web Services, Inc. or discussed by the parties.

ANY REQUESTED EXCEPTIONS NOT APPEARING BELOW HAVE BEEN DECLINED BY THE STATE

General Terms, Compliance with Applicable Laws (Section 9.1, pg. 10)	<p>Section 9.1 shall be modified as follows:</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 its present compliance, and shall have an ongoing obligation to comply, with all applicable federal, State, and local laws, rules, regulations, ordinances, including but 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, 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;</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. 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;</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 Verification Program (E-Verify) through the Department of Homeland Security, and is available at www.dhs.gov/E-Verify; and</p> <p>H. 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>
--	---



Attachment F to

**STATE OF OKLAHOMA CONTRACT WITH Amazon Web Services, Inc.
 RESULTING FROM SOLICITATION NO. #0900000556
 Negotiated Exceptions to the Solicitation**

The Solicitation is hereby amended as set forth below and supersedes all prior Exceptions submitted by Amazon Web Services, Inc. or discussed by the parties.

ANY REQUESTED EXCEPTIONS NOT APPEARING BELOW HAVE BEEN DECLINED BY THE STATE

General Terms, Compliance with Applicable Laws (Section 9.2, pg. 11)	<p>Section 9.2 is deleted in its entirety and replaced with the following:</p> <p>To the extent applicable and agreed upon to be the Supplier's responsibility in the terms of this Contract: (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; and</p> <p>(2) 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.html</p>
General Terms, Compliance with Applicable Laws (Section 9.4, pg. 11)	<p>Section 9.4 shall be modified as follows:</p> <p>In addition to compliance under subsection 9.1 above, upon presentment to and Supplier's agreement, Supplier shall have an obligation to comply with applicable Customer-specific mandatory contract provisions required in connection with the receipt of federal funds or other funding source.</p>
General Terms, Compliance with Applicable Laws (Section 9.5, pg. 12)	Section 9.5 is deleted in its entirety.
General Terms, Compliance with Applicable Laws (Section 9.7, pg. 12)	Section 9.7 is deleted in its entirety.
General Terms, Compliance with Applicable Laws (Section 9.9, pg. 12)	Section 9.9 is deleted in its entirety.

Attachment F to

**STATE OF OKLAHOMA CONTRACT WITH Amazon Web Services, Inc.
 RESULTING FROM SOLICITATION NO. #0900000556
 Negotiated Exceptions to the Solicitation**

The Solicitation is hereby amended as set forth below and supersedes all prior Exceptions submitted by Amazon Web Services, Inc. or discussed by the parties.

ANY REQUESTED EXCEPTIONS NOT APPEARING BELOW HAVE BEEN DECLINED BY THE STATE

General Terms, Compliance with Applicable Laws (Section 9.10, pg. 12)	<p>Section 9.10 is deleted in its entirety and replaced with the following:</p> <p>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/divisions/information-services/about-information-services/policy-and-standards/information-and-communication-technology-accessibility-standards.html. Subject to an executed Non-Disclosure Agreement, Supplier will make available through AWS Artifact or its successor Service, a Voluntary Product Accessibility Template (“VPAT”) describing accessibility compliance.</p> <p>All representations contained in the VPAT provided will be relied upon by the State or a Customer, as applicable, for accessibility compliance purposes.</p>
General Terms, Audits and Records Clause (Section 10.1, pg. 13)	<p>Section 10.1 shall be modified as follows:</p> <p>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 payment records relevant to the execution and performance of the Contract except, unless otherwise agreed, costs of Supplier that comprise pricing under the Contract. Notwithstanding the forgoing, the Parties agree that “record” does not include Customer Data and the audit rights does not include a right to enter any of the Supplier’s facilities or buildings.</p>
General Terms, Audits and Records Clause (Section 10.3, pg. 13)	<p>Section 10.3 shall be modified as follows:</p> <p>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. All items of the Supplier that relate to the professional services shall mean the scope of work in a statement of work and in no event, shall this provision grant the State agency, State Auditor and Inspector and the State Purchasing Director access to AWS facilities or data centers.</p>

Attachment F to

**STATE OF OKLAHOMA CONTRACT WITH Amazon Web Services, Inc.
 RESULTING FROM SOLICITATION NO. #0900000556
 Negotiated Exceptions to the Solicitation**

The Solicitation is hereby amended as set forth below and supersedes all prior Exceptions submitted by Amazon Web Services, Inc. or discussed by the parties.

ANY REQUESTED EXCEPTIONS NOT APPEARING BELOW HAVE BEEN DECLINED BY THE STATE

General Terms, Confidentiality (Section 11.1, pg. 13)	<p>Section 11.1 shall be modified as follows:</p> <p>(a) Subject to the Limitation of Liability (Attachment B, General Terms, Section 16.5), Supplier will have an ongoing obligation to implement reasonable and appropriate measures for the AWS Network (as determined by Supplier) designed to help Customer secure Customer Data against accidental or unlawful loss, access or disclosure (the “Security Objectives”) in accordance with the AWS Security Standards. Supplier may modify the AWS Security Standards from time to time, but will continue to provide at least the same level of security as is described in the AWS Security Standards on the Effective Date.</p> <p>(b) Customers have a variety of options to choose from when configuring their accounts, and for all sensitive or otherwise valuable content Supplier recommends that Customer uses strong security and redundancy features, such as access controls, encryption, and backup. Customer is responsible for properly configuring and using the Service Offerings in a manner that provides security and redundancy of its AWS Enterprise Accounts and Customer Data, such as, for example, using enhanced access controls to prevent unauthorized access to AWS Enterprise Accounts and Customer Data, using encryption technology to prevent unauthorized access to Customer Data, and ensuring the appropriate level of backup to prevent loss of Customer Data.</p>
General Terms, Confidentiality (Section 11.2, pg. 14)	Section 11.2 is deleted in its entirety.
General Terms, Confidentiality (Section 11.3, pg. 14)	Section 11.3 is deleted in its entirety.
General Terms, Confidentiality (Section 11.4, pg. 14)	Section 11.4 is deleted in its entirety.
General Terms, Confidentiality (Section 11.5, pg. 14)	Section 11.5 is deleted in its entirety.

Attachment F to

**STATE OF OKLAHOMA CONTRACT WITH Amazon Web Services, Inc.
 RESULTING FROM SOLICITATION NO. #0900000556
 Negotiated Exceptions to the Solicitation**

The Solicitation is hereby amended as set forth below and supersedes all prior Exceptions submitted by Amazon Web Services, Inc. or discussed by the parties.

ANY REQUESTED EXCEPTIONS NOT APPEARING BELOW HAVE BEEN DECLINED BY THE STATE

General Terms, Confidentiality (Section 11.6, pg. 15)	Section 11.6 is deleted in its entirety.
General Terms, Confidentiality (Section 11.7, pg. 15)	Section 11.7 is deleted in its entirety.
General Terms, Assignment and Permitted Subcontractors (Section 13.1, pg. 16)	Supplier and State's obligations under the Contract may not be assigned or transferred to any other person or entity without the prior written consent of the other Party which may be withheld at the other Party'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.
General Terms, Assignment and Permitted Subcontractors (Section 13.2, pg. 16)	Section 13.2 shall be modified as follows: Notwithstanding the foregoing, the Contract may be assigned by Supplier to any corporation or other entity in connection with a merger, acquisition, 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; or to any Affiliate or as part of a corporate reorganization. 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.
General Terms, Assignment and Permitted Subcontractors (Section 13.3, pg. 16)	Section 13.3 shall be modified as follows: 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.

Attachment F to

**STATE OF OKLAHOMA CONTRACT WITH Amazon Web Services, Inc.
 RESULTING FROM SOLICITATION NO. #0900000556
 Negotiated Exceptions to the Solicitation**

The Solicitation is hereby amended as set forth below and supersedes all prior Exceptions submitted by Amazon Web Services, Inc. or discussed by the parties.

ANY REQUESTED EXCEPTIONS NOT APPEARING BELOW HAVE BEEN DECLINED BY THE STATE

General Terms, Assignment and Permitted Subcontractors (Section 13.4 pg. 17)	Section 13.4 shall be modified as follows: 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.
General Terms, Assignment and Permitted Subcontractors (Section 13.5, pg. 17)	Section 13.5 shall be modified as follows: 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 with the prior written approval of the Supplier.
General Terms, Background Checks and Criminal History Investigations (Section 14, pg. 17)	Section 14 is deleted in its entirety and replaced with the following: Where permitted by law, and to the extent available from applicable governmental authorities, AWS will require that each employee undergo a background investigation that is reasonable and appropriate for that employee's position and level of access to the AWS Network.
General Terms, Patents and Copyrights (Section 15, pg. 17)	Section 15 is deleted in its entirety.
General Terms, Indemnification, Acts or Omissions (Section 16.1, pg. 18)	Section 16.1 is deleted in its entirety.
General Terms, Indemnification, Infringement (Section 16.2, pg. 18)	Section 16.2 is deleted in its entirety.

Attachment F to

STATE OF OKLAHOMA CONTRACT WITH Amazon Web Services, Inc.

RESULTING FROM SOLICITATION NO. #0900000556

Negotiated Exceptions to the Solicitation

The Solicitation is hereby amended as set forth below and supersedes all prior Exceptions submitted by Amazon Web Services, Inc. or discussed by the parties.

ANY REQUESTED EXCEPTIONS NOT APPEARING BELOW HAVE BEEN DECLINED BY THE STATE

General Terms, Indemnification, Notice and Cooperation (Section 16.3, pg. 19)	Section 16.3 is deleted in its entirety.
General Terms, Indemnification, Coordination of Defense (Section 16.4, pg. 19)	Section 16.4 is deleted in its entirety.



Attachment F to

STATE OF OKLAHOMA CONTRACT WITH Amazon Web Services, Inc.

RESULTING FROM SOLICITATION NO. #0900000556

Negotiated Exceptions to the Solicitation

The Solicitation is hereby amended as set forth below and supersedes all prior Exceptions submitted by Amazon Web Services, Inc. or discussed by the parties.

ANY REQUESTED EXCEPTIONS NOT APPEARING BELOW HAVE BEEN DECLINED BY THE STATE

General Terms, Indemnification, Limitations of Liability (Section 16.5, pg. 20)	<p>Section 16.5 shall be modified as follows:</p> <p>A. EXCEPT FOR OBLIGATIONS ARISING UNDER ENTERPRISE AGREEMENT SECTION 9.1, NEITHER AWS NOR CUSTOMER, NOR ANY OF THEIR AFFILIATES OR LICENSORS, WILL BE LIABLE TO THE OTHER UNDER ANY CAUSE OF ACTION OR THEORY OF LIABILITY, EVEN IF A PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES, FOR (A) INDIRECT, INCIDENTAL, SPECIAL, CONSEQUENTIAL OR EXEMPLARY DAMAGES (B) LOSS OF PROFITS, REVENUES, CUSTOMERS, OPPORTUNITIES, OR GOODWILL, OR (D) UNAVAILABILITY OF THE SERVICE OFFERINGS (THIS DOES NOT LIMIT ANY SERVICE CREDITS THAT MAY BE AVAILABLE UNDER SERVICE LEVEL AGREEMENTS).</p> <p>B. 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; and indemnity, security or confidentiality obligations under the Contract are subject to the Limitation of Liability (Attachment B, General Terms, Section 16.5).</p> <p>C. THE AGGREGATE LIABILITY UNDER THIS CONTRACT OF EITHER SUPPLIER OR CUSTOMER, AND ANY OF THEIR RESPECTIVE AFFILIATES OR LICENSORS, WILL NOT EXCEED \$20,000,000 (USD TWENTY MILLION); SUBJECT TO STATE LAW, EXCEPT THAT NOTHING IN THIS SECTION 16.5 WILL LIMIT A CUSTOMER’S OBLIGATION TO PAY AWS FOR CUSTOMER’S USE OF THE SERVICES, OR ANY OTHER PAYMENT OBLIGATIONS UNDER THIS CONTRACT. For clarification, the twenty million dollar limitation of liability is a cumulative figure for all Customers as a singular unit for purposes of this section. Therefore, Supplier's total liability under this Contract is strictly USD Twenty Million irrespective of the number of Customers.</p> <p>D. 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.</p>
General Terms, Termination for Funding Insufficiency (Section 17.2, pg. 21)	<p>Section 17.2 shall be modified as follows:</p> <p>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 its duties and responsibilities under the Contract. If a purchase order or other payment mechanism has been issued and a product or service has been received then the termination does not relieve an obligation to pay for the product or service.</p>



Attachment F to

**STATE OF OKLAHOMA CONTRACT WITH Amazon Web Services, Inc.
 RESULTING FROM SOLICITATION NO. #0900000556
 Negotiated Exceptions to the Solicitation**

The Solicitation is hereby amended as set forth below and supersedes all prior Exceptions submitted by Amazon Web Services, Inc. or discussed by the parties.

ANY REQUESTED EXCEPTIONS NOT APPEARING BELOW HAVE BEEN DECLINED BY THE STATE

General Terms, Termination for Cause (Section 18.1, pg. 21)	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.
General Terms, Termination for Cause (Section 18.2, pg. 21)	Section 18.2 is deleted in its entirety.
General Terms, Termination for Cause (Section 18.3, pg. 21)	Section 18.3 shall be modified as follows: If a purchase order or other payment mechanism has been issued and the Services have been received, then the termination does not relieve an obligation to pay for the product or service. Such termination is not an exclusive remedy but is in addition to any other rights and remedies provided for by law. Termination of the Contract under this section, in whole, shall not relieve the Supplier or Customer of liability for claims arising under the Contract.
General Terms, Termination for Cause (Section 18.4, pg. 22)	Section 18.4 shall be modified as follows: 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.
General Terms, Termination for Cause (Section 18.5, pg. 22)	Section 18.5 shall be added as follows: AWS may terminate this Contract for cause upon 30 days' Notice to the State in order to comply with applicable law or requirements of governmental entities.
General Terms, Termination for Convenience (Section 19.1, pg. 22)	Section 19.1 shall be modified as follows: The State may terminate the Contract, in whole, 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. Supplier may terminate this Contract for any reason by providing the Customer or the State at least two years Notice.

Attachment F to

**STATE OF OKLAHOMA CONTRACT WITH Amazon Web Services, Inc.
 RESULTING FROM SOLICITATION NO. #0900000556
 Negotiated Exceptions to the Solicitation**

The Solicitation is hereby amended as set forth below and supersedes all prior Exceptions submitted by Amazon Web Services, Inc. or discussed by the parties.

ANY REQUESTED EXCEPTIONS NOT APPEARING BELOW HAVE BEEN DECLINED BY THE STATE

General Terms, Termination for Convenience (Section 19.2, pg. 22)	<p>Section 19.2 shall be modified as follows:</p> <p>If a purchase order or other payment mechanism has been issued and a product or service has been used, then the termination does not relieve an obligation to pay for the product or service. 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 for refundable Services that are unused when the Contract or certain obligations are terminated shall be refunded. To the extent required by law (which includes but not limited to Oklahoma Constitution Article X, Section 15(A) and 74 O.S. 85.44(B)), Supplier shall refund any amount paid to Supplier in the form of prepaid fees for non-refundable Services that are unused when the Contract is terminated. Termination of the Contract under this section, shall not relieve the Supplier of liability for claims arising under the Contract.</p>
General Terms, Suspension of Supplier (Section 20.1, pg. 23)	Section 20.1 is deleted in its entirety.
General Terms, Suspension of Supplier (Section 20.2, pg. 23)	Section 20.2 is deleted in its entirety.
General Terms, Suspension of Supplier (Section 20.3, pg. 23)	Section 20.3 is deleted in its entirety.
General Terms, Certification Regarding Debarment, Suspension, and Other Responsibility Matters (Section 21, pg. 23)	<p>Section 21 shall be modified as follows:</p> <p>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 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.</p>

Attachment F to

**STATE OF OKLAHOMA CONTRACT WITH Amazon Web Services, Inc.
 RESULTING FROM SOLICITATION NO. #0900000556
 Negotiated Exceptions to the Solicitation**

The Solicitation is hereby amended as set forth below and supersedes all prior Exceptions submitted by Amazon Web Services, Inc. or discussed by the parties.

ANY REQUESTED EXCEPTIONS NOT APPEARING BELOW HAVE BEEN DECLINED BY THE STATE

General Terms, Certification Regarding Debarment, Suspension, and Other Responsibility Matters (Section 22, pg. 23)	<p>Section 22 shall be modified as follows:</p> <p>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 directly to the State.</p>
General Terms, Force Majeure (Section 23.1, pg. 24)	<p>Section 23.1 shall be modified as follows:</p> <p>23.1 Except for payment obligations, no party will be liable for any delay or failure to perform to the extent such delay or failure is 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 notify, as reasonably possible, the other party of its best reasonable assessment of the nature and duration of the force majeure event.</p>
General Terms, Force Majeure (Section 23.2, pg. 24)	<p>Section 23.2 shall be modified as follows:</p> <p>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.</p>
General Terms, Force Majeure (Section 23.3, pg. 24)	<p>Section 23.3 is deleted in its entirety.</p>

Attachment F to

STATE OF OKLAHOMA CONTRACT WITH Amazon Web Services, Inc.

RESULTING FROM SOLICITATION NO. #0900000556

Negotiated Exceptions to the Solicitation

The Solicitation is hereby amended as set forth below and supersedes all prior Exceptions submitted by Amazon Web Services, Inc. or discussed by the parties.

ANY REQUESTED EXCEPTIONS NOT APPEARING BELOW HAVE BEEN DECLINED BY THE STATE

General Terms, Notices, Section 25	<p>Section 25 is deleted and replaced with the following:</p> <p>(a) General. Except as otherwise set forth in Enterprise Agreement Section 12.10(b), to give notice to a party under the Contract, each party must contact that other party as follows: (i) by facsimile transmission; or (ii) by personal delivery, overnight courier or registered or certified mail. Notices must be sent to the fax number of the other party listed on the Cover Page to this Contract or addressed to the address of the other party listed on the Cover Page to this Contract (or in the case of any AWS Contracting Party that is added to the Contract pursuant to Enterprise Agreement Section 12.14, to such fax number or address provided on the AWS Contracting Party Site), or such other fax number or address as a party may subsequently provide in writing to the other party. Notices provided by personal delivery will be effective immediately. Notices provided by facsimile transmission or overnight courier will be effective one business day after they are sent. Notices provided by registered or certified mail will be effective three business days after they are sent.</p> <p>(b) Notice for purposes of this Contract:</p> <p>If sent to the Supplier: 410 Terry Avenue North, Seattle, WA 98109-5210 Attention: AWS General Counsel</p> <p>If sent to the State: State Purchasing Director 2401 North Lincoln Boulevard, Suite 116 Oklahoma City, Oklahoma 73105</p> <p>Chief Information Officer 3115 N. Lincoln Blvd Oklahoma City, OK 73105</p> <p>With a copy, which shall not constitute notice, to: Purchasing Division Deputy General Counsel 2401 North Lincoln Boulevard, Suite 116 Oklahoma City, Oklahoma 73105</p> <p>Information Services Deputy Counsel 3115 North Lincoln Boulevard</p>
------------------------------------	--



Attachment F to

**STATE OF OKLAHOMA CONTRACT WITH Amazon Web Services, Inc.
 RESULTING FROM SOLICITATION NO. #0900000556
 Negotiated Exceptions to the Solicitation**

The Solicitation is hereby amended as set forth below and supersedes all prior Exceptions submitted by Amazon Web Services, Inc. or discussed by the parties.

ANY REQUESTED EXCEPTIONS NOT APPEARING BELOW HAVE BEEN DECLINED BY THE STATE

	<p>Oklahoma City, Oklahoma 73105</p> <p>(c) Electronic Notice. AWS may provide notice to Customer (i) under Enterprise Agreement Sections 2.2 or 5.1 by (A) sending a message to the email address then associated with at least one of Customer's AS Enterprise Accounts, or (B) posting a notice on the AWS Site, (ii) under Section 6 or Attachment A of the Enterprise Agreement by sending a message to the email address then associated with Customer's applicable AWS Enterprise Account, and (iii) under Enterprise Agreement Section 2.1 by sending a message to the email address then associated with at least one of Customer's AWS Enterprise Accounts (or such other email address as agreed upon by the parties) or via a support case. Any notices provided by posting on the AWS Site will be effective upon posting and notices provided by email will be effective when AWS sends the email.</p>
General Terms, Miscellaneous, Choice of Law and Venue (Section 26.1, pg. 25)	<p>Section 26.1 shall be modified as follows:</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. 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 state or federal courts in Oklahoma County, Oklahoma.</p>
General Terms, Miscellaneous, Transition Services (Section 26.4, pg. 26)	<p>Section 26.4 is deleted in its entirety.</p>
General Terms, Miscellaneous, Publicity (Section 26.5, pg. 26)	<p>Section 26.5 is deleted in its entirety and replaced with the following:</p> <p>Except to the extent permitted by applicable law, neither Customer nor Supplier will issue any press release or make any other public communication with respect to this Agreement or Customer's use of the Service Offerings. This section does not limit the State's right to communicate or announce the existence of a Contract between the State and AWS.</p>

Attachment F to

STATE OF OKLAHOMA CONTRACT WITH Amazon Web Services, Inc.

RESULTING FROM SOLICITATION NO. #0900000556

Negotiated Exceptions to the Solicitation

The Solicitation is hereby amended as set forth below and supersedes all prior Exceptions submitted by Amazon Web Services, Inc. or discussed by the parties.

ANY REQUESTED EXCEPTIONS NOT APPEARING BELOW HAVE BEEN DECLINED BY THE STATE

Statewide Contract Terms (Attachment C), Statewide Contract Type, Section 1.2	Section 1.2 is deleted in its entirety.
Statewide Contract Terms, Orders and Addendums (Section 2, pg. 1)	Section 2 is deleted in its entirety.
Statewide Contract Terms, Termination for Funding Insufficiency (Section 3, pg. 1)	Section 3 is deleted in its entirety.
Statewide Contract Terms, Termination for Cause (Section 4, pg. 2)	Section 4 is deleted in its entirety.
Statewide Contract Terms, Termination for Convenience (Section 5, pg. 2)	Section 5 is deleted in its entirety.



Attachment F to

**STATE OF OKLAHOMA CONTRACT WITH Amazon Web Services, Inc.
 RESULTING FROM SOLICITATION NO. #0900000556
 Negotiated Exceptions to the Solicitation**

The Solicitation is hereby amended as set forth below and supersedes all prior Exceptions submitted by Amazon Web Services, Inc. or discussed by the parties.

ANY REQUESTED EXCEPTIONS NOT APPEARING BELOW HAVE BEEN DECLINED BY THE STATE

Statewide Contract Terms, Contract Management Fee and Usage Report (Section 6.1, pg. 2)	<p>Section 6.1 shall be modified as follows:</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 transactions for Services (as defined by the AWS Enterprise Agreement) under the Agreement, 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 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 if agreed upon by the Parties.</p>
Statewide Contract Terms, Contract Management Fee and Usage Report (Section 6.3.v, pg. 3)	<p>Section 6.3.v shall be modified as follows:</p> <p>Reports must include the following information:</p> <ul style="list-style-type: none"> a. Procuring entity; b. Order date; c. Purchase Order number as applicable or note that the transaction was paid by Purchase Card; d. Product description; e. Quantity f. Unit list price or MSRP, as applicable; and g. Unit price charged to the purchasing entity.
Solicitation No. 0900000556 (Attachment A), Purpose	<p>The Purpose section shall be modified as follows:</p> <p>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 and services pursuant to the Contract.</p>

**Attachment F-1 to
STATE OF OKLAHOMA CONTRACT WITH AMAZON WEB SERVICES, 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.

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

By: _____

Name: _____

Title:

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: _____



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

Contract title: Software Value Added Reseller

Contract Number: SW1041A

Date of Contract issuance: 12.22.2023

Contract period: 12.22.2023 through 03.13.2024

Agreement period: 12.23.2023 through 03.14.2028

Type of contract: Mandatory ☐ Non-Mandatory ☒

OMES POC Skyler J. Greco

Title: SW Contracting Officer

Phone: (405) - 521 - 2174

Email: skyler.greco@omes.ok.gov

Vendor POC

Vendor POC:
Colette Buxton
972-745-5021
cbuxton@avaya.com

Supplier ID:

Supplier 0000583733
AVAYA HOLDINGS CORP
AVAYA LLC
350 MOUNT KEMBLE AVE
MORRISTOWN NJ 07960-0001
USA

Contract ID: 0000000000000000000007211

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.

Contract Overview: Value-Added Software

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:

Contact POC listed above

Ensure quote references SW1041A

.

Available Brands:

See pricing attachment.

Available Products and Services:

Software, Value-Added

Authorized Dealer/Reseller(s): N/A



Experiences That Matter

Request for Proposal (RFP) Response for:

Software as a Service



OKLAHOMA
Office of Management
& Enterprise Services

RFP No:

0900000556

Due Date:

10/12/2022

Submitted to:

OMESCPeBID@omes.ok.gov
Mark Brown
marc.brown@omes.gov
Phone No. 405-521-6669

Submitted by:

Colette Buxton
SLED Account Manager
Office: 972-745-5021
Mobile: 405-641-6024
Email: cbuxton@avaya.com

Exhibit 1: Price Avaya State of Oklahoma (RFP 0900000556) Avaya Discount Summary		
Material Product Group (MPG)	Group / Description	State of Oklahoma Discount off Avaya Price List
5P	Software Contact Center – Heritage Nortel	20%
7P	OEM	12%
8P	Video	32%
9P	SMEC	20%
1R	Avaya Cloud Office / SIP	0.0%
8S	Contact Center Subscription Services	0.5%
9S	Unified Communications Subscription Services	0.5%
1T	Cloud Offers	0.5%
2R	Alliances	0.0%

Exhibit 2: Value Added Services State of Oklahoma (RFP 0900000556) Avaya Discount Summary		
Material Product Group (MPG)	Group / Description	State of Oklahoma Discount off Avaya Price List
1P	Hardware – Heritage Avaya	28%
2P	Software UC – Heritage Avaya	32%
3P	Peripheral Equipment	32%
4P	HW2 – Heritage Nortel	20%
1Z	Non-Discountable	0.0%
1C	Support Services	0.5%
1N	Support Services	0.5%
1S	Maintenance Services	0.5%
2S	Technical Services	0.5%
3S	Avaya Prof Cloud Services	0.5%
5S	Support Services	0.5%
6S	Maintenance Services	0.5%
7S	Maintenance Services	0.5%

Professional Services (Hourly Not To Exceed Rates) State of Oklahoma (RFP 0900000556) Avaya Discount Summary		
Description	List Rate	Discounted Hourly Rate
Technical Project Manager	\$225	\$ 223.88
Advanced Solutions Architect	\$300	\$ 298.50
Technician	\$205	\$ 203.98
Software Associate	\$175	\$ 174.13
Software Specialist	\$225	\$ 223.88

Pricing Notes:

1. Greater discounts may be available provided one of the following conditions are met:

(i) Multi-year Maintenance Commitment: Avaya's acceptance and fulfillment of any order to which the Discounts apply is contingent upon the purchase by Customer of a minimum of two years Maintenance Service on each of the Products referenced on the order. Such purchase of maintenance shall be made coincident with the purchase of Product.

(ii) Pre-Paid Maintenance Commitment: Avaya's acceptance and fulfillment of any order to which the Discounts apply is contingent upon the Customer's advanced payment, in full, for one year of Maintenance Service on each of the Products referenced on the order

(iii) Multi-Year Subscription Commitment: Avaya's acceptance and fulfillment of any order to which the Discounts apply is contingent upon the purchase by Customer of a minimum of a three year Subscription License Term on each of the Software and Products referenced on the order with early termination penalty fees. Such purchase of Subscription License shall be made coincident with the purchase of Product and any Maintenance for said product.

(iv) Pre-paid Subscription Commitment: Avaya's acceptance and fulfillment of any order to which the Discounts apply is contingent upon the Customer's advanced payment, in full, for the term of the Subscription.

(v) Sole Source Commitment : Avaya's acceptance and fulfillment of any order to which the Discounts apply is contingent upon Customer agreeing to purchase all its requirements for Products and new equipment comparable to the Products providing materially the same features and functionality ("Sole Sourced Equipment") from Avaya for the period of this Agreement.

2. Professional Services rates do not include travel and living expenses

3. Professional Services engagements require a Scope of Work.

Avaya SIP Services Rate Card Summary (US Calling)

Exhibit 2: Value Added Services

State of Oklahoma (RFP 0900000556) Avaya Discount Summary

Service Type	Material Code	USA	
			Rate per Unit (USD)
Phone Numbers			
Local Number / month	407965	\$	1.00
Toll Free Number / month	407966	\$	1.00
Toll Free Number Setup One time	407967	\$	-
DDI Setup Fee One time	407968	\$	-
DDI Porting Out Fee One time	407954	\$	2.75
Emergency Services / month	407970	\$	0.50
Per User Bundle / Per month Pricing (includes 1000 US/Canada minutes, DID, Emergency Services) (Note: User bundle is not applicable for CC user case)	407976	\$	7.00
International Calling Bundle (includes 1000 minutes inbound/outbound) Per month / per user (Note: User bundle not is applicable for CC use case)	407979	\$	21.00
Service Description / Call Type (Usage based pricing)		Usage Based Minutes (and coverage for per user bundle)	
Local Inbound Calling /min	407971	\$	0.0080
Local Outbound calling /min	407972	See Outbound Rate Card	
Toll Free Inbound Calling / min	407974	\$	0.0200
International Outbound Calling	410546	See Outbound Rate Card	

Pricing Notes:

1. See you Avaya Account Manager for most current rate card
2. Services contracted and invoiced by Avaya Cloud Inc.
3. Pricing excludes taxes, fees, and surcharges.



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

Statewide Contract #: SW1041A

PeopleSoft Contract ID: 7211

Contract Title: Software Value Added Reseller

Contract Issuance Date: 12/22/2023

Contract Supplier: Avaya

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 Avaya per the original T&C's.

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

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



**STATE OF OKLAHOMA STATEWIDE CONTRACT WITH
AVAYA, 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 Avaya, 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 D-1;
 - 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. 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.

[Remainder of page intentionally left blank.]

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

AVAYA, INC.

By: 
Joe McIntosh (Dec 22, 2023 10:09 CST)
Name: Joe McIntosh
Title: CIO
Date: Dec 22, 2023

By: 
Jenifer Bond (Dec 21, 2023 17:26 CST)
Name: Jenifer Bond
Title: VP US SLED
Date: Dec 21, 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 [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 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.

Attachment E-1

Additional Terms

State and Supplier further agree that the terms and conditions of Attachment A through D-1 control and therefore take precedence over the embedded hyperlinks, or any terms and conditions contained within this attachment. Any terms and conditions of any embedded hyperlinks or terms or conditions contained within this attachment which expand liabilities or reduce rights and protections for the State are not agreed to by the State.

Customer represents that it is an agency or department of a State, County or Municipal Government, or a public educational institution.

ORDER SPECIFIC TERMS

The terms for the offers listed below ("**Order Specific Terms**") found at <https://support.avaya.com/TermsOfSale> (or a successor site that is properly noticed) apply to the Order with respect to the Products and Services included in the Order:

- **Products and Subscription Licenses**
- **Professional Services**
- **Support & Managed Services**
- **Cloud Services**

1. ORDERS, INVOICING, PAYMENT AND TAXES

1.1 Orders. All Orders accepted by Avaya are subject to the terms of this SLSA, except where the terms conflict with the terms and conditions of the SW1041 contract.

1.2 Invoicing and Payment. Unless otherwise governed by applicable law, or unless specified otherwise in this SLSA or otherwise agreed to in writing,

- Avaya will invoice Customer for Products after deliver and acceptance..
- Avaya will invoice to, and process associated payments from, Customer via Avaya's electronic bill application, unless otherwise requested in writing in advance by Customer.
- Payment is due within 45 days from the date of Avaya's invoice other than with respect solely to those portions that are disputed by Customer and noticed by Customer to Avaya within 15 days from the date of Avaya's invoice.
- If a payment is not timely received from Customer, late payments will be subject to an incremental fee equal to the lesser of 1.5% per month or the maximum rate allowed by applicable law that must be paid in order for overdue amounts to be deemed paid in full.

1.3 Reserved.

1.4 Reserved.

2. LICENSE INFORMATION

except where the terms conflict with the terms and conditions of the Attachment A through D-1 of this Contract.. Any Software licenses (including Subscription Licenses) granted by Avaya to the Customer under this SLSA shall be in accordance with the then-current terms and conditions set forth in the Avaya Global Software License Terms, found at <http://support.avaya.com/LicenseInfo> (or a successor site properly noticed) which may be updated from time to time and will apply prospectively (the "EULA").

3. WARRANTY AND DISCLAIMER OF OTHER WARRANTIES

3.1 Warranties. Warranties for Products and Services provided to Customer shall be set forth in the Order Specific Terms.

3.2 RESERVED.

3.3 Avaya provides Third-Party Products and Third-Party Services on an "**AS IS**" **BASIS WITHOUT WARRANTIES OF ANY KIND**. However, such Third-Party Products or Third-Party Services may carry warranties from their manufacturers or providers, and Avaya will pass through to Customer any such warranties to the extent authorized. Exercise of such warranties will be directly between Customer and the relevant Third Party.

4. CUSTOMER RESPONSIBILITIES

4.1 Cooperation. Customer agrees to:

- Cooperate with Avaya as reasonably necessary for Avaya's delivery of Products and performance of Services in a timely manner.
- Adequately secure its networks and systems against unauthorized intrusion or attack.
- Properly use, safeguard, and return to Avaya any Avaya Tools (items that Avaya lends or makes available to Customer for purposes of the Order (e.g., Secure Access Link, etc.)). It being understood that Avaya Tools are not Products.

4.2 Customer acknowledges that its cooperation hereunder is essential to Avaya's performance of the Services. Avaya is not liable for any delay or deficiency in performing the Services as a result of Customer not meeting their responsibilities.

5. IP OWNERSHIP

5.1 Avaya Intellectual Property. Avaya, its Affiliates, licensors and suppliers own all rights, title and interest in and to any intellectual property in the Products, the Services, any and all Deliverables provided to Customer hereunder as well as any know-how, derivative works, inventions, processes, databases, Documentation, training materials, and any other intellectual property and any tangible embodiments of it (collectively, "Avaya Intellectual Property"), except for software developed under the terms of the contract. Customer shall not copy, modify, rent, lease, sell, loan, distribute, or create derivative works of any Avaya Intellectual Property. Customer shall receive a license to use Deliverables as described in the applicable Order Specific Terms.

5.2 Customer Intellectual Property. Customer reserves all rights, including, but not limited to, ownership, title, intellectual property rights and all other rights and interest in and to any Intellectual Property that Customer owns and makes available to Avaya under this Agreement.

5.3 Marks. Nothing herein grants Customer any right to use any trade names, trademarks, service marks, logos, domain names, trade dress, or other distinctive brand features of Avaya or its subcontractors or suppliers. Customer shall not remove, obscure, or alter any proprietary rights notices, such as copyright or trademark notices, attached to or contained within Avaya Intellectual Property, Services or Software.

6. INDEMNIFICATION

6.1 Defense and Indemnity. Subject to Sections 6.2, 6.3, and 6.4 below, Avaya will defend and indemnify Customer for any judgments, settlements and court awarded attorneys' fees resulting from a Claim, provided Customer:

- (a) Promptly notifies Avaya of the Claim in writing upon becoming aware of a potential Claim

(b) Reserved.

(c) Provides information and assistance reasonably requested by Avaya to defend against or settle the Claim.

6.2 Remedial Measures. If a Product becomes, or its use reasonably may become, the subject of a Claim, Avaya may opt to: (i) procure for Customer the right to continue use of the Product; (ii) replace or modify the Product;

6.3 Reserved.

6.4 Reserved.

6.5 General Indemnification. Avaya shall defend Customer, Customer's agents, servants and employees against all third party actions, suits or proceedings (as used in this Section 6.5, "Claim") for damages to real or tangible personal property or for bodily injury or death to any person arising out of, or in connection with this Agreement, to the extent such damage, injury or death was caused by the negligence of Avaya, any subcontractor of Avaya or their employees, servants or agents while performing under this Agreement, and shall indemnify Customer for any judgments, settlements and reasonable attorney fees resulting from a Claim as provided in this Section; Customer agrees: (i) that Avaya shall be notified in writing promptly of any such Claim, (ii) reserved; and that (iii) Customer provides all information and assistance reasonable requested by Avaya to handle the settlement or defense of the Claim.

7. TERM AND TERMINATION

7.1 Termination for Breach. Either Party may terminate the Order by giving written notice to the other Party if the other Party breaches any material term of this SLSA and fails to cure such breach within 30 days after receipt of such notice.

7.2 Termination for Convenience. Reserved.

8. LIMITATION OF LIABILITY

8.1 Limitation of Liability. reserved.

8.2 Exclusion of Consequential and Related Damages. NEITHER PARTY NOR ITS RESPECTIVE LICENSORS OR SUPPLIERS HAVE ANY LIABILITY ARISING OUT OF OR RELATED TO THIS SLSA FOR ANY INCIDENTAL, SPECIAL, PUNITIVE, INDIRECT OR CONSEQUENTIAL DAMAGES, LOSS OF PROFITS OR REVENUE, LOSS OR CORRUPTION OF DATA, COST OF COVER, COST OF SUBSTITUTE GOODS OR COST OF SUBSTITUTE PERFORMANCE.

8.3 Applicability.

reserved.

9. CONFIDENTIALITY

9.1 Confidential Information. Each party acknowledges that it may receive Confidential Information from the other party in connection with this SLSA, any Order, and during the course of the parties' general business relationship.

9.2 Authorized Disclosure. Subject to applicable all state and federal law, including but not limited to the Oklahoma Open Records Act, the receiving party may disclose Confidential Information only to its employees, contractors, agents, directors, officers, professional legal advisors, Affiliates or subcontractors with a need to know and who are bound by confidentiality obligations at least as protective as the terms stated in this Section 9 (collectively, the "Authorized Parties"). Each party is responsible for any Authorized Party's breach of this Section 9. Notwithstanding the foregoing, the receiving party is authorized to disclose Confidential Information as required by applicable law or in accordance with a valid order issued by a court, government agency or relevant regulatory or listing exchange authority. The confidentiality obligations of each party will survive following the expiration or termination of this SLSA or the Order. Upon such termination or expiration, the receiving party, upon request of the disclosing party, will cease all use of and/or destroy the disclosing party's Confidential Information (including any copies thereof) in the receiving party's possession, custody, or control, provided that the receiving party may keep archival copies due to mandatory retention laws, for regulatory purposes or to enforce its rights, subject to the confidentiality obligations as stated in this Section 9.

10. GOVERNING LAW AND DISPUTE RESOLUTION

10.1 Governing Law. This SLSA, including any Dispute under the Order or this SLSA, will be governed by the laws of Oklahoma excluding both conflict of laws principles and United Nations Convention on Contracts for International Sale of Goods.

10.2 Dispute Resolution. In the event of any Dispute, the disputing party shall give the other party written notice of the Dispute in accordance with the notice provision of this SLSA.

10.3 Choice of Forum. For any Dispute arising or based upon an alleged breach committed, then either party may bring an action or in either the state or federal courts in Oklahoma. Each party consents to the exclusive jurisdiction of those courts, including their appellate courts, for the purpose of all actions and proceedings arising out of or relating to this Agreement.

10.4 Undisputed Invoices. reserved.

10.5 Injunctive Relief. Nothing in this Agreement will be construed to preclude either party from seeking provisional remedies, including temporary restraining orders and preliminary injunctions from any court of competent jurisdiction in order to protect its rights at any time.

10.6 Time Limit. reserved.

11. THIRD PARTY TERMS

Third-Party Terms. Customer may elect to purchase Third-Party Products and Third-Party Services from Avaya and, in that case, Customer agrees to be bound by any additional terms and conditions negotiated for the Third-Party Products and/or Third-Party Services ("Third-Party Terms"). In case of a conflict, the terms of the Statewide 1041 will control.

12. DATA PRIVACY

12.1 DPA. Avaya respects Customer's privacy and will only use information provided to Avaya by Customer or collected by Avaya in the provision of Services in accordance with Avaya's data privacy policies and the DPA. To the extent Avaya processes Personal Data on behalf of Customer, the most current Avaya DPA, published on <http://support.avaya.com/TermsOfSale> at the time of the Order, applies and is incorporated herein by reference. The DPA is considered a Supplemental Term, if applicable.

12.2 Where Avaya has received Customer's electronic contact data (e.g. e-mail address) in connection with a Product or Service Order, Avaya may occasionally send Customer information about similar Products and Services that may be of interest to Customer. If Customer does not wish to receive such information, Customer should contact Avaya Sales or notify Avaya via email at dataprivacy@avaya.com.

13. MISCELLANEOUS

13.1 Compliance. The parties will observe all applicable laws and regulations when using the Products and Services. Avaya Products and Services are subject to applicable import and export control laws and regulations of the United States and other countries. Each party, at its own expense, will comply with applicable export and import laws and regulations, including those of the United States that prohibit or limit export to certain countries, for certain uses, or to certain end users. Each party agrees to provide the other party the information, support documents and assistance as may be reasonably required in connection with securing necessary authorizations or licenses required for the transactions contemplated by this SLA or in connection with associated reporting or recordkeeping obligations.

13.2 Assignment, Independent Contractor, & Subcontractors. Avaya is an independent contractor and no partnership, joint venture, or agency relationship exists between the parties. Each party will be responsible for paying its own employees, including employment related taxes and insurance.

13.3 Force Majeure. Neither party will be liable for any delay or failure in performance to the extent the delay or failure is caused by events beyond the party's reasonable control, including without limitation, fire, flood, Act of God, explosion, terroristic acts, war, strike, embargo, labor dispute,

13.4 Notices. Any required notice will be addressed to the applicable party as set forth below. Notices will be delivered by: (i) personal delivery; (ii) courier or first class mail (with all fees or postage prepaid). Notices will be deemed to have been given, as applicable, on the earlier of: (a) the date of receipt.

For Customer: Address as set forth on the Order form

For Avaya: Avaya Inc. Attn: Law Dept. 350 Mount Kemble Avenue Morristown, NJ 07960 United States, Email: lglnoticescomm@avaya.com

For Customer notification of cancellation or intent not to renew maintenance, managed service and subscription services, send notice to Avaya: Avaya World Services Inc., Customer Care Center - Attn: Services Termination, 14400 Hertz Quail Spring Pkwy, Oklahoma City, OK 73134, Email: mycontract@avaya.com, Facsimile: 800-441-6371. If the order was placed on an Avaya Affiliate, the notice of cancellation must be sent to the e-mail or address stated on the relevant order.

13.5 Reference. Neither Party may use the name, logos and trademark(s) of the other Party or to list it as a provider or recipient of Products or Services for marketing purposes, whether on websites, social media or in public announcements, without the prior consent of the other Party

13.6 Construction. The provisions concerning confidentiality, license grant to Customer, indemnity, and any other terms which, by their nature, are intended to survive termination or expiration of the Order will survive. If any term of this SLA is found to be invalid, the remaining provisions will remain effective. No waiver of any term, condition, or breach shall be construed as a waiver of subsequent terms, conditions, or breaches. Only written and signed modifications shall be enforceable. Paragraph headings are for reference only. The singular includes the plural, and vice versa. Each party represents that the person signing this SLA or an associated Order on its behalf has authority to contractually bind such party to the terms and conditions of this SLA. This SLA or any related documents may be executed by electronic signature in lieu of a handwritten signature. This SLA may be executed in one or more counterparts (including by facsimile), each of which when so executed shall be deemed to be an original and shall have the same force and effect as an original.

13.7 Avaya's Ethics, Compliance and Corporate Responsibility. Avaya is committed to ethical business conduct and corporate responsibility.

13.8 Order of Precedence.

(a) reserved.

(b) reserved.

14. DEFINITIONS

"Avaya" means, as the context requires, either Avaya Inc. or the appropriate Avaya Affiliate or permitted assignee accepting an Order from or entering into a with Customer.

"Claim" means a claim, action, suit or proceeding brought by a third party against a party alleging that a Product, as of its Delivery Date under the Order infringes a patent, copyright or trademark.

Order Specific Terms: Sale of Products and Subscription Licenses

These Order Specific Terms apply to Orders for any Products and/or Subscription Licenses. These terms are incorporated into the SLSA between Avaya and Customer. Capitalized terms not otherwise defined here or in the SLSA have the meaning in Section 5.

1. ORDERS AND CHANGES

1.1 Product Changes. Prior to its delivery, Avaya may make changes to the Product, modify the drawings and specifications relating to the Product, or substitute the Product for a Product of later design; provided that the changes do not have a materially adverse effect on the function of the Product. Notwithstanding the foregoing, the parties may agree to change an Order at any time and such changes may be subject to additional charges.

1.2 Cancellation of Product Orders. Customer may cancel an Order for Product prior to shipping by written notice to Avaya as follows:

1.2.1 within 72 hours of Order placement: subject to a cancellation fee of 5% of the purchase price

1.2.2 more than 72 hours after Order placement: subject to a cancellation fee of 10% of the purchase price

1.2.3 Avaya may invoice for cancellation fees immediately.

1.2.4 Customer may not cancel an Order once the relevant Product(s) has been shipped or made available for download.

1.3 Delays to Product Orders. Customer may request that the Delivery Date for Products be delayed by up to 75 days from the original Delivery Date. Any request for delay by Customer in excess of 75 days from the Delivery Date will entitle Avaya to cancel the Order for Products that have not yet been delivered, subject to a cancellation fee of 10 % of the Product price for such cancelled Products, payable by Customer upon cancellation by Avaya. The remainder of the Order will remain in full force.

1.4 Termination of Subscription Licenses. Subscription Licenses terms, termination and any applicable termination fees are set forth in the applicable Subscription License Supplement.

2. DELIVERY, TITLE, AND RISK OF LOSS

2.1 Delivery and Risk of Loss. Unless otherwise agreed in an order, all deliveries of Products will be made CIP (Destination on Order or Delivery Point). Avaya may charge Customer for shipping and handling charges in relation to the delivery of the Products, which will be reflected as a separate line item in Avaya's invoice. Risk of loss will pass to Customer on the Delivery Date.

2.2 RESERVED.

2.3 Title to Software does not Pass. Software that is a Product is licensed to Customer as specified in Section 3. Title to Software will remain with Avaya and its licensors (provided that Customer will be entitled to retain the copies of the Software supplied for the duration of the license term that applies to the use of the Software concerned).

2.4 RESERVED

3. SUBSCRIPTION LICENSE

Subscription licenses are also subject to then-current Subscription License Supplement.

4. WARRANTIES

4.1 Warranty Scope. Avaya warrants to Customer that during the applicable warranty period that Products will conform to and operate in accordance with the applicable Documentation in all material respects.

4.2 Warranty Period. The warranty periods are as follows: (i) RESERVED (ii) Software and Software media: 90 days, beginning on the In-Service Date for Avaya-installed

Software; on the Delivery Date for all other Software and media; or the Subscription License Term Start Date as set forth in the SLS.

4.3 Remedies. If a Product does not conform to the warranty above and Avaya receives from Customer during the applicable warranty period a written notice describing in reasonable detail how the Product failed to be in conformance, then Customer's sole and exclusive remedy, Avaya will, at its option: (i) repair or replace same to achieve conformance or (ii) refund to Customer the applicable fees paid for the non-conforming hardware or Software, upon return of the non-conforming hardware, Software media to Avaya in accordance with Avaya's instructions. Customer will return Products subject to a warranty claim to Avaya in accordance with Avaya's instructions. Replacement hardware may be new, factory reconditioned, refurbished, re-manufactured or functionally equivalent and will be furnished only on an exchange basis. Returned hardware that has been replaced by Avaya will become Avaya's property. Replacement Products are warranted as above for the remainder of the original applicable Product warranty period. For Software warranty claims, Avaya will provide access to available Software corrective content and Product support knowledge base on a self-service basis.

4.4 Costs. If a Product is returned within the applicable warranty period subject to a valid warranty claim, Avaya will not charge for any repair, replacement, error identification or correction, or return shipment of the non-conforming Product. If Avaya determines that the Product was operating in conformance with its applicable warranty, Avaya may charge Customer for error identification or correction efforts, repair, replacement and shipment costs at Avaya's then current time and materials rates.

4.5 Exclusions and Disclaimers. The warranties do not extend to any damages, malfunctions, or non-conformities caused by: (i) Customer's use of Products in violation of the license granted under this SLSA or in a manner inconsistent with the Documentation; (ii) normal wear due to Product use, including but not limited to Product cosmetics and display scratches; (iii) use of non-Avaya furnished equipment, software, or facilities with Products (except to the extent provided in the Documentation); (iv) Customer's failure to follow Avaya's installation, operation or support instructions; (v) Customer's failure to permit Avaya timely access, remote or otherwise, to Products; or (vi) failure to implement updates provided by Avaya. Warranties do not extend to Products that have been serviced or modified by a party other than Avaya or a third party specifically authorized by Avaya to provide the service or modification.

5. DEFINITIONS

"In-Service Date" means the earlier date of (i) Avaya notifying Customer that the Products are installed and available for production use; or (ii) Customer begins using the Product in a production environment.

"Subscription Licensing Supplement" or "SLS" means the then-current Avaya offer description document for Subscription Licenses found at <http://support.avaya.com/LicenseInfo> or a successor site and incorporated herein by this reference as of the date of Avaya's acceptance of an Order.

"Subscription License(s)" means the software licenses ordered by Customer which are subject to a Subscription.

These Professional Services Terms apply to Orders for Professional Services. Capitalized terms have the meaning given in the Definitions.

1. SCOPE

Avaya will provide Professional Services as specified in an Order, a Service Description Document (SDD) and/or a SOW (the "Order") describing the Professional Services to be performed. Professional Services may include installation and configuration of Products, consulting and other Professional Services where Avaya creates a Deliverable and/or completes other defined objectives or a project phase on a milestone basis, time and material basis, or other basis.

2. ACCEPTANCE

2.1 T&M Services. T&M Services are deemed accepted upon performance.

2.2 Order without Acceptance Procedures. Where the Order does not contain specific acceptance criteria and procedures, Professional Services are deemed accepted upon the earlier of either: (i) Avaya providing notice of completion to Customer; or (ii) Customer signing of an acceptance certificate.

2.3 Order with Acceptance Procedures. The Professional Services are deemed accepted upon the earlier of either: (i) the end of the acceptance period as set out in the Order, unless before the end of the acceptance period Avaya has received from Customer a rejection notice; or (ii) Customer signing of an acceptance certificate. If the Professional Services fail to conform to the agreed acceptance criteria and Avaya has received a rejection notice, then Avaya will re-perform the non-conforming Professional Services and re-submit it for acceptance as described above. If, after resubmission, the Professional Services fail to conform to the agreed acceptance criteria in any material respect, then Customer's sole and exclusive remedies will be for Customer to either: (i) terminate the non-conforming Professional Services and return all non-conforming Deliverables for a refund of fees paid under the SOW for the non-conforming Professional Services; or (i) accept the Professional Services, subject to the warranties and remedies described in Section 6. Customer will be deemed to have accepted the applicable Professional Services, in accordance with subsection 2.2 above if Avaya has not received a written termination notice within 5 days of Avaya's resubmission for acceptance.

2.4 Acceptance certificate. Upon acceptance in accordance with this Section 2, Customer will promptly sign and return an acceptance certificate. Acceptance certificates may be provided by Customer to Avaya by electronic mail, at the email address provided by Avaya to Customer from time to time, or other agreed means of electronic communication.

2.5 Production Use. Notwithstanding any other provisions above, production use by customer will constitute acceptance for all purposes under the SLSA.

3. TRANSFER OF RISK AND LICENSE TO DELIVERABLES

3.1 Transfer of Risk. If the Professional Services include tangible items to be delivered to Customer, risk of loss and title shall pass when carrier receives the Deliverable for shipment to Customer.

3.2 License to Deliverables. Subject to Customer's payment of fees for the Professional Services, Avaya grants Customer a non-exclusive, non-transferable, limited, non-sublicensable license to use Deliverables created by Avaya and delivered to Customer. Software contained in Deliverables will be licensed subject to the Avaya Global Software License Terms found at <http://support.avaya.com/LicenseInfo> or a successor site.

4. INVOICING OF PROFESSIONAL SERVICES

4.1 Professional Services will be invoiced in advance, or as specified in the Order.

4.2 T&M services will be invoiced monthly in arrears.

5. DELAYS

Any delays in the performance of Professional Services caused by Customer may result in additional applicable charges for resource time. If such delay continues for more than 30 days, Avaya may terminate the Order and Customer agrees to pay for all Professional Services performed to date of termination and if applicable, any termination fees.

6. WARRANTY

6.1 Avaya warrants that Professional Services will be performed in a professional and workmanlike manner by qualified personnel, and that for a period of 30 days from the acceptance or deemed acceptance date of the Professional Services, the Professional Services will conform in all material respects to the specifications contained in the Order.

6.2 Remedy. If the Professional Services do not conform to the warranty above and Avaya receives from Customer during the applicable warranty period a written notice describing in reasonable detail how the Professional Services failed to be in conformance, Avaya will, at its option: (i) re-perform the applicable Professional Services or (ii) refund to Customer the fees for the non-conforming Professional Services. In the case of T&M Services, Customer may cancel the affected T&M Services, subject to payment of fees for T&M Services already performed. THESE REMEDIES WILL BE CUSTOMER'S SOLE AND EXCLUSIVE REMEDIES AND WILL BE IN LIEU OF ANY OTHER RIGHTS OR REMEDIES CUSTOMER MAY HAVE AGAINST AVAYA WITH RESPECT TO THE NON-CONFORMANCE OF PROFESSIONAL SERVICES.

6.3 Disclaimer. Professional Services provided to enhance network security are not a guaranty against malicious code, deleterious routines, and other techniques and tools employed by computer "hackers" and other third parties to create security exposures. Neither Avaya nor its suppliers make any warranty, express or implied, that all security threats and vulnerabilities will be detected or that the Professional Services will render an end user's network or particular network elements safe from intrusions and other security breaches.

7. ORDER TERMINATION

RESERVED

8. DEFINITIONS

"Professional Services" means the implementation of Products and other Services described in an Order or Service Description (hereinafter "Services").

"T&M Services" or "time and material Services" are Professional Services which are billed by Avaya based upon the time spent to perform the work and for the materials used.

Order Specific Terms: Support and Managed Services

These Order Specific Terms apply to Orders for Managed or Support Services. Capitalized terms have the meaning given in the Definitions.

1. ORDER AND PROVISION OF SERVICES

In return for the payment of applicable fees and subject to compliance with the terms of the SLA, these Order Specific Terms, and the applicable Service Description or Service Agreement Supplement, Avaya will provide the Support or Managed Services (collectively "Services") options selected by Customer for Supported Products at the Supported Sites set forth in the applicable Order.

2. MONITORING

Avaya may electronically monitor Supported Products for the following purposes: (i) to perform remote diagnostics and corrective actions; (ii) to determine system configuration and applicable charges; (iii) to verify compliance with applicable End User License Agreement; (iv) to assess Customer needs for additional Products or Services to address or resolve Services issues; or (v) as otherwise provided in the Service Description.

3. INCIDENT CORRECTION

Some Services options may include correction of incidents. The incident categories and the corresponding support level, if any, are further described in the applicable Service Description.

4. HELP LINE SUPPORT

Where the selected Services option includes help line support, Avaya will provide it in accordance with the coverage option (service hours, target response intervals, etc.) that Customer has selected.

5. END OF SUPPORT

Periodically, Avaya or a third party manufacturer may declare end of support for certain Supported Products. Customer may access Avaya's user support website (<http://support.avaya.com>, or such successor site) for end of support notifications, and to register an e-mail address to receive e-mail notifications of the same, when published by Avaya. For Products subject to End of Support, Avaya will continue to provide extended support (except for the end of support exceptions listed therein). If the Service Description does not include extended support information, Avaya will make available the description of extended support (if available) for the Products concerned at the same time as its end of support notification. For Products not subject to extended support, if Services are discontinued for a Supported Product, the Supported Product will be removed from the Order and rates will be adjusted accordingly.

6. REPLACEMENT HARDWARE

RESERVED.

7. ADDED PRODUCTS

Added Products will be added to the Order automatically for the remainder of the term at the applicable rates. Customer will inform Avaya without undue delay of any added Products not acquired from Avaya. Added Products purchased from a party other than the manufacturer or an Avaya channel partner may be added to or declined from being added to the Supported Products at Avaya's discretion, and will be subject to certification by Avaya at Avaya's then current Services rates.

8. GENERAL LIMITATIONS

Unless the applicable Service Description provides otherwise, Avaya will provide software Services only for the unaltered current release of the Software and the prior release. The following items are included in the Services only if the Service Description specifically includes them: (i) support of user-defined applications; (ii) support of Supported Products that have been modified by a party other than Avaya (except for installation of standard, self-installed Updates provided by the manufacturer); (iii) making corrections to user-defined reports; (iv) data recovery services; (v) services associated with relocation of Supported Products; (vi) correction of Incidents arising from causes external to the Supported Products (such as power failures or surges); and (vii) services for Supported Products that have been misused, used in breach of their license restrictions, improperly installed or configured, have had their serial numbers altered, defaced or deleted.

9. ADDITIONAL CUSTOMER RESPONSIBILITIES

9.1 General. At Customer's expense, Customer will cooperate with Avaya as reasonably necessary for Avaya's performance of its obligations, including, without

limitation: (i) providing Avaya with full, free and safe access to its facilities; (ii) providing telephone numbers, network addresses and passwords necessary for remote access; (iii) providing interface information for Supported Products and necessary third party consents and licenses to access them; and (iv) any other responsibilities as set out in the applicable Service Description or SOW. If Avaya provides patches or Updates as part of Services, Customer will implement them promptly.

9.2 Provision of Supported Products and Systems. Customer will provide all Supported Products and Supported Sites. Customer continuously represents and warrants that: (i) Customer is either the owner of, or is authorized to access and use, each of them; and (ii) Avaya, its suppliers, and subcontractors are authorized to do the same to the extent necessary to provide the Services in a timely manner.

9.3 Moves of Supported Products. Customer will notify Avaya in advance before moving Supported Products. Identical Services may not be available in all locations and in such circumstances either cancellation charges will apply, or additional charges may apply if Avaya incurs additional costs in providing Services as a result of such moves.

9.4 Vendor Management. Where the applicable SAS states that Avaya provides vendor management for Customer, Customer will provide Avaya, upon request, a letter of agency or similar document, permitting Avaya to perform Vendor Management. Where the third-party vendor's consent is required for Avaya to be able to perform Vendor Management in a timely manner, Customer will obtain the written consent of the vendor and provide Avaya a copy of it upon request.

9.5 Third-Party Hosting. In the event one or more network addresses to be monitored by Avaya are associated with systems owned, managed, and/or hosted by a third-party service provider, Customer will: (i) notify Avaya of the third-party service provider prior to commencement of the Services; (ii) obtain the third-party service provider's advance written consent for Avaya to perform the Services on the third-party service provider's computer systems and provide Avaya with a copy of the consent upon request; and (iii) facilitate necessary communications between Avaya and the third-party service provider in connection with the Services.

9.6 Access to Personal Data. From time to time, Customer may require Avaya to access a Supported Product containing Personal Data. Where Customer instructs Avaya to access any Personal Data, or to provide Customer or a third party identified by Customer with access, Customer will: (i) notify all relevant employees and other individuals of the fact that Avaya will have access to such Personal Data in accordance with Customer's instructions, and (ii) indemnify Avaya and its officers, directors, employees, subcontractors and Affiliates against, and hold each of them harmless from, any and all liabilities, costs, damages, judgments and expenses (including reasonable attorneys' fees and costs) arising out of Avaya accessing or providing access in accordance with Customer's instructions.

10. WARRANTY

10.1 Warranty Scope. Avaya warrants to Customer that, during the applicable warranty period, Services will be carried out in a professional and workmanlike manner by qualified personnel.

10.2 Warranty Period.

10.3 Remedies. If the Service does not conform in any material respect to the warranty above and Avaya receives from Customer during the applicable warranty period a written notice describing in reasonable detail how the Service failed to be in conformance, Customer's sole and exclusive remedy will be for Avaya to re-perform non-conforming Support Services or Managed Services or, if Avaya is unable to re-perform the Services within a reasonable period of time such that they conform in all material respects with the applicable warranty, Avaya shall refund the fees paid for the non-conforming Services.

10.3.1 Warranty Procedures. Customer must provide written notice to Avaya during the applicable warranty period describing in reasonable detail how the Support Services, or Managed Services failed to be in conformance with the applicable warranty.

11. TERM

11.1 Support Service Term. Unless a different term is specified in the applicable Service Description, Avaya will provide Services for an initial term of 1 year. Services will be renewed automatically for successive 1-year terms (unless a longer renewal period is specified in the applicable Service Description) applying the most similar generally available support offer and then current rates, unless either party gives the other written notice of its intent not to renew at least 30 days prior to the expiration of the applicable initial or renewal term.

11.2 Managed Services. Unless a longer initial term or different renewal terms are defined in the Order or Statement of Work, Avaya will provide Managed Services for an initial term of 3 years and such initial term will be renewed automatically for subsequent

1 year periods, applying the then-current rates, unless either party gives the other party written notice of its intent not to renew at least 90 days prior to the expiration of the applicable initial or renewal term.

12. DEFINITIONS

"Managed Services" means the management of Supported Products, including (where applicable) automated client notifications, configuration management, incident and problem management, service desk, and monitoring.

"SAS" or **"Service Agreement Supplement"** means a document that describes the features, terms and conditions of an Avaya Support Services offer.

"SD" or **"Service Description"** means the features, terms and conditions of an Avaya service offer as described in, as the context requires, SOWs or SASs.

"Support Services" means the maintenance and support of Products in accordance with the SD.

"Supported Products" means the Products for which the Services are to be provided, as identified in the applicable Order or SOW, together with any added Products, which may include Products made available for Customer's use as part of Subscription Services and non-Avaya Products to the extent they are specified in the relevant Order or Service Description.

"Supported Sites" means Customer's location(s) to which Services are to be provided, as set out in the applicable Order or SOW.

Order Specific Terms: Cloud Terms

These Order Specific Terms and the Supplemental Terms apply to Orders for Avaya OneCloud™ services and other services delivered from the 'cloud', all as listed in the Matrix ("Cloud Service"). Capitalized terms not defined herein or in the SLSA have the meaning assigned in Exhibit A and, if applicable,

- Schedule 1 (Terms for the purchase of Avaya OneCloud™ CPaaS Services) are part of these Order Specific Terms; and
- Country Specific Additional Terms available at <https://support.avaya.com/TermsOfSale> (or such successor site).

1 TERMS OF SERVICE

- 1.1 Terms of Service.** Upon acceptance of an Order (pursuant to Section 1.1 of the General Terms), Avaya will make the Cloud Services available to Customer for the Initial Term. The Initial Term will renew for consecutive Renewal Terms where auto renew is available, unless either party gives the other 30 days (or longer period if expressly stated in the applicable SOW or Supplemental Terms) advance written notice before the end of the Initial Term or current Renewal Term of their intent not to renew. Where autorenewal is available, the Renewal Term shall be as described in the SOW or Supplemental Terms.
- 1.2 Changes to, and Discontinuation of, the Cloud Service.** From time to time Avaya may update or modify the Cloud Service, including features, functionality and Supplemental Terms, provided that: (a) the change and modification applies to all customers generally, and are not targeted to any particular customer; and (b) one-month prior notice is provided to Customer for any material changes to the Cloud Service or the Supplemental Terms and in such case, Customer has the right to discontinue using the Cloud Service and terminate the respective Service Order without penalty in case of any change to the Cloud Service or Supplemental Terms that is of material detriment to Customer, by written notice within 60 days after Avaya notifies Customer of the change.
- 1.2.1** Avaya will use commercially reasonable efforts to provide 60 days' notice prior to ending the sale of a Cloud Service, at which time the Cloud Service will no longer be available for order. Avaya will continue to provide the Cloud Service through the end of Customer's then current Cloud Service Period.
- 1.3 System Requirements.** Cloud Services are dependent upon Customer's maintenance of internet access, network access and power. Customer is responsible for maintaining all telecommunications (including mobile service and devices), broadband and computer equipment and services needed to access and use the Cloud Services, and for paying all charges associated with these services.
- 1.4 Registration.** Customer may be required to register to use the Cloud Services. Registration may include providing information (e.g., email or physical addresses, etc.) and Customer agrees to keep such information updated.
- 1.5 Use Policies.** When Customer accesses and uses a Cloud Service, Customer is responsible for complying with the SLSA, applicable laws and the Use Policies referenced in the Matrix. The Use Policies are posted on this website: <http://support.avaya.com/TermsOfSale> (or such successor site) and are incorporated into and form part of this SLSA. Avaya may update the Use Policies from time to time and will post the updated version. Such updates will become effective on the next calendar month in which Avaya posts the updated version. Customer is responsible for reviewing the Matrix to determine which Use Policy applies to each Service.

2 PAYMENT, INVOICING, FEES and TAXES

- 2.1 Charges.** Unless otherwise stated in the Supplemental Terms or Order, prices are quoted on a consumption and/or subscription basis and are expressed in local currency. Pricing herein does not include charges for taxes, fees, and government-imposed surcharges, which may be included in the invoices. All fees due to Avaya under this SLSA are non-cancellable and the sums paid are non-refundable, except as otherwise expressly provided in this SLSA. Payments must be made at the address designated on the invoice or as otherwise indicated by Avaya.
- 2.2** If Customer adds or removes users or numbers, during a month, the applicable Subscription fees will be pro-rated for the month.
- 2.3 Price Changes.** Avaya may change the fees associated with any Cloud Services upon 30 days advance written notice. Customer's continued use of the Service after any price change becomes effective constitutes Customer acceptance of the modified fees, and such amounts shall

apply as of the first day of the next month after the fee change was posted or communicated to Customer.

- 2.4 Regulatory Fees.** Customer will be responsible for all governmental assessments, surcharges and regulatory fees pertaining to Customer's use of the Service, that are imposed on Avaya or any Affiliate of Avaya incident to the provision or sale of the Service or chargeable to customers by any governmental entity, including, but not limited to, any government assessment or regulatory fees imposed on Avaya as a result of a material change in the manner in which the Service or Avaya is regulated.

3 SERVICES PROVIDED, USE OF THE SERVICE

- 3.1 Commencement of Cloud Services.** Avaya will notify Customer of the Service Activation Date. Unless Customer notifies Avaya by the close of the second Business Day following the Service Activation Date that the Cloud Services are not operational, the Service Period will commence on the Service Activation Date and will continue until expiration or termination of the Cloud Services.
- 3.2 Support.** Customer may access technical support by sending an email or calling the numbers detailed in the applicable Supplemental Terms.
- 3.3 Customer's Use of Service.** Customer may use the Service solely for Customer's internal business use in accordance with and in the countries designated in the applicable Supplemental Terms, this SLSA and the Order, for avoidance of doubt, not for further sublicense or resale. Customer shall be solely responsible for all activities that occur under Customer's account. Upon request, Customer will provide Avaya with signed confirmation of its compliance with this provision.
- 3.4 Co-operation with Law Enforcement Authorities.** Avaya may charge Customer an administrative fee to recover Avaya's costs that arise from requests from law enforcement authorities, regulatory authorities, or court orders resulting from Customer's use of the Cloud Service.

4 AGREEMENT TERM; TERMINATION; DOWNTIME AND SERVICE SUSPENSION; SURVIVAL

- 4.1 RESERVED).**
- 4.2 Expiration/Termination.** Upon expiration of the Service Period or termination pursuant to Section 4.1 Customer shall immediately cease use of the Service and return or destroy (in accordance with Avaya's instructions) any Deliverables provided to Customer in connection with the Service, including any Avaya's Intellectual Property. Upon request, Customer shall certify in writing to Avaya that Customer has complied with this provision and Avaya may provide such certification to its suppliers.
- 4.3 Service Availability.** Cloud Services (or part) may be unavailable for use by Customer (a) for scheduled downtime to permit Avaya to conduct maintenance, or to modify, upgrade or update the Service, and Avaya will use reasonable efforts to notify Customer of such scheduled downtime in advance in accordance with the Supplemental Terms, (b) without notice in the event that Avaya reasonably believes there may be a denial of service attack or other security risk to the Service, Customer (or its users) or Avaya's other customers, or (c) without notice in the event that Avaya determines that it is necessary or prudent to do so to or for legal or regulatory reasons (collectively, "Service Suspensions"). Avaya shall not be liable to Customer for Service Suspensions.

5 CUSTOMER CONTENT AND MARKS

- 5.1** Customer is solely responsible for Customer Content, including any loss or damage to Avaya, its suppliers or a third party arising from or relating to Customer Content. Customer represents and warrants that it has all necessary rights to, and hereby does, grant to Avaya a limited, non-exclusive, non-transferable, non-sublicensable license to access, use, store, archive for a period of time, modify, display, reproduce, prepare

derivative works of, and distribute Customer Content to the extent necessary for the purpose of providing the Cloud Service.

- 5.2 As between Avaya and Customer, Customer retains all right, title and interest in and to Customer Content. Avaya will not share Customer Content or Other Users' Content with any third parties unless: (a) Avaya has Customer written or electronic consent for sharing any of Customer Content and Other Users' Content; (b) it is required by law; or (c) Avaya provides Customer Content or Other Users' Content to third parties (e.g. sub-contractors) to carry out tasks on Avaya's behalf (e.g., data storage, etc.) as directed by Avaya and subject to appropriate agreements with those third parties.
- 5.3 In connection with the provision of the Cloud Service, Customer hereby grants Avaya a limited, non-exclusive, non-transferable, non-sublicensable license to display Customer trade names, trademarks, service marks, logos, domain names and the like ("Customer Marks") and to host and display likenesses and photo images; provided, that the use of Customer Marks in connection with this SLSA shall not create any right or title in or to the use of Customer Marks and all such use and goodwill associated with Customer Marks will inure to the benefit of Customer.

6 RIGHTS AND DISCLAIMERS

- 6.1 All information transmitted through the Cloud Service is the sole responsibility of the person from whom such information originated. Avaya reserves the right, but is not obligated to pre-screen, refuse, flag, filter, or remove any material posted on the Cloud Service, including any Customer Content, which Avaya, in its sole discretion, deems inconsistent with this Agreement, including any material Avaya has been informed or has reason to believe constitutes intellectual property infringement. Avaya may take the action(s) set forth above, or similar actions, without notice or liability to Customer or any other party. Accordingly, Avaya assumes no liability for any action or inaction regarding transmissions, communications, or content provided by Customer or any third parties.
- 6.2 Customer acknowledges that, in performing the Cloud Service, Avaya may archive Customer Content and Other Users' Content and may periodically delete Customer Content and Other Users' Content without notice to Customer. Customer is solely responsible to ensure that any information, including Customer Content, Customer wishes to retain is downloaded, saved and/or backed-up. Avaya may implement reasonable limits as to the size or duration of storage of any Customer Content or Other Users' Content related to the use of the Service.
- 6.3 Any software security feature is not a guaranty against malicious code, deleterious routines, and other techniques and tools employed by computer "hackers" and other third parties to create security exposures.
- 6.4 It is Avaya's policy to respond to notices of alleged copyright infringement that comply with the United States Digital Millennium Copyright Act and where appropriate at Avaya's discretion to terminate the accounts or subscription of infringers. If Customer would like to send Avaya an alleged copyright infringement notice as it pertains to the Service, go to the following link <http://support.avaya.com/AvayaCopyrightAgent> (or such successor site) and follow the instructions on how to get in touch with Avaya. If Customer has trouble accessing this link, then Customer may contact Avaya for further information at copyrightagent@avaya.com with the subject line: "DMCA Takedown Request" or by mail to:
Avaya Copyright Agent Notification
350 Mount Kemble Avenue, Room 2C109
Morristown, NJ 07960
1-908-953-2044

7 INDEMNIFICATION

RESERVED

8 FEEDBACK

Avaya welcomes Customer Feedback about the Service. All such Feedback provided by Customer or its users to Avaya or its authorized channel partners becomes Avaya's property and Customer agrees to and does hereby grant and assign all intellectual property rights therein to Avaya. Customer agrees to cooperate fully with Avaya in connection with such transfer and assignment and Avaya may use such Feedback however it elects without any monetary or other consideration of any kind owed to Customer or any third party.

9 EXTERNAL LINKS AND THIRD-PARTY SERVICES

In some cases, the Service may contain hyperlinks to External Services and Sites. Customer's use of such External Services and Sites is at Customer's own risk. Customer acknowledges and agrees that Avaya neither endorses nor has any responsibility for the External Services and Sites.

10 SOFTWARE LICENSE TERMS AND UPDATES

- 10.1 If use of the Service requires Customer to download Software or Software is otherwise made available to Customer, such Software is licensed pursuant to (a) the terms and conditions made available to Customer when Customer downloads or installs the Software portion of the Service, or (b) if no such terms and conditions exist, then the applicable Avaya Global Software License Terms posted at <http://support.avaya.com/LicenseInfo> (or such successor site) in effect as of the Service Activation Date will apply, for the sole purpose of using the Service, and solely for the duration of the Service Period.
- 10.2 It is possible that Software may automatically download and install Updates from Avaya or its Affiliates from time to time. In such event, Customer agrees to promptly allow such Updates to be downloaded and installed.

11 RECORDING

If conferences are applicable to the Service Customer is subscribing to, Customer acknowledges that the laws of certain states, provinces or countries require that if a conference is to be recorded, all participants in the conference must be informed of that prior to the recording taking place, so they may consent to being recorded (if required by applicable laws) in the relevant jurisdictions when using recording features. Customer acknowledges and agrees that Customer shall be solely responsible for complying with the local laws in the relevant jurisdictions when using recording features (this includes Customer's obligation to obtain the consent, if required by applicable laws, of all participants before the commencement of the recording). Avaya shall have no liability to Customer or any user or third party if consent is not obtained.

12 EMERGENCY SERVICES, HIPAA and PCI DISCLAIMERS

CUSTOMER HAS READ, UNDERSTOOD, AND AGREES, UNLESS OTHERWISE STATED HEREIN OR IN THE SUPPLEMENTAL TERMS THAT:

- A. THE SERVICE, AS PROVIDED BY AVAYA, IS NOT CONFIGURED TO SUPPORT OR PROVIDE EMERGENCY CALLS OR COMMUNICATIONS OF ANY KIND, INCLUDING, BUT NOT LIMITED TO 112, 999, 911 AND E911 SERVICE.
- B.
- C. THE SERVICE DOES NOT COMPLY WITH THE REQUIREMENTS OF THE PAYMENT CARD INDUSTRY DATA SECURITY STANDARD ALSO REFERRED TO AS PCI OR PCI DSS.

13 GENERAL

Message Routing. Customer may not use phone numbers provided by Avaya to route SMS messages over any other provider's network. All SMS messages sent and received for an Avaya number must be sent and received via the Cloud Services. If Customer uses SMS it is Customer's responsibility to ensure that if Customer initiates any unsolicited SMS, Customer provides Customer's end user with the option to opt in or opt out of receiving those messages as required by applicable law.

EXHIBIT A- Definitions

Defined terms are identified by capitalized letters and have the meaning given in this Exhibit or elsewhere in the Agreement. This Exhibit A is incorporated into and part of the Agreement.

“Acceptable Use Policy” or “AUP” means the document posted at <http://support.avaya.com/TermsOfSale> (or such successor site) which describes actions that Avaya prohibits when any party uses its services.

“Add-on Services” means the implementation, onboarding, professional and/or managed services as described in the applicable Order Specific Terms.

“Affiliate” means, with respect to either party, an entity that is directly or indirectly controlling, controlled by, or under common control with a signatory of this Agreement. For purposes of this definition, **“control”** means the power to direct the management and policies of such party, directly or indirectly, whether through ownership of voting securities, by contract or otherwise; and the term **“controlled”** has the meaning correlative to the foregoing.

“Application” means a software application or website within a Customer’s domain or that Customer creates using the API’s that interfaces or connects to the Cloud Services.

“Business Days” means Monday through Friday, 8:00 to 5:00 pm ET, excluding Avaya holidays.

“Confidential Information” means non-public confidential or proprietary information of the disclosing party that is (a) clearly marked confidential at the time of disclosure or (b) a reasonable person would know, based on the circumstances surrounding disclosure and the nature of the information, that the information should be treated as confidential.

“Customer” means the legal entity which signs this Agreement.

“Customer Content” means the content of all data, information and communications, whether visual, written, audible, or of another nature, sent, displayed, uploaded, posted, published, or submitted by Customer or Customer personnel, including Other Users Content, while utilizing the Service.

“Data Subject” means an identified or identifiable natural person.

“Delivery Date” means the date on which Avaya delivers Equipment in accordance with the applicable Order Specific Terms or, in the case of Software that can be enabled by Avaya remotely or delivered via electronic means, the date the Software is enabled or downloaded to the target processor.

“Deliverables” means customized software, customized documentation, or other work product provided under the applicable Order Specific Terms.

“Dispute” means any dispute, claim or controversy arising out of or relating to this Agreement.

“DPA” means Data Privacy Addendum.

“Documentation” means information published by Avaya or its Affiliates in varying mediums which may include product information, operating instructions and performance specifications that Avaya or its Affiliates generally makes available to users of its products. Documentation does not include marketing materials.

“Effective Date” means the date in which the last party signs this Agreement.

“Equipment” means phones compatible with the Service or other hardware.

“External Services and Sites” means non-Avaya websites, content, or resources or otherwise interface or work with third party services which are not maintained or controlled by Avaya.

“Feedback” means comments or suggestions.

“Initial Term” means the term of the Subscription that is indicated in Customer’s order and commences upon the date the Service is available for Customer’s use.

“Matrix” means the chart that is posted on the following website (or such successor site): <http://support.avaya.com/TermsOfSale> and referred to as the Master Cloud Agreement Matrix that indicates the Schedules and Supplemental Terms that apply to a specific Service. Avaya reserves the right to update the Matrix.

“Other Users’ Content” means the content of any information and communications, whether visual, written, audible, or of another nature, sent, displayed, uploaded, posted, published, or submitted by other users while interacting with the Service, including, without limitation, likenesses or photo images, advertisements or sponsored content.

“Personal Data” means data that identifies or may be used to identify an individual.

“Processing,” “Process,” “Processed” means any operation or set of operations which is performed on Personal Data or on sets of Personal Data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

“Project Phase” means a defined activity, objective or period as set out in the applicable SOW during which Add-On Services will be provided.

“Rejection Notice” means a notice Avaya receives from Customer before the end of the Acceptance Period indicating in reasonable detail the material failure of the Add-On Services, Deliverable, or Project Phase to conform to the agreed acceptance criteria in the acceptance procedures.

“Renewal Term” means each of the subsequent terms after the Initial Term.

“Service Activation Date” means the date Avaya advises Customer that the Cloud Services are available for Customer’s use.

“Service Description” means the applicable description of the Cloud Services then current as of the date of Customer’s ordering of the Cloud Services which is incorporated by reference and is available to Customer upon request or via links in the Matrix.

“Service Period” means the period of time in which Avaya is providing Cloud Services to Customer, whether the Initial Term or Renewal Term.

“Software” means computer programs in object code, provided by Avaya whether as stand-alone products or pre-installed on Equipment, and any upgrades, Updates, patches, bug fixes, or modified versions thereto.

“Statement of Work” or “SOW” means a Customer-specific document(s) that describes the features, terms and conditions of an Avaya service being purchased by Customer.

“Supplemental Terms” means, individually or collectively, the Use Policies and Service Descriptions.

“T&M Services” or “time and material Services” means Add-On Services which are billed by Avaya based upon the time spent to perform the work and for the materials used.

“Third-Party Products” means any product made or provided by a party other than Avaya, including: (i) products ordered by Customer from third parties; (ii) products provided by Avaya that are recognizable as standalone items, and; (iii) products identified as separate items on Avaya’s price list, quotes, Order specification forms or Documentation.

“Third-Party Services” means any non-Avaya branded service provided under this Agreement.

“Traffic Data” means user billing data and/or metadata, including Caller ID, name, number dialed, duration of call, landline or mobile originated call, SMS send / receive destinations.

SCHEDULE 1 - Terms for the Purchase of Avaya OneCloud™ CPaaS

These terms for the purchase of Avaya OneCloud™ CPaaS apply to Customer's purchase and use of any CPaaS Services. Any capitalized terms used in this Schedule have the meaning given to them herein or in the General Terms.

1. MANDATORY PREREQUISITES FOR THE AVAYA ONECLOUD™ CPAAS TERMS OF SERVICE

In order to use the Avaya API's and markup language (the "API"), or make use of the Properties and various Avaya OneCloud™ CPaaS services and information contained therein (the API, Properties and Avaya OneCloud™ CPaaS services are collectively referred to herein as the "**Avaya CPaaS Services**") and are included within the definition of "Services, Customer must accept the terms in this Schedule.

Customer agrees to incorporate terms and conditions into the terms and conditions that apply to Customer's own products and services using applications that incorporate the Avaya CPaaS Services ("**Customer's End User Agreements**") that enable Avaya to use Customer's or any of Customer's users, employees, clients or customers' ("**End Users**") data as necessary to provide the Avaya CPaaS Services and that protect Avaya's rights to the same extent as the terms and conditions of this Schedule and the Agreement. By way of example, Customer's End-User Agreements must include terms concerning restrictions on use, protection of proprietary rights, disclaimer of warranties, and limitations of liability. Customer must ensure that Customer's End Users using applications that incorporate the API or the Avaya CPaaS Services adhere to this Agreement, and Customer agrees to notify Avaya promptly if Customer becomes aware of any breach of the terms of Customer's End-User Agreements that may impact Avaya. Customer will take all reasonable precautions to prevent unauthorized access to or use of the Avaya CPaaS Services and notify Avaya promptly of any such unauthorized access or use.

2. GRANT OF RIGHTS TO USE THE SERVICE

2.1 So long as Customer is in compliance with this Agreement, Avaya hereby grants Customer a limited, non-exclusive, non-transferable, non-sublicensable, revocable right and license during the Service Period to access and use the Avaya CPaaS Services, solely in accordance with this Agreement. Unless explicitly stated otherwise, any new features provided by Avaya that augment or enhance the current Avaya CPaaS Services shall also constitute "Avaya CPaaS Services" and shall be subject to this Agreement. Customer may not, nor may Customer allow any third party to, copy, distribute, sell, disclose, lend, transfer, convey, modify, decompile, disassemble or reverse engineer the Avaya CPaaS Services for any purpose whatsoever. Customer may not allow any unauthorized third party to access the Avaya CPaaS Services for any purpose whatsoever. All rights not expressly granted under this Agreement are retained by Avaya or its Affiliates, licensors or suppliers.

2.2 Customer may create a software application or website (an "**Application(s)**") that interfaces with the Avaya CPaaS Services, provided that Customer complies with this Agreement. Customer may use the Avaya CPaaS Services to execute Applications owned or lawfully obtained by Customer, except as limited by this Agreement or Customer's End User Agreement.

2.3 Customer and any Applications that Customer may create, build or distribute may make network calls or requests to the Avaya CPaaS Services, or may receive telephone calls via the Avaya CPaaS Service, at any time that the Avaya CPaaS Services are available, provided that those requests do not violate this Agreement.

2.4 Customer may not remove, obscure, or alter any notice of any Avaya trademark, service mark ("**Marks**") or other intellectual property or proprietary right appearing on the Avaya CPaaS website posted at <https://www.avaya.com/en/products/CPaaS/> or such successor site ("**Website**") or contained within the Avaya CPaaS Services.

2.5 Customer acknowledges that Avaya may change APIs for any Avaya CPaaS Service or any feature of an Avaya CPaaS Service from time to time, and that it is Customer's responsibility to ensure that calls or requests from Customer's Applications made to or via Avaya CPaaS Services are compatible with then-current APIs for the Avaya CPaaS Services. Avaya will attempt to provide reasonable prior notice to Customer of any API changes so Customer can adjust Customer's Applications, but Avaya is under no obligation to do so.

2.6 Customer is solely responsible for Customer's Applications, including any data, text, images or content contained therein. Customer is also solely responsible for all traffic originating from Customer's Applications that uses Customer's account credentials to access the Avaya CPaaS Services. Actions taken using Customer's credentials shall be deemed to be actions taken by Customer, with all associated consequences including charges for Avaya CPaaS Services, service termination, civil and criminal penalties.

2.7 Avaya may make available to Customer, for Customer's installation, copying or use in connection with the Avaya CPaaS Services, a variety of software, data and other content and printed and electronic documentation (the "**Properties**"). Avaya hereby grants to Customer a limited, non-exclusive, non-transferable, non-sublicensable, revocable license, during the Service Period only, to install, copy and use the Properties solely in connection with and as necessary for Customer's use of the Avaya CPaaS Services in accordance with this Agreement. The Properties may include, without limitation: (a) The Website; (b) APIs; (c) Documentation; and (d) Specifications describing the operational and functional capabilities, use limitations, technical and engineering requirements, and testing and performance criteria relevant to the proper use of the Avaya CPaaS Service and its related APIs and technology.

2.8 Avaya may make additional content or software available under another license agreement, such as an open source license. Any such content or software will be clearly marked with such a license indicating the usage rights available for that content or software. Such content or software may include: (a) Developer tools, such as software development kits or sample code for use in connection with the APIs; and (b) Articles and documentation for use in connection with the use and implementation of the APIs (collectively, "**Documentation**").

2.9 Except as may be expressly authorized under this Agreement: (a) Customer may not, and may not attempt to, modify, alter, tamper with, repair, or otherwise create derivative works of the Properties; (b) Customer may not, and may not attempt to, reverse engineer, disassemble, or decompile the Properties or the Avaya CPaaS Service or apply any other process or procedure to derive the source code of any software included in the Properties.

2.10 Customer hereby grants Avaya a limited, non-exclusive, non-transferable, non-sublicensable license to display Customer's trade names, trademarks, service marks, logos, domain names and the like for the purpose of providing the Avaya CPaaS Services to Customer or promoting or advertising that Customer uses the Avaya CPaaS Services. Customer may not display or use the Properties in any manner unless Customer obtains Avaya's prior written consent. All uses of the Marks and goodwill associated therewith shall inure to the benefit of Avaya or its Affiliates.

The rights granted by Avaya in this Agreement with respect to the Properties and the Avaya CPaaS Services are nonexclusive, and Avaya reserves the right to: (i) act as a developer of products or services similar to any of the products or services that Customer may develop in connection with the Properties or the Avaya CPaaS Services; and (ii) grant similar rights to those provided under this Agreement to third parties that as developers or systems integrators may offer products or services which compete with Customer's Application(s).

2.11 Customer understands and acknowledges that Avaya is not certifying or endorsing, and has no obligation to certify or endorse, any of Customer's Applications or Customer's Content.

3. SUSPENSION OR TERMINATION

Avaya may suspend or terminate Customer's right to use the Avaya CPaaS Service for cause immediately upon Avaya's notice to Customer in accordance with the notice provisions set forth in this Agreement if: (i) Customer or Customer's End Users violate, or Avaya has reason to believe that Customer or Customer's End Users have violated, any provision of the AUP; (ii) there is an unusual spike or increase in Customer's use of the Avaya CPaaS Service, and there is reason to believe such traffic or use is fraudulent or negatively impacting the operating capability of the Avaya CPaaS Service; (iii) Avaya determines, in Avaya's sole discretion, that Avaya's provision of the Avaya CPaaS Service to Customer is prohibited by applicable law, or has become impractical or unfeasible due to any legal or regulatory change; or (iv) subject to applicable law, upon Customer's liquidation, Customer's commencement of dissolution proceedings, the disposal of Customer's assets, the failure to continue Customer's business, an assignment for the benefit of Customer's creditors, or Customer's becoming the subject of a voluntary or involuntary bankruptcy or similar proceeding.

4. BACKUP AND RETENTION

Notwithstanding Sections 8 and 9 of the General Terms, Customer acknowledges that Customer bears sole responsibility for adequate backup of Customer's Content, including all audio recordings associated with Customer's account. AVAYA SHALL HAVE NO LIABILITY WHATSOEVER FOR ANY DAMAGE, LIABILITIES, LOSSES

(INCLUDING ANY LOSS OF DATA OR PROFITS) OR ANY OTHER CONSEQUENCES THAT CUSTOMER OR CUSTOMER'S END USERS MAY INCUR WITH RESPECT TO LOSS OF DATA ASSOCIATED WITH CUSTOMER'S ACCOUNT AND CUSTOMER'S OR ANY OF CUSTOMER'S END USERS' CONTENT DATA THEREIN.

5. INTELLECTUAL PROPERTY

5.1 Other than the limited use and access rights and licenses expressly set forth in this Agreement, Avaya and/or its Affiliates, suppliers and licensors reserve all right, title and interest (including all intellectual property and proprietary rights) in and to: (i) the Avaya CPaaS Services; (ii) the Properties; (iii) the Marks; and (iv) any other technology and software that Avaya provides or uses to provide the Avaya CPaaS Services and the Properties. Customer does not, by virtue of this Agreement or otherwise, acquire any ownership interest or rights in the Avaya CPaaS Services, the Properties, the Marks, or any other technology and software, except for the limited use and access rights described in this Agreement.

5.2 Avaya may, at its discretion, offer certain software development kits, tools, application samples, documentation or other software under an open source license. Any such products will be marked with copyright details, and those copyrights will apply to those and only those software development kits, tools, application samples, documentation or other software. Avaya, its Affiliates, suppliers and licensors reserve all rights to any documents, tools, services, technologies and the like not subject to an open source license.

5.3 Other than the rights and interests expressly set forth in this Agreement and excluding any and all works derived from Properties, Customer reserves all right, title and interest (including all intellectual property and proprietary rights) in and to: (i) Customer Content Customer may send to Avaya or use as part of Customer's use of the Avaya CPaaS Services; and (ii) Customer's Applications.

5.4 During and after the Services Period, with respect to the Avaya CPaaS Services that Customer elects to use, Customer will not assert, nor will Customer authorize, assist, or encourage any third party to assert, against Avaya or any of Avaya's Affiliates, customers, end users, vendors, business partners (including third-party sellers on websites operated by or on behalf of Avaya), sub-licensees or transferees, any patent infringement or other intellectual property infringement claim with respect to such Avaya CPaaS Services.

6. REPRESENTATIONS

6.1 Customer represents and warrants that Customer will not use the Avaya CPaaS Services, Properties, Marks, Customer's Application or Customer's Content in a manner that violates this Agreement. Although Avaya does not assume the duty or obligation to monitor any materials created, posted or uploaded by Customer or any third parties, Avaya reserves the right, in its sole and absolute discretion, to monitor any and all materials posted or uploaded by Customer or any third parties at any time without prior notice to ensure that they conform to any usage guidelines or policies (including Avaya's AUP).

6.2 Customer shall not use the Avaya CPaaS Services to create a medical device or take other action that would violate regulations promulgated by the Food and Drug Administration, including but not limited to (i) diagnosing a disease or other condition, (ii) curing, mitigating, treating, or preventing a disease or condition, or (iii) using the Avaya CPaaS Services in a way that may affect the structure or function of the body of a human or animal. Avaya shall have no liability of any kind whatsoever as a result of Customer's violation of this Section. Customer's violations of this Section will be subject to the indemnification provisions in this Agreement.

6.3 Customer represents and warrants that Customer is responsible for any charges incurred by virtue of Customer's use of the Avaya CPaaS Services, no matter whether Customer's Application acted in error. Customer also represents and warrants: (i) that Customer is solely responsible for the development, operation, and maintenance of Customer's Application and for Customer's Content, including, the accuracy, appropriateness and completeness of Customer's Content and all product-related materials and descriptions; (ii) that Customer has the necessary rights and licenses, consents, permissions, waivers and releases to use and display Customer's Application and Customer's Content; (iii) that neither Customer's Application nor Customer's Content (a) violates, misappropriates or infringes any rights of Avaya or any third party, (b) constitutes defamation, invasion of privacy or publicity, or otherwise violates any rights of any third party, (c) violates any applicable laws or regulations, or (d) is designed for use in any illegal activity or promotes illegal activities, including, without limitation, activity that might be libelous or defamatory or otherwise malicious, illegal or harmful to any person or entity, or discriminatory based on race, sex, religion, nationality, disability, sexual orientation, or age; (iv) that neither Customer's Application nor Customer's Content contains any components capable of harming Avaya's network or Avaya CPaaS Services; and (v) to the extent to which Customer is authorized by Avaya to use any of the Marks, that Customer will conduct Customer's business in a professional manner and in a way that reflects favorably on the goodwill and reputation of Avaya.

6.4 Customer agrees to abide by all applicable local, state, national, foreign and international laws and regulations and that Customer will be solely responsible for all acts or omissions that occur under or through Customer's account or password, including the content of Customer's and Customer's customers' transmissions through the Avaya CPaaS Services. Customer further agrees that neither Customer nor Customer's End Users will use the Avaya CPaaS Service for any purpose that is unlawful, abusive, intrusive on another's privacy, harassing, libelous, threatening or hateful, or in any other way that would violate any applicable laws or regulations. Customer represents and warrants that (i) Customer has the legal right and authority, and will maintain the legal right and authority during each Service Term, to install and use the Avaya CPaaS Services as contemplated hereunder; (ii) the performance of Customer's obligations under this Agreement and use of Avaya CPaaS Services will not violate any applicable law, rule or regulation or any applicable manufacturers' specifications or unreasonably interfere with Avaya's or its other customers' use of the Avaya CPaaS Services or network; (iii) Customer is authorized and has completed all required corporate actions necessary to execute this Agreement; and (iv) Customer shall not intentionally carry out any act or omission that results in Avaya breaching any law, rule or regulation. Customer shall comply with all the applicable legal and/or regulatory licenses and consents specifically required from the relevant governmental authorities with respect to any permitted resale of the Avaya CPaaS Services. Customer shall be solely responsible and liable for any misuse of the Avaya CPaaS Services by Customer's End Users or any third parties in respect of Customer's resale of the Avaya CPaaS Services and shall defend and indemnify and hold harmless Avaya for against any claims or proceedings, including any judgments, settlements and reasonable attorneys' fees resulting from and against any and all third party claims or proceedings arising from or related to such resale of the Avaya CPaaS Services by Customer. Any failure by any third party (including End Users) to comply with any applicable law rule or regulation regarding sale or use of the Avaya CPaaS Services shall be attributable to Customer for the purposes of this Agreement. Any resale or sublicense by Customer of the Avaya CPaaS Services shall not relieve Customer of Customer's obligations under this Agreement. Any such third party waives any liability by Avaya in connection therewith.

6.5 Customer represents and warrants that without Avaya's express written consent Customer will not use, and will not authorize any third party to use, any Public Software (as defined below) in connection with the Avaya CPaaS Services in any manner that requires, pursuant to the license applicable to such Public Software, that any Properties or the Avaya CPaaS Services be (i) disclosed or distributed in source code form, (ii) made available free of charge to recipients, or (iii) modifiable without restriction by recipients. Customer represents and warrants that all Feedback and Communications contributed by or through Customer (a) are legally distributable by Customer, either because Customer owns the copyright or because Customer has fully complied with any copyright terms associated with the software or content, (b) contain no third-party software or any software that may be considered Public Software, and (c) do not violate, misappropriate or infringe any intellectual property rights of any third party. **"Public Software"** means any software, documentation or other material that contains, or is derived (in whole or in part) from, any software, documentation or other material that is distributed as free software, open source software (e.g., Linux or Asterisk) or similar licensing or distribution models, including, but not limited to software, documentation or other material licensed or distributed under any of the following licenses or distribution models, or licenses or distribution models similar to any of the following: (1) GNU Affero General Public License (AGPL), Common Public Attribution License (CPAL), European Public License (EURL), GNU's General Public License (GPL), Lesser/ Library GPL (LGPL), or Free Documentation License, (2) The Artistic License (e.g., PERL), (3) the Mozilla Public License, (4) the Netscape Public License, (5) the Sun Community Source License (SCSL), (6) the Sun Industry Standards License (SISL), (7) the BSD License and (8) the Apache License.

6.6 In addition to the foregoing, Avaya specifically disclaims all liability for, and Customer agrees that Customer shall be solely responsible for:

- the development, operation, and maintenance of Customer's Application, all related equipment, and all materials that appear on or within Customer's Application and Customer's Content;
- the accuracy and appropriateness of any materials posted on or within Customer's Application or Customer's Content (including, among other things, any product-related materials);
- ensuring that any materials posted on Customer's site or within Customer's Application do not violate Avaya's AUP, are not illegal and do not promote illegal activities, including any activities that might be libelous or defamatory or otherwise malicious, illegal or harmful to any person or entity, or discriminatory based on race, sex, religion, nationality, disability, sexual orientation, or age;

- ensuring that Customer's Application accurately and adequately discloses, either through a privacy policy or otherwise, how Customer collects, uses, stores, and discloses data collected from visitors, including, where applicable, that third parties (including advertisers) may serve content and/or advertisements and collect information directly from visitors and may place or recognize cookies on visitors' browsers; and
- any of Customer's End Users' claims relating to Customer's Application or Customer's Content or the Avaya CPaaS Services utilized in connection with Customer's Application.

7. LIABILITY FOR EMERGENCY CALLING

TO THE EXTENT PERMITTED UNDER APPLICABLE LAW, AVAYA AND ITS AFFILIATES, OFFICERS, DIRECTORS, EMPLOYEES, CONTRACTORS, AGENTS, LICENSORS, SUPPLIERS, AND RESELLERS ("EMERGENCY SERVICES INDEMNIFIED PARTIES") WILL HAVE NO LIABILITY TO CUSTOMER, CUSTOMER'S USERS, OR ANY THIRD PARTY, AND CUSTOMER WAIVES ALL CLAIMS AND CAUSES OF ACTION, ARISING OUT OF OR RELATED TO CUSTOMER'S, CUSTOMER'S USERS, OR ANY THIRD PARTY'S INABILITY TO DIAL LOCAL EMERGENCY NUMBERS (SUCH AS 112, 911, 999) OR ANY OTHER EMERGENCY TELEPHONE NUMBER OR TO ACCESS AN EMERGENCY SERVICE OPERATOR OR EMERGENCY SERVICES. CUSTOMER HEREBY RELEASES AND AGREES TO INDEMNIFY, DEFEND, AND HOLD HARMLESS THE EMERGENCY SERVICES INDEMNIFIED PARTIES FROM ANY AND ALL CLAIMS, LIABILITY, DAMAGES, LOSSES, EXPENSES, AND/OR COSTS (INCLUDING BUT NOT LIMITED TO ATTORNEYS' FEES AND COST OF SUIT) BY OR ON BEHALF OF CUSTOMER OR ANY THIRD PARTY OR USER ARISING FROM OR RELATED TO THE FAILURE OF EMERGENCY SERVICES TO FUNCTION OR FUNCTION PROPERLY OR AVAYA'S PROVISION OF EMERGENCY SERVICES OR FAILURE TO PROVIDE ACCESS TO EMERGENCY SERVICES.

ATTACHMENT E2

MASTER TERMS

Intentionally left blank.

ATTACHMENT E3

PRICING



Section Nine: Pricing

Pricing associated with the Bid shall be inserted in this section and shall be in the required structure set forth above in Subsection 8.1, if any.

AVAYA RESPONSE:

Avaya is pleased to provide its suite of SaaS communications solutions and products to the State of Oklahoma and its eligible customers. The table below and also included in Appendix I – Pricing, Exhibit 1: Price provides a summary of the discounts by Avaya Material Group. Appendix I provides the details of Exhibit 1 and Exhibit 2.

Exhibit 1: Price Avaya State of Oklahoma (RFP 0900000556) Avaya Discount Summary		
Material Product Group (MPG)	Group / Description	State of Oklahoma Discount off Avaya Price List
5P	Software Contact Center – Heritage Nortel	20%
7P	OEM	12%
8P	Video	32%
9P	SMEC	20%
1R	Avaya Cloud Office / SIP	0.0%
8S	Contact Center Subscription Services	0.5%
9S	Unified Communications Subscription Services	0.5%
1T	Cloud Offers	0.5%
2R	Alliances	0.0%

Cost Savings

The Bidder will work in the best interest of the state and its customers to leverage volume or enterprise license agreements and maximize cost savings through better pricing, publisher's promotions, or other savings opportunities.



OKLAHOMA
Office of Management
& Enterprise Services

BID RESPONSE PACKET

AVAYA

ATTACHMENT E4
VALUE ADD SERVICES



Section Ten: Offer of Value-Added Products and/or Services

If a Bid includes an offer of value-added products and/or services, such offer shall be inserted in this section and include associated pricing and any other information relevant to such value-added offer. However, the State is not obligated to purchase value-added products or services.

AVAYA RESPONSE:

10.0 Introduction

Avaya's approach to value-added services is more than a marketing slogan; value permeates how we build solutions, transact business and interact with customers. State customers will benefit from a range of value-added services, including:

- Flexible procurement options
- Scalable and modular solutions with an open architecture
- Design review solution ROI assessments
 - Help determine the impact of a total solution on the organization
- State customer campaigns and promotions
 - Try it before you buy it
 - Trade-in / Trade up incentives
 - Software/licensing credits
 - Solutions with features such as training, reporting, and management built-in' not added on

Bidder should provide information on value-add services that include but are not limited to product installation, maintenance and support, managed services, professional services and product training. Any Bidder offering product-related services must submit a description of those services and the related pricing in the Excel spreadsheet attached as Exhibit 2.

AVAYA RESPONSE:

Avaya is the only major communications and collaboration solution provider that can offer public, private, or hybrid cloud at enterprise scale to customers of all kinds – this is a true differentiator. In addition, our expertise in building open, converged, and innovative solutions to enhance and simplify communications and collaboration in the cloud, on-premise, or a hybrid of both. Avaya provides Oklahoma with the complete catalog of our products and services to allow for the selection of the right solution at a competitive price. Our experienced team delivers award-winning services including, initial planning and design, seamless implementation and integration, ongoing managed operations, optimization, training, and support.

Highlighted below are examples of additional Avaya offerings that enhance and augment Avaya's SaaS solutions.



10.1 Communications Platform as a Service (CPaaS)

Elastic SIP: The Avaya cloud SIP trunking offers a flexible and pure consumption-based voice service. Avaya’s CPaaS enables our customers and partners to integrate a wide range of features, including SIP Trunking, global DID and 800 services, voice notification messaging, and API workflows into a new cloud or even their current premise-based communications systems – the latter two previously highlighted. Avaya CPaaS can be used in support of both cloud and premises solutions.

The Avaya Elastic SIP services offer is typically a lower-cost alternative to traditional digital trunking, such as PRI, T1/E1, FT1/FE1, as well as Analog Trunks. A simpler, more affordable solution does not mean lower service quality or fewer options. Avaya’s cloud-based Elastic SIP services no longer require PRI, legacy SIP trunks, etc., and it is now connected via existing customer Internet services. The customer is responsible to provide sufficient internet connectivity to use the Services. Our Elastic SIP services will make the State’s communications architecture more flexible and resilient.

There are multiple components to Avaya’s elastic SIP services offer:

- Local inbound & outbound voice calling
- International Long-Distance calling
- Toll-Free Service
- Local Number (DID)
- Emergency Services (E911)
- Number Porting

Key Features

Exhibit 10-1: Avaya Elastic SIP Service Key Features



**CPaaS solutions are provided by Avaya Cloud Inc., a wholly-owned subsidiary of Avaya Inc, and will be separately contracted and invoiced through Avaya Cloud Inc.*

The table below provides a comparison of traditional Telco SIP Trunking vs. Avaya’s cloud-based Elastic SIP Services.



Traditional Telco SIP Trunking		Avaya Cloud Elastic SIP
Service Availability	Customers should consider the limitation of region-based numbers of Telco and the long process of porting over numbers.	Generally quicker with provisioning and porting phone numbers. Wider reach in regions including providing in-country local voice services in US, Canada, UK, and Ireland.
Pricing	Charge for usage minutes as well as a monthly capacity fee for each trunk.	Only charge on usage.
Service Provisioning	Weeks	Minutes
Scalability	Fixed capacity - customers must plan for their peak periods up-front.	On-demand capacity – elasticity allows customers to be covered during peak periods without planning ahead.

Local and Domestic Inbound and Outbound Calling

Two Options are available to the Customers:

Per-Seat

- Each seat can receive inbound calls and place outbound calls and includes one DID.
- Includes an “unlimited” number of Local and Domestic Long Distance Inbound and Outbound minutes, subject to Avaya Cloud Inc.’s Fair Usage Policy of a combined 1000 minutes of calling traffic per month per seat.

A la Carte

- Select for SIP Trunking purely based on minutes and billed at the end of each month for minutes used.

International Long Distance

Avaya supports calling-to approximately 200 destinations worldwide. The international long-distance bundle is available to be purchased only with any of the other bundles. It includes 1000 minutes of calling per month to the indicated countries.

International long-distance rates for all other countries are charged by the minute specific to the country called. All billing is calculated in 1-minute increments.

Toll-Free Service

Toll-Free/Free-Phone Service allows the customer to receive calls without Long Distance charges incurred by their customers.

Local Number (DID)

Additional DID/DDI numbers may be purchased for those choosing the Per Trunk service

Emergency Services (E911)

Emergency Services are supported subject to certain limitations and require phone and softphone registration. Customers must read and understand their service agreement.

Number Porting



Avaya lets Customers keep their current phone number and incorporate it into the new Avaya elastic SIP service. Transferring an existing number into a new service requires the Customer's permission and is called porting. Porting times vary and are dependent on the Customer's current provider.

The Customer's current number will continue to work until the provider processes the request. Since there is no way to predict when that will occur, Avaya will provide the Customer with a temporary number until the porting is completed. This temporary number is automatically attached to the Service and will work with all telephones and softphones connected to the Service. Once the existing number has been successfully ported, it will be added to the Customer's Service, and the temporary number will be removed.

In addition to the Value Added services OMES directly associated with the sales of software, such as related maintenance and support agreements for new and previously purchased software, the Bidder would provide, at no additional cost, management services to include, but not be limited to, providing price quotes, tracking licenses (new and existing), management of licenses, monitoring volume levels and opportunities for cost savings, training, installation/de-installation/implementation support, and software advisement to OMES and/or OMES Customers.

Bidders would be expected to provide, at no additional cost, assistive and support services regarding the software that is representative of the State's interest and best value.

AVAYA RESPONSE:

10.2 Avaya OneCloud Private and OneCloud for Government Implementation Team

Included with Avaya cloud implementations, a team of subject matter experts (SMEs) having the following roles and overall responsibilities will be available to the State at no extra charge:

Team Member Role	Overall Responsibility
Program Manager:	Overall project success.
Enterprise Architect:	Cloud architecting and design.
Project Coordinator:	Serves as a deputy to the Program Manager.
Transition Coordinator:	Manages transition and onboarding.
Business Integration Manager:	All application integration.
Service Delivery Manager:	Change management.

10.3 Investment Protection Program

Avaya values its loyal customers and offers Investment Protection Program discounts which are applied to the first term of the Avaya Subscription contract as follows:

- Licenses surrendered under current Support + Upgrade Subscription contracts are eligible for 40% credit at the initial first contract term.
- Licenses surrendered under current Support contracts are eligible for 20% credit at the initial first contract term.



OKLAHOMA
Office of Management
& Enterprise Services

BID RESPONSE PACKET



-
- In cases where there is a mix of coverage levels across a product category Investment Protection Credits will be determined based on the coverage level associated with the majority of the licenses.
 - Investment Protection Credits will be calculated as a percentage off the List Price.

ATTACHMENT E5

THIRD PARTY TERMS

Intentionally left blank.

ATTACHMENT F

Any requested exceptions not listed below are declined.

All requested exceptions are declined by the State of Oklahoma.

(remainder of page intentionally left blank)

ATTACHMENT F1
STATE OF OKLAHOMA CONTRACT WITH AVAYA 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

AVAYA 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: _____









Final Contract

Final Audit Report

2023-12-22

Created:	2023-12-21
By:	Beth Vincent (beth.vincent@omes.ok.gov)
Status:	Signed
Transaction ID:	CBJCHBCAABAArRg6u35403Sj07GVSzT6T2RM24WVKYKB

"Final Contract" History

-  Document created by Beth Vincent (beth.vincent@omes.ok.gov)
2023-12-21 - 9:34:31 PM GMT
-  Document emailed to jeniferbond@avaya.com for signature
2023-12-21 - 9:35:50 PM GMT
-  Email viewed by jeniferbond@avaya.com
2023-12-21 - 11:02:47 PM GMT
-  Signer jeniferbond@avaya.com entered name at signing as Jenifer Bond
2023-12-21 - 11:26:42 PM GMT
-  Document e-signed by Jenifer Bond (jeniferbond@avaya.com)
Signature Date: 2023-12-21 - 11:26:44 PM GMT - Time Source: server
-  Document emailed to Joe McIntosh (joe.mcintosh@omes.ok.gov) for signature
2023-12-21 - 11:26:46 PM GMT
-  Document e-signed by Joe McIntosh (joe.mcintosh@omes.ok.gov)
Signature Date: 2023-12-22 - 4:09:29 PM GMT - Time Source: server
-  Agreement completed.
2023-12-22 - 4:09:29 PM GMT