



STATE OF OKLAHOMA STATEWIDE CONTRACT WITH DELOITTE

This State of Oklahoma Statewide Contract (“Contract”) is entered into between the state of Oklahoma by and through the Office of Management and Enterprise Services and Deloitte (“Supplier”) in connection with Oklahoma Statewide Contract No. 1044 and is effective as of the date of last signature to this Contract. The term of this Contract is for one (1) year and there are four (4) one-year options to renew the Contract which the parties may exercise via signed, written agreement.

Purpose


The State is awarding this Contract to Supplier for the provision of eDiscovery as a Service 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 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 # 09000000467, Attachment A;
 - 2.2. State of Oklahoma General Terms, Attachment B;
 - 2.3. Statewide Contract Terms, Attachment C;
 - 2.4. State of Oklahoma Hosting Terms, Attachment D;
 - 2.5. Supplier Pricing & Portions of the Bid, Attachment E
 - i. SOW Template; Attachment E, Ex-1;
 - ii. Behavior and User Agreement, Attachment E, Ex-2
 - 2.6. Negotiated Vendor Exceptions, Attachment F.
3. Any reference to a Contract Document refers to such Contract Document as it may have been amended. If and to the extent any provision is in multiple documents and addresses the same or substantially the same subject matter but does not create an actual conflict, the more recent provision is deemed to supersede earlier versions.

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

Deloitte

By: 

Name: D. Jerry Moore

Title: Chief Information Officer

Date: Nov 17, 2021

By: 
[Christopher Knox \(Nov 16, 2021 16:03 EST\)](#)

Name: Christopher Knox

Title: Managing Director

Date: Nov 16, 2021

ATTACHMENT A
SOLICITATION NO. 0900000467

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 eDiscovery as a Service Supplier. The Office of Management and Enterprise Services (OMES) Information Services (IS) has a data team that handles Oklahoma Agencies electronically stored information (ESI) discovery requests and fulfills them using Veritas Clearwell and Microsoft Office 365.

OMES averages 80 requests per month resourced from approximately four petabytes of stored data. The Supplier(S) awarded a contract under this solicitation will be required to work with the OMES IS data team to facilitate agency requests.

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 four (4) options to renew the Contract.

Exhibit 7a Safeguarding Contract Language for General Services

I. PERFORMANCE

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

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

(Include any additional safeguards that may be appropriate.)

II. CRIMINAL/CIVIL SANCTIONS

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

- (1) Each officer or employee of any person to whom returns or return information is or may be disclosed shall be notified in writing by such person that any return or return information made available in any format shall be used only for the purpose of carrying out the provisions of this contract. Information contained in such material shall be treated as confidential and shall not be divulged or made known in any manner to any person except as may be necessary in the performance of this contract. Inspection by or disclosure to anyone without an official need-to-know constitutes a criminal misdemeanor punishable upon conviction

by a fine of as much as \$1,000.00 or imprisonment for as long as 1 year, or both, together with the costs of prosecution. Such person shall also notify each such officer and employee that any such unauthorized inspection or disclosure of returns or return information may also result in an award of civil damages against the officer or employee [United States for Federal employees] in an amount equal to the sum of the greater of \$1,000.00 for each act of unauthorized inspection or disclosure with respect to which such defendant is found liable or the sum of the actual damages sustained by the plaintiff as a result of such unauthorized inspection or disclosure plus in the case of a willful inspection or disclosure which is the result of gross negligence, punitive damages, plus the costs of the action. The penalties are prescribed by IRCs 7213A and 7431 and set forth at 26 CFR 301.6103(n)-1.

- (2) Additionally, it is incumbent upon the contractor to inform its officers and employees of the penalties for improper disclosure imposed by the Privacy Act of 1974, 5 U.S.C. 552a. Specifically, 5 U.S.C. 552a(i)(1), which is made applicable to contractors by 5 U.S.C. 552a(m)(1), provides that any officer or employee of a contractor, who by virtue of his/her employment or official position, has possession of or access to agency records which contain individually identifiable information, the disclosure of which is prohibited by the Privacy Act or regulations established thereunder, and who knowing that disclosure of the specific material is so prohibited, willfully discloses the material in any manner to any person or agency not entitled to receive it, shall be guilty of a misdemeanor and fined not more than \$5,000.
- (3) Granting a contractor access to FTI must be preceded by certifying that each individual understands the agency's security policy and procedures for safeguarding IRS information. Contractors must maintain their authorization to access FTI through annual recertification. The initial certification and recertification must be documented and placed in the agency's files for review. As part of the certification and at least annually afterwards, contractors must be advised of the provisions of IRCs 7431, 7213 and 7213A (see [Exhibit 4, Sanctions for Unauthorized Disclosure](#) and [Exhibit 5, Civil Damages for Unauthorized Disclosure](#)). The training provided before the initial certification and annually thereafter must also cover the incident response policy and procedure for reporting unauthorized disclosures and data breaches. (See [Section 1.8, Reporting Improper Inspections or Disclosures](#)) For both the initial certification and the annual certification, the contractor must sign, either with ink or electronic signature, a confidentiality statement certifying their understanding of the security requirements.

III. DATA INCIDENT RESPONSE

The contractor will:

- (1) Cooperate with and exchange information with agency officials, as determined necessary by the agency, in order to effectively report and manage a suspected or confirmed breach.
- (2) Properly encrypt FTI in accordance with Publication 1075 and other applicable policies and to comply with any agency-specific policies for protecting FTI.
- (3) Complete regular training on how to identify and report a breach;
- (4) Report a suspected or confirmed breach in any medium or form, including paper, oral and electronic, as soon as possible and without unreasonable delay, consistent with the agency's incident management policy;
- (5) Maintain capabilities to determine what FTI was or could have been accessed and by whom, construct a timeline of user activity, determine methods and techniques used to access FTI and identify the initial attack vector; Allow for an inspection, investigation, forensic analysis and any other action necessary to ensure compliance with Publication 1075, the agency's breach response plan and to assist with responding to a breach; Identify roles and responsibilities, in accordance with Publication 1075 and the

agency's breach response plan; and, explain that a report of a breach shall not, by itself, be interpreted as evidence that the contractor or its subcontractor failed to provide adequate safeguards for FTI.

IV. INSPECTION

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

Exhibit 7b Safeguarding Contract Language for Technology Services

I. PERFORMANCE

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

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

(Include any additional safeguards that may be appropriate.)

II. CRIMINAL/CIVIL SANCTIONS

- (1) Each officer or employee of any person to whom returns or return information is or may be disclosed will be notified in writing by such person that returns or return information disclosed to such officer or employee can be used only for a purpose and to the extent authorized herein, and that further disclosure of any such returns or return information for a purpose or to an extent unauthorized herein constitutes a felony punishable upon conviction by a fine of as much as \$5,000 or imprisonment for as long as 5 years, or both, together with the costs of prosecution. Such person shall also notify each such officer and employee that any such unauthorized further disclosure of returns or return information may also result in an award of civil damages against the officer or employee in an amount not less than \$1,000 with respect to each instance of unauthorized disclosure. These penalties are prescribed by IRCs 7213 and 7431 and set forth at 26 CFR 301.6103(n)-1.
- (2) Each officer or employee of any person to whom returns or return information is or may be disclosed shall be notified in writing by such person that any return or return information made available in any format shall be used only for the purpose of carrying out the provisions of this contract. Information contained in such material shall be treated as confidential and shall not be divulged or made known in any manner to any person except as may be necessary in the performance of the contract. Inspection by or disclosure to anyone without an official need-to-know constitutes a criminal misdemeanor punishable upon conviction by a fine of as much as \$1,000 or imprisonment for as long as 1 year, or both, together with the costs of prosecution. Such person shall also notify each such officer and employee that any such unauthorized inspection or disclosure of returns or return information may also result in an award of civil damages against the officer or employee [United States for Federal employees] in an amount equal to the sum of the greater of \$1,000 for each act of unauthorized inspection or disclosure with respect to which such defendant is found liable or the sum of the actual damages sustained by the plaintiff as a result of such unauthorized inspection or disclosure plus in the case of a willful inspection or disclosure which is the result of gross negligence, punitive damages, plus the costs of the action. These penalties are prescribed by IRC 7213A and 7431 and set forth at 26 CFR 301.6103(n)-1.
- (3) Additionally, it is incumbent upon the contractor to inform its officers and employees of the penalties for improper disclosure imposed by the Privacy Act of 1974, 5 U.S.C. 552a. Specifically, 5 U.S.C. 552a(i)(1), which is made applicable to contractors by 5 U.S.C. 552a(m)(1), provides that any officer or employee of a contractor, who by virtue of his/her employment or official position, has possession of or access to agency records which contain individually identifiable information, the disclosure of which is prohibited by the Privacy Act or regulations established thereunder, and who knowing that disclosure of the specific material is prohibited, willfully discloses the material in any manner to any person or agency not entitled to receive it, shall be guilty of a misdemeanor and fined not more than \$5,000.
- (4) Granting a contractor access to FTI must be preceded by certifying that each individual understands the agency's security policy and procedures for safeguarding IRS information. Contractors must maintain their authorization to access FTI through annual recertification. The initial certification and recertification must be documented and placed in the agency's files for review. As part of the certification and at least annually afterwards, contractors must be advised of the provisions of IRCs 7431, 7213 and 7213A (see [Exhibit 4, Sanctions for Unauthorized Disclosure](#) and [Exhibit 5, Civil Damages for Unauthorized Disclosure](#)). The training provided before the initial certification and annually thereafter must also cover the incident response policy and procedure for reporting unauthorized disclosures and data breaches. (See [Section 1.8, Reporting Improper Inspections or Disclosures](#)) For both the initial certification and the annual certification, the contractor must sign, either with ink or electronic signature, a confidentiality statement certifying their understanding of the security requirements.

III. DATA INCIDENT RESPONSE

The contractor will:

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

IV. INSPECTION

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

ATTACHMENT B

STATE OF OKLAHOMA GENERAL TERMS

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

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

1 Scope and Contract Renewal

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

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

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

2 Contract Effectiveness and Order of Priority

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

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

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

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

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

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

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

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

4 **Definitions**

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

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

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

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

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

5 Pricing

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

6 Ordering, Inspection, and Acceptance

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

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

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

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

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

7 Invoices and Payment

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

The following terms additionally apply:

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

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

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

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

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

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

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

9 Compliance with Applicable Laws

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

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

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

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

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

10 Audits and Records Clause

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

11 Confidentiality

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

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

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

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

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

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

12 Conflict of Interest

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

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

13 Assignment and Permitted Subcontractors

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

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

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

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

14 Background Checks and Criminal History Investigations

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

15 Patents and Copyrights

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

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

16 Indemnification

16.1 Acts or Omissions

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

16.2 Infringement

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

16.3 Notice and Cooperation

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

16.4 Coordination of Defense

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

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

16.5 Limitation of Liability

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

17 Termination for Funding Insufficiency

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

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

18 Termination for Cause

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

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

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

19 Termination for Convenience

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

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

20 Suspension of Supplier

20.1 Supplier may be subject to Suspension without advance notice and may additionally be suspended from activities under the Contract if Supplier fails to comply with confidentiality, privacy, security, environmental or safety requirements applicable to Supplier's performance or obligations under the Contract.

20.2 Upon receipt of a notice pursuant to this section, Supplier shall immediately comply with the notice terms and take all necessary steps to minimize the incurrence of costs allocable to the work affected by the notice. If a purchase order or other payment mechanism has been issued and a product or service has been accepted as satisfactory prior to receipt of notice by Supplier, the Suspension does not relieve an obligation to pay for the product or service but there shall not be any liability for further payments ordinarily due under the Contract during a period of Suspension or suspended activity or for any damages or other amounts caused by or associated with such Suspension or suspended activity. A right exercised under this section shall not be an exclusive remedy but shall be in addition to any other rights and remedies provided for by law. Any amount paid to Supplier in the form of prepaid fees attributable to a period of Suspension or suspended activity shall be refunded.

20.3 Such Suspension may be removed, or suspended activity may resume, at the earlier of such time as a formal notice is issued that authorizes the resumption of performance under the Contract or at such time as a purchase order or other appropriate encumbrance document is issued. This subsection is not intended to operate as an affirmative statement that such resumption will occur.

21 Certification Regarding Debarment, Suspension, and Other Responsibility Matters

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

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

22 Certification Regarding State Employees Prohibition From Fulfilling Services

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

23 Force Majeure

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

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

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

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

24 Security of Property and Personnel

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

25 Notices

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

If sent to the State:

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

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

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

26 Miscellaneous

26.1 Choice of Law and Venue

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

26.2 No Guarantee of Products or Services Required

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

26.3 Employment Relationship

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

26.4 Transition Services

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

26.5 Publicity

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

26.6 Open Records Act

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

26.7 Failure to Enforce

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

26.8 Mutual Responsibilities

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

26.9 Invalid Term or Condition

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

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

26.10 Severability

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

26.11 Section Headings

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

26.12 Sovereign Immunity

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

26.13 Survival

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

26.14 Entire Agreement

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

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

26.15 Gratuities

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

26.16 Import/Export Controls

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

ATTACHMENT C

OKLAHOMA STATEWIDE CONTRACT TERMS

1. Statewide Contract Type

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

2. Orders and Addendums

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

3. Termination for Funding Insufficiency

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

4. Termination for Cause

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

5. Termination for Convenience

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

6. Contract Management Fee and Usage Report

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

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

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

6.3 All Contract Usage Reports shall meet the following criteria:

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

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

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

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

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

ATTACHMENT D

STATE OF OKLAHOMA INFORMATION TECHNOLOGY TERMS

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

1 Definitions

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

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

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

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

2 Termination of Maintenance and Support Services

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

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

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

3 Compliance and Electronic and Information Technology Accessibility

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

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

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

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

5 Offshore Services

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

6 Compliance with Technology Policies

- 6.1** The Supplier agrees to adhere to the State of Oklahoma "Information Security Policy, Procedures, and Guidelines" available at https://omes.ok.gov/s/g/files/gmc316/f/InfoSecPPG_0.pdf.

Supplier's employees and subcontractors shall adhere to the applicable State IT Standard Methodologies and Templates including but not limited to Project Management, Business Analysis, System Analysis, Enterprise and IT Architecture, Quality, Application and Security Methodologies and Templates as set forth at <http://eclipse.omes.ok.gov>.

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

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

7 Emerging Technologies

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

8 Extension Right

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

9 Source Code Escrow

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

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

10 Commercial Off The Shelf Software

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

11 Ownership Rights

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

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

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

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

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

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

12 Intellectual Property Ownership

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

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

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

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

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

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

13 Hosting Services

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

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

14 Change Management

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

15 Service Level Deficiency

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

16 Notices

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

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

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

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

Appendix 1 to State of Oklahoma Information Technology Terms

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

A. Customer Data

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

B. Data Security

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

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

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

C. Security Assessment

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

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

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

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

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

d. Document all Security Incidents and their outcomes.

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

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

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

F. **Notices**

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

Chief Information Security Officer

3115 N. Lincoln Blvd

Oklahoma City, OK 73105

and

servicedesk@omes.ok.gov.

G. Supplier Representations and Warranties

Supplier represents and warrants the following:

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

H. Indemnity

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

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

I. Termination, Expiration and Suspension of Service

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

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

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

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

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

c. a combination of the two immediately preceding options.

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

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

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

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

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

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

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

Appendix 2 to State of Oklahoma Information Technology Terms

INTRODUCTION

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

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

CJIS SECURITY POLICY REQUIREMENTS GENERALLY

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

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

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

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

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

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

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

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

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

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

Section Nine: Pricing (RFP Sections 8.1.F and 8.2.H)**Pricing Overview**

Deloitte is pleased to present our price proposal as part of our overall response to the Oklahoma Office of Management & Enterprise Services (“OMES”) request for proposal for professional services, eDiscovery as a Service Provider (Solicitation No. 0900000467) (the “RFP”) to provide electronic discovery services to the OMES. Such services will include collection, processing, hosting, analysis, review and production of litigation case documents including electronically stored information (ESI), paper documents and other media.

The information in this section details Deloitte’s pricing within the price proposal format contained in the RFP. In accordance with instructions in the RFP, Deloitte’s price proposal consists of the completed price proposal format. This section presents Deloitte’s fixed unit costs to provide managed services for each of the services specified in the RFP.

Proposed Pricing**Pricing – Fixed Unit Costs**

Table 9-1 presents the pricing for Base Year services, in the format as provided in the Exhibit Price schedule made part of the RFP. For each of the line items proposed on an hourly basis Deloitte proposes an escalator of 3% over the Base Year rate for the each of the Option Years, if exercised.

Table 9-1: State of Oklahoma – eDiscovery as a Service Pricing – Fixed Unit Costs

Subscription Based Hosting	Services Included	Per Month/Per Year	Cost
Platform Hosting User Access	See Section 5	User/Month	\$29.38
Additional Storage	Description	Unit of Measure	Cost
Platform Hosting Storage - 0 to 500 GB	See Section 5	GB/Month	\$6.50
Platform Hosting Storage - 501 to 1,000 GB		GB/Month	\$5.00
Platform Hosting Storage - > 1,000 GB		GB/Month	\$3.50
Near-line Storage		GB/Month	\$2.00
A La Carte Services	Description	Unit of Measure	Cost
OCR	See Section 5	Image	\$0.01
On-site Forensic Imaging		Hourly	\$244.23
On-site non-Forensic Collection		Hourly	\$182.58
Remote Collection		Hourly	\$125.56
Loading		GB	\$12.00
Full Processing		GB	\$38.33
Native Processing		GB	\$18.67
Production		Each	\$245.36
Analytics		Hourly	\$132.29
Document Review		Hourly	\$118.00

Training	Description	Unit of Measure	Cost
eDiscovery Basic Training Sessions	See Section 5	Training Session	\$2,080.00
eDiscovery Advanced Training		Hourly	\$173.33
Professional Services	Description	Unit of Measure	Cost
Managing Director	See Section 5	Hourly	\$310.00
Senior Manager		Hourly	\$280.00
Senior Solution Manager		Hourly	\$175.00
Manager		Hourly	\$250.00
Solution Manager		Hourly	\$155.00
Senior Consultant		Hourly	\$220.00
Senior Solution Specialist		Hourly	\$135.00
Consultant		Hourly	\$180.00
Analyst		Hourly	\$145.00

Invoicing

Deloitte proposes to invoice OMES on a monthly basis utilizing standard billing formats that conform to Deloitte's established billing policies and procedures and align with the services contract to be executed between Deloitte and the OMES. Invoices will be based on actual usage and services rendered.

Travel and Other Direct Costs (ODCs)

Deloitte has not included any travel or ODCs in our proposed price. Should the need arise for travel and other direct costs during the execution of this contract, Deloitte will obtain authorization from the appropriate representative of OMES prior to incurring or invoicing of these costs.

Assumptions and Clarifications

1. Assumptions and Clarifications. Our proposal is based upon the following assumptions and clarifications:

Our pricing methodology is tailored to meet the needs of each client. As a result, the fees we propose may vary based a variety of factors. We have prepared our price proposal based upon a careful consideration of your requirements and we believe that our proposal is highly competitive. To the extent there are additional requirements we have not priced, Deloitte would be happy to discuss pricing of additional a la carte services based on OMES needs.

Service Category	Description of Service	Assumptions
Subscription Based Hosting	Platform Hosting User Access	License fee per named OMES or participating State Agency user, within Relativity charged on a monthly basis.
Additional Storage	Platform Hosting Storage	Web-based platform monthly hosting services. Cost is based on the cumulative data hosted on behalf of OMES and will be charged based on unit rates for the respective volume tier(s) shown in Section Nine.
	Near-line Archive	Web-based storage of archived data. Data accessible within 48 hours of client request. Cost is based on the cumulative data hosted on behalf of OMES and will be charged based on the unit rate shown in Section Nine.
A La Carte Services	Optical Character Recognition (OCR)	Includes one pass through OCR engine. Does not include any manual clean-up.

	On-site Forensic Imaging	Forensically sound collection of data at client and/or other sites.
	On-site Non-Forensic Collection	Collection of data at client and/or other sites but does not include forensic collection measures.
	Remote Collection	Deloitte will assist OMES in collecting information without being on-site.
	Loading	Ingestion of pre-processed data to review platform.
	Full Processing	Includes standard processing and indexing (staging, unpacking, virus-scan, file-level inventory and loading). Inventory and De-duplication based on MD5Hash determination. Creation of TIFF images, extraction of text and metadata. Includes comparison to media inventory to verify all files processed. Price is based on unpacked volume processed.
A La Carte Services	Native Processing	Ingestion of native files without full standard processing and indexing. De-duplication is not included. No metadata will be extracted beyond basic file attributes. Includes comparison to media inventory to verify all files processed. Price is based on unpacked volume processed.
	Production	Running production, including QA/QC. Includes the “machine time” to run a production and create a native production export.
	Analytics	Includes Near Duplication, Email Threading, Predictive Coding, Predictive Redactions and other analytics. Includes time spent in defining specifications, selection of methodology and implementation of analytics within the appropriate Deloitte technology. Includes QA/QC measures and verification of results. Output within the hosted platform.
	Document Review	Review services are provided for non-technical and non-litigation review support across a variety of requirements such as identification of potential PHI/PII information, Multi-Language identification, identification of specific field values and similar non-technical and non-litigation oriented reviews. Review services are typically conducted using online tools.
Training	eDiscovery Basic Training	Includes the time to provide basic training on how to access the hosted environment. Does not include specific training on using the various capabilities of the Relativity platform.
	eDiscovery Advanced Training	Training to include specific capabilities and functionality of the Relativity platform as requested by OMES.

Professional Services	Hourly Professional Services	Professional services for services not covered above, delivered on an hourly basis.

**Attachment E, Ex-1 SOW Template to
STATE OF OKLAHOMA CONTRACT WITH Deloitte
RESULTING FROM SOLICITATION NO. 09000000467 and SW1044**

The **DRAFT Statement of Work Template** is hereby amended as set forth below and supersedes all prior documents submitted by **Deloitte** or discussed by the parties. The parties agree to use this **DRAFT Statement of Work Template** or a document substantially similar in the form of this **DRAFT Statement of Work Template**.

[Remainder of Page Intentionally Left Blank]

OMES eDiscovery as a Service – Draft SOW

DRAFT Statement of Work: State of Oklahoma OMES eDiscovery as a Service

1.0 BACKGROUND

The State of Oklahoma’s Office of Management and Enterprise Services (OMES) is seeking statewide support of eDiscovery services including collection, processing, hosting, analysis, review and production of litigation case documents including ESI, paper documents and other media, for various matters including, but not limited to litigation and Freedom of Information Act (FOIA) requests.

2.0 PERFORMANCE WORK STATEMENT (PWS)

OMES has a requirement for continued managed discovery services to respond to numerous ongoing/pending (or imminent or reasonably anticipated), requests for documents related to litigation and FOIA requests. Over time, the level and type of support may vary whether due to evolving nature of information requests, technology innovation, or the emergence of mission- critical issues. As specific services and types and sizes of matters are undetermined at this time, OMES seeks a contract vehicle that allows the State flexibility to scale over time and to respond to support needs as they arise.

Task 1. Full-Service Discovery Support for a Matter(s)

For purposes of this PWS, full-service discovery support will be based on a “matter” as a unit. A “matter” for these purposes is discovery work relating to a case or inquiry surrounding a defined topic or issue. Data processing and data hosting will be based on gigabytes or terabytes. The level of effort involved, and the volume of data are considerations when determining a matter.

Sections 1.1 – 1.8 below identify the types of services potentially needed for an initial 12-month period of support for matters. Beyond the initial 12-month period, OMES seeks up to four optional 12-month periods of performance for managed discovery services.

1.1 Document/Data Collection: The support for each request may include some or all of the following: onsite or remote collection of data from OMES sources or systems; developing a list of potential document custodians and data sources; conducting a fully documented interview process with selected custodians to develop a comprehensive list of actual information sources; assisting OMES staff with collections from such sources; developing detailed instructions for custodians to search and collect data in a forensically sound manner that preserves native format and metadata; and developing and implementing a chain-of-custody form that accompanies the data and which describes the data collected.

1.2 Data Processing: During the data processing phase services may include: ingesting electronically stored information (ESI) to industry leading processing platforms to provide data transformation and extraction support. As necessary, hard copy documents may also need to be imaged and Optical Character Recognition (OCR) applied to make the documents text searchable. ESI processing may include, but is not limited to, extraction of metadata, conversion of image only files, as well as the identification of exact duplicates.

1.3 Externally Hosted Discovery Platform (or “Data Hosting”): Document collections shall be hosted on a FedRAMP secure online repository that allows for easy access and collaboration by authorized personnel from anywhere and at any time. Such hosting would allow attorneys and other authorized persons to monitor the progress of the review effort and offer comments, further guidance, and an enhanced level of participation. Hosting platforms will include advanced analytics capabilities and shall integrate with other solutions that augment the discovery process (e.g., text analytics, audio/video analytics; advanced redaction support).

1.4 Assisted Document Analysis and Review: OMES may require access to experienced internal and external specialists to drive the analytic analysis. Working side-by-side with OMES and other State Agency stakeholders, these Analysts will drive tasking such as: identification of extraneous, non-relevant, non-responsive, duplicative, or nearly duplicative material; identification of missing documents or gaps in information (custodians, types of documents, date ranges, etc.); using tools and techniques to search and categorize the data/documents with a goal of understanding the document universe and building an efficient review plan to be used, including use of automated search tools and processes in conjunction with specific search criteria to reduce the eventual population needing review. Any and all review support would be conducted under the guidance of OMES or the designated State agency.

1.5 Production: Based upon specification of the requesting Agency, productions shall be timely. They may be required to be in: native file format, with extracted text and metadata, image format, OCR text format, load file format for other systems, indexed with hyperlinks to the file/image, and/or entered information into shared repositories.

1.6 Training and User Support: Training may be necessary for differing levels of end users (e.g., basic reviewer, advanced analytic user; admin/technical). Training resources and formats may include live (in-person and remote), stored on demand and tips and FAQs. In addition, Helpdesk availability and technical support for the hosted application are required.

1.7 Consultation Project Management and Program Management: Consulting project management services may be required to optimize OMES’ or the State agency’s procedures for utilization of tools and related processes, from collection through production phases. In addition to process support, overall Program reporting, case tracking and change management support services may be necessary.

1.8 Data Migration: If necessary, facilitate transfer of data from workspaces using commercially reasonable efforts and secure methods. Migration requirements may include, but are not limited to, creating a data migration plan, evaluating tools necessary to ensure compatibility of data and environments, addressing data cleanup, assessing post-transfer audit protocols, and educating users on changes in data.

Deliverables:

Will be a function of the services required for any matters.

Task 2. Consulting in Support of OGC Managed Discovery Services (Optional)

OMES or another State agency may seek advice and support regarding managed discovery services. Specific subject areas may include, but are not limited to, greater coordination between agencies regarding discovery requests and responses, the development of guidelines and processes to increase efficiency in information identification, preservation and collection, or assessment of existing processes to determine areas available for process improvement.

Deliverables:

Will be a function of the services required.

Rules of Behavior and Computer User Agreement



GPS Technology Center (GPSTC)

Deloitte

Version 7.0

January 14, 2020



Table of Contents

Rules of Behavior	4
Overview	4
Applicability	4
Personnel Screening.....	4
Acceptable Use	5
Laptop Security.....	5
Media Protection.....	5
Passwords, Passphrases and Credentials	5
Information Handling	7
System Privileges/Access Control	7
Continuity of Operations/Restoration of Service.....	8
Printing	8
Social Media	8
Non-Compliance	9
Incident Reporting	9
Deloitte GPS Computer User Agreement (CUA).....	10

Document Revision History

Date	Description	Version	Author
05/02/2012	Document Publication	1.0	FedRAMP Office
05/26/2016	Annual Review	2.0	Andrew Martin
05/25/2017	Annual Review, minor edits	3.0	Maria Keady
11/09/2017	Minor edits	4.0	Brook Peed
05/24/2018	Updated Password Length	5.0	Brook Peed
01/25/2019	Updated Password Requirements	6.0	Brook Peed
09/27/2019	Updated Password Length	6.1	Brook Peed
01/14/2020	Annual Review and Update	7.0	Misha Lott

ABOUT THIS DOCUMENT

This document has been developed to provide guidance on how to participate in and understand the FedRAMP program.

Who should use this document?

This document is intended to be used by Cloud Service Providers (CSPs), Third Party Assessor Organizations (3PAOs), government contractors working on FedRAMP projects, government employees working on FedRAMP projects, and any outside organizations that want to make use of the FedRAMP Contingency Planning process.

How to contact us

If you have questions about FedRAMP or something in this document, please write to:

info@fedramp.gov

For more information about the FedRAMP project, please see the website at:

<http://www.fedramp.gov>.

Rules of Behavior

Overview

The System Rules of Behavior (RoB) and Computer Use Agreement (CUA) are part of a comprehensive program to provide information security for the Deloitte GPS Technology Center (GPSTC) and Deloitte GPS SharePoint (hereafter referred to as SharePoint), collectively referred to as “the system”, in accordance with federal laws, regulations, mandates and contractual requirements. The system is owned and operated by the Deloitte US Firms, under the purview of Deloitte GPS Cyber Security Team, on behalf of the Deloitte GPS Practice; however, the system is used to create, collect, store, process, display and transmit information that is the property of the U.S. Government and is therefore subject to federal security requirements as defined by law, regulation, and/or contractual agreement.

These requirements establish standards of acceptable behavior, hold users accountable for their actions, and assign responsibilities for information security in recognition of the fact that knowledgeable users are the foundation of a successful security program. Users are required to be aware of their individual responsibilities that are associated with the security of U.S. Government information, and must understand that the security of their computer and the data it contains is an essential part of their job.

Applicability

These rules extend to all non-Deloitte persons who have been granted access to the system, including contractors, and other third parties. All users of the system are required to receive initial system security awareness training (by reading and understanding this document) and complete and sign a CUA prior to receiving access. The Deloitte GPS Cyber Security Team collects and retains all CUAs and serves as the authoritative records source for CUA information. All users of the system are also required to receive annual refresher security awareness training in order to retain access.

Most U.S Government entities (commonly referred to as “Federal Agencies” or just “Agencies”) have, within the scope of law and regulation, created agency-specific security policies and regulations. These issuances usually refine and amplify applicable laws and regulations, and tailor them to the specific needs and mission of the agency, usually resulting in the creation of additional security requirements. When preparing contracts into which Deloitte will enter with the U.S Government, the agency customarily invokes their specific issuances, thus binding Deloitte to comply with the requirements included in them. In many cases, these invocations are by citation to the issuance and the contract will not specifically itemize every security requirement being levied upon Deloitte.

Personnel Screening

Initial:

Users that access the GPSTC and SharePoint are required to be subjected to screening against specific personnel security requirements prior to being granted access to the system or data therein. The personnel security requirements for access to the system and U.S. Government data vary according to agency, job function, position sensitivity, contract, and level of risk as defined by the agency. The agency is the “data owner of record” for the U.S. Government’s data, and personnel security is applied to users who will obtain access to the data owner’s information as mandated by the agency.

Acceptable Use

Initial:

- Users are required to refrain from using information system resources, including servers, applications, and networks, for personal use. Personal use is not permitted.
- Users may not use personally owned equipment or software to create, collect, store, process, display or transmit U.S. Government information.
- Users may not attempt to modify (including changing, adding or deleting) any software on the system. All requests for changes to system components are required to be made to the Deloitte GPS Cyber Security Team or Client Solutions-Federal and must be approved by the Change Control Board (CCB) and the Deloitte GPS Cyber Security Team prior to implementation.
- Users are required to comply with all software copyrights and license requirements.
- Users may not make unauthorized copies of software.

Laptop Security

Initial:

- Users are required to secure all laptop computers containing sensitive government data and other mobile computing devices when unattended in a manner consistent with security standards established by the data owner of record. However, at a minimum before leaving their laptops unattended users will exit the GPSTC website, close the web browser, and lock their screens by removing their common access cards (CACs) from their machines. If practicable, users should also physically secure unattended laptops using a locking cable or a locked cabinet, desk, drawer, or door.
- When working away from their normal duty locations, users should power off their laptops that contain sensitive government data when unattended for an extended period of time, (i.e. in excess of four hours), and when transporting the laptop between locations.

Media Protection

Initial:

- Users are required to ensure that all media containing U.S. Government information, including backup media and removable media such as external hard drives and compact disks, are secured in accordance with rules established by the data owner concerning encryption, password protection, physical controls (e.g., a locked office, room, desk, bookcase, file cabinet, or other storage prohibiting access by unauthorized persons), and other information security measures.

Passwords, Passphrases and Credentials

Initial:

- Users are required to comply with the password management rules defined below for their GPSTC user accounts, including situations in which “passphrases” are used in lieu of traditional passwords.
- These rules apply to users whether or not the system is automatically enforcing them.
- Users are required to change passwords at least once every 45 days.

- Users may not change their password more than once a day.
- Users may not reuse their previous 24 passwords.
- Users are required to use “strong” (complex and hard-to-guess) passwords. Strong passwords are defined as meeting the following criteria:
 - Must be at least 15 characters in length;
 - Must contain at least one instance of a character selected from at least three of these four categories:
 - An Uppercase alphabetic character, (e.g. A, B, C);
 - A Lowercase alphabetic character, (e.g. a, b, c);
 - A Numeric character, (e.g. 1, 2, 3);
 - A Special character, (e.g. !, #, \$, %);
 - Must not contain the username;
 - Must not be composed solely of a single dictionary word with or without (i) numbers or special characters at the beginning or end or (ii) letter, numbers or character exchanges;
 - Must not contain any proper nouns, or the name of any person, pet, child, or fictional character, either forwards or backwards;
 - Must not contain any employee number, social security number, birth date, phone number, or any information that is guessable based on personal knowledge of the account owner;
 - Must not contain any simple patterns of letters or numbers, (e.g. qwerty, xyz123); and
 - Must not be a variation of the prior password (e.g. P@ssw0rd1!, P@ssword2!) at a minimum 8 characters are required to be unique from previous password used.
- Users may never provide their password to anyone, including their superiors or system administrators. System administrators will never ask for a user’s password.
- Users may not record their password, either electronically, or in writing.
- Users are required to IMMEDIATELY contact the Deloitte Call Center (1 800 Deloitte) and their Deloitte contact, in the event that their password is compromised, or if there is a suspicion that their password might have been compromised.
- Users are required to immediately change their password in the event that their password is compromised, or if there is a suspicion that their password might have been compromised.
- Users may not allow any other person to access the system by employing the user's identity (for example, logging on and then turning the computer over to someone else for them to use).

- Users are required to secure all authentication materials, such as certificates, tokens, Smart Cards, Personal Identity Verification (PIV) cards, Common Access Card (CAC), upon their person or in a locked container when not in use.
- Users may not employ “hard-coded” or scripted passwords in any automated mechanisms, such as scripts or programs that authenticate to another computer or process.

Information Handling

Initial:



THE SYSTEM IS NOT APPROVED FOR CLASSIFIED INFORMATION. UNDER NO CIRCUMSTANCES ARE USERS TO CREATE, COLLECT, STORE, PROCESS, DISPLAY, OR TRANSMIT CLASSIFIED INFORMATION USING ANY SYSTEM RESOURCES. UNDER NO CIRCUMSTANCES ARE DOCUMENTS, FILES OR E-MAIL MESSAGES CONTAINING CLASSIFIED U.S. GOVERNMENT INFORMATION TO BE MOVED INTO THE SYSTEM



IF A USER RECEIVES CLASSIFIED MATERIAL, OR HAS REASON TO BELIEVE THAT CLASSIFIED MATERIAL HAS ENTERED THE SYSTEM, THEY ARE REQUIRED TO IMMEDIATELY CONTACT THE DELOITTE CALL CENTER (1800DELOITTE) AND THEIR DELOITTE CONTACT AS WELL AS AGENCY SECURITY OFFICIALS.



- Users are required to scan all files for malicious content prior to transferring them to or from the system.
- Users are required to IMMEDIATELY contact the Deloitte Call Center (1-800-Deloitte) and their Deloitte contact as well as agency security officials when any malware is detected, either inbound to, or outbound from, the system.
- Users are required to dispose of durable media (CD/DVD, USB drive, etc.) that has been used to store or transmit U.S. Government information in a manner consistent with the requirements of the data owner of record. Users should purge media that is not stored in a secure location (e.g., a locked office, room, desk, bookcase, file cabinet, or other storage prohibiting access by unauthorized persons).
- Users are required to apply cryptographic protections required by the data owner of record to U.S. Government information being copied to removable media.
- Users are required to follow all information categorization guidance.

System Privileges/Access Control

Initial:

- Users are granted access to the DFed/GPSTC and U.S. Government information only in situations where they meet agency personnel security eligibility requirements and they require a need to such access in order to perform specific work in support of the U.S Government client.

- Users will be granted the access to the minimum amount of privilege, access to resources, and access to information, needed to perform their assigned job, and no more.
- Users may not attempt to escalate their privilege, their level of access to DFed/GPSTC resources, or the scope of the information to which they have access, beyond that which has been authorized.
- Users are required to notify the Project Manager upon completion of their engagement, when they will be on an extended leave of absence, or when they are terminating their employment.
- Project Managers are required to plan the revocation of access to the system upon notification that an associate is leaving the program. Project Managers are required to immediately revoke access to the system in the event of an unexpected departure of an associate.
- Users may not disable, bypass or otherwise seek to circumvent any security controls, including malicious code protection, screensaver, and session deactivation.

Continuity of Operations/Restoration of Service

Initial:

- In the case of an interruption in service, a communication will be sent out to users explaining the situation and the approximate time it may take to restore services.

Printing

Initial:

- Any printed documents containing sensitive government information will be secured in a manner consistent with the requirements of the data owner of record.

Social Media

Initial:

- Users are restricted from using social media in an official capacity except as part of an authorized media initiative or in the conduct of official business by approved Deloitte communicators.
- Users are prohibited from posting any information that may be construed as an official communication by Deloitte.
- Users are prohibited from uploading or otherwise disclosing any non-public data or information that is considered sensitive in part or in whole. This includes any information that may reveal potentially sensitive information through inference or association (Example: revealing a specific client or location of work being performed).
- Users are prohibited from downloading, copying, or installing unauthorized applications through social media sites.
- Users are prohibited from correspondence for the purposes of personal gain or the solicitation of individuals.

Non-Compliance

Initial:

Users who do not comply with the System Rules of Behavior are subject to penalties that can be imposed under U.S. federal regulations, including suspension of system privileges, and criminal or civil prosecution, with sanctions commensurate with the assessed level of the infraction. Any failure to comply with these rules will be considered a security incident, to be investigated by and reported to the Deloitte Call Center (1 800 Deloitte) and their Deloitte contact, the U.S. CERT, as necessary, and other federal agencies as required. Security incidents involving persons with security clearances may be reported to Defense Security Service or the adjudicating agency and may result in the suspension or revocation of that individual's security clearance, and may impair the future ability of that individual to obtain and hold a security clearance.

Incident Reporting

Initial:

Users are responsible for IMMEDIATELY reporting any actual or suspected security incidents to the Deloitte Call Center (1 800 Deloitte) and their Deloitte contact. Incidents must be reported immediately upon discovery/detection, regardless of the manner in which the incident may have occurred.

NIST defines five types of incidents, but these are not published here with the intent of being an exhaustive itemization of every possible type of incident. **When in doubt, report the situation!** It is better to report something that ultimately resolves as being a “non-issue” than it is to fail to report something. This is particularly applicable when a person observes “something odd” and assumes that someone else will report the issue.

Here are the five types of incidents that are defined in NIST Special Publication 800-61, “Computer Security Incident Handling Guide”

- **Denial of Service (DoS)**— Defined as an attack that prevents or impairs the authorized use of networks, systems, or applications by exhausting resources
- **Malicious Code**— Defined as a virus, worm, Trojan horse, or other code-based malicious entity that infects a host
- **Unauthorized Access**— Defined as a scenario when a person gains logical or physical access without permission to a network, system, application, data, or other resource
- **Inappropriate Usage**— Defined as a scenario when a person violates acceptable computing use policies
- **Multiple Component**— Defined as a single incident that encompasses two or more types of incidents; for example, a malicious code infection leads to unauthorized access to a host, which is then used to gain unauthorized access to additional hosts.

Deloitte GPS Computer User Agreement (CUA)

By signing this agreement, I acknowledge and consent to the following conditions:

CONDITION	INITIAL
I have read the System Rules of Behavior for the Deloitte GPS Technology Center and Deloitte GPS SharePoint, I understand them, and I will exercise my duties as conveyed therein.	<hr/>
Failure to comply with the aforementioned rules could result in disciplinary action, including, but not limited to, the following: <ul style="list-style-type: none">• A written and/or verbal report to your manager• Denial of System Access• Criminal or Civil Prosecution in accordance with U.S. Federal laws• Reporting to U.S. Government entities, including agencies managing security clearances	
I understand the system implements specific security controls to protect U.S. Government information, interests as well as Deloitte data. The system is intended solely for the purposes of supporting GPS Practice engagements, and is not intended for commercial or personal use.	
I do not have any right to, or expectation of, privacy while using the system.	
I understand that use of the system is subject to monitoring for the purposes of administrative oversight, law enforcement, criminal investigation, inquiries into suspected misuse, and to ensure the proper performance of applicable security features and procedures.	
I understand that as a part of system monitoring Deloitte may acquire, access, retain, intercept, capture, retrieve, record, read, inspect, analyze, audit, copy, and disclose any information that is created, collected, stored, processed, and transmitted within the system. If monitoring reveals potential misuse of system resources, non-compliance of the System Rules of Behavior, or criminal activity, notification will be reported to the Deloitte Call Center (1-800-Deloitte) and/or law enforcement for investigation.	
I understand that nothing in this agreement shall be interpreted to limit my consent to, or in any way restrict or affect any actions for the purposes of network administration, operation, protection, or defense, or for communications security. This includes all communications and data on the system, regardless of any applicable privilege or confidentiality.	
I understand that I must comply with all password management rules identified in the System Rules of Behavior for the GPS Technology Center.	
I understand that all of the above conditions, as well as the System Rules of Behavior, remain applicable, regardless as to whether a Notice and Consent Banner is displayed upon accessing the system.	



Prior to signing this form, you must thoroughly read and understand the System Rules of Behavior, and ensure that all of



**your questions have been answered to your satisfaction by your
Deloitte representative or the Deloitte GPS Cyber Security
Team.**

Acknowledgement Statement

I acknowledge receipt of, understand my responsibilities, and will comply with the EMS System Rules of Behavior and Computer User Agreement. I understand that these Rules of Behavior establish standards for my actions in recognition of the fact that privileged users are provided unique system access, and that non-compliance to these rules will be enforced through coaching and/or disciplinary actions up to and including termination with respect to the level of infraction or severity of the violation. I further understand that violation of these rules and responsibilities may be prosecutable under local, state, and/or Federal Law.

Full Name (Printed):	
Organization:	
Phone Number:	
Email Address:	
Work Address:	
Service Now Ticket Number:	

Signature

Date

**Attachment F to
STATE OF OKLAHOMA CONTRACT WITH Deloitte
RESULTING FROM SOLICITATION NO. 09000000467**

Negotiated Exceptions and Additional Terms to the Solicitation

The Solicitation is hereby amended to include the terms as set forth below and supersedes all prior terms and Exceptions submitted by **Deloitte** or discussed by the parties.

**Any Requested Exceptions or Additional Terms Not Appearing Below Have Been
Rejected By The State.**

RFP Section	Exception
Attach A, Sol. 09000000467, Exhibit 7a, General Sections, Sec IV	This section is hereby deleted in its entirety and is replaced with the following: “The IRS and the Agency, with reasonable prior 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 right to request Contractor to use of manual and/or automated scanning tools to perform compliance and vulnerability assessments of information technology (IT) assets that access, store, process or transmit FTI. On the basis of such inspection, corrective actions may be required in cases where the contractor is found to be noncompliant with contract safeguards.”
Attach A, Sol. 09000000467, Exhibit 7b, General Sections, Sec IV	This section is hereby deleted in its entirety and is replaced with the following: “The IRS and the Agency, with reasonable prior 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 right to request Contractor to use of manual and/or automated scanning tools to perform compliance and vulnerability assessments of information technology (IT) assets that access, store, process or transmit FTI. On the basis of such inspection, corrective actions may be required in cases where the contractor is found to be noncompliant with contract safeguards.”
Attach B, General Terms, Scope and Contract Renewal (Section 1.2)	This section is hereby deleted in its entirety and is replaced with the following: “At no time during the performance of the Contract shall the Supplier have the authority to obligate 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 in accordance with the acceptance provisions herein.”
Attach B, General Terms, Scope and	This section is hereby deleted in its entirety and is replaced with the following:

RFP Section	Exception
Contract Renewal (Section 1.3)	<p>“If applicable, prior to any Contract renewal, the State shall in good faith 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 reasonably 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. If the parties are unable to reach agreement on such required changes, either party may choose not to renew the Contract. 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.”</p>
Attach B, General Terms, Scope and Contract Renewal (Section 1.4)	<p>This section is hereby deleted in its entirety and is replaced with the following:</p> <p>“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 request subsequent ninety (90) day extensions at the Contract pricing rate which the Supplier may accept or decline at its sole discretion, to facilitate the finalization of related terms and conditions of a new award or as needed for transition to a new Supplier.”</p>
Attach B, General Terms, Modification of Contract Terms and Contract Documents (Section 3.1)	<p>This section is hereby deleted in its entirety and is replaced with the following:</p> <p>“The Contract may only be modified, amended, or expanded by an Addendum. Any change to the Contract, including the addition of work or materials, the revision of payment terms, or the substitution of work or materials made unilaterally by either the State or the Supplier, is not a valid addition or revision to the terms and shall not be binding upon the parties hereto. 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 a party shall not be entitled to any claim under the Contract based on those changes. No oral statement of any person shall modify or otherwise affect the terms, conditions, or specifications stated in the Contract.”</p>
Attach B, General Terms, Definitions (Section 4.18)	<p>This section is hereby deleted in its entirety and is replaced with the following:</p> <p>“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, and in this case means Deloitte Advisory.”</p>
Attach B, General Terms, Definitions	<p>This section is hereby deleted in its entirety and is replaced with the following:</p>

RFP Section	Exception
(Section 4.21, page 6)	<p>“4.21 Work Product(s) means any and all deliverables produced by Supplier for delivery to Customer as a result of the Services pursuant to this Contract, including, as may be applicable, 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 or 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.</p>
<p>Attach B, General Terms, Ordering, Inspection, and Acceptance (Section 6.2, pages 7-8)</p>	<p>Item 6.2 of Section 6 is hereby deleted in its entirety and replaced with the following:</p> <p>“Services will be performed in accordance with industry standard practices and are subject to acceptance by the Customer. Customer shall approve each deliverable that conforms in all material respects to the requirements therefor set forth in the Contract. Notwithstanding any other provision in the Contract, deemed acceptance of a service or associated deliverable shall apply automatically if Customer has not delivered to Supplier a notice that such service or deliverable does not conform with the foregoing within fifteen (15) business days of receipt of a deliverable or upon provision of a service.</p> <p>To the extent expressly agreed upon in the applicable statement of work, Supplier warrants and represents that a 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</p>

RFP Section	Exception
	<p>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. Supplier shall have no obligation to make warranty modifications attributable to: (i) modification of the deliverable other than by Supplier or its subcontractors, or use thereof in a manner not contemplated in the Contract Document; (ii) Customer's failure to use any corrections or modifications made available by Supplier; (iii) a failure to fulfill any Customer obligation under the Contract Document with respect to such deliverable; (iv) Customer's failure to reasonably cooperate with Supplier in the resolution of the defect; (v) the quality or integrity of data from other automated or manual systems not provided or controlled by Supplier or Supplier's contractors or vendors.; (vi) hardware or software that is supplied by a third party to Customer; or (vii) hardware, software, networks or systems not a part of the deliverable which is inadequate to allow proper operation of the deliverable. If any such exception applies, Customer shall compensate Supplier for Supplier's effort in validating and remedying such condition on a time and materials basis.</p> <p>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.</p> <p>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."</p>
<p>Attach B, General Terms, Maintenance of Insurance, Payment of Taxes, and Workers' Compensation (Section 8.1)</p>	<p>The following section is deleted in its entirety and is replaced with the following:</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 or the equivalent rating from Standard & Poors (S&P).</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 and include the State and its agencies as certificate holder on the commercial general</p>

RFP Section	Exception
	<p>liability and auto liability coverage with respect to Supplier's acts or omissions in performance under this Agreement and shall promptly provide proof to the State of any renewals, additions, or adverse changes to such insurance coverage unless replacement coverage meeting the terms and conditions hereunder are obtained without lapse. 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 and advertising injury, bodily injury (including death) and property damage, including coverage for contractual liability pursuant to policy terms and conditions, with a limit of liability of not less than \$1,000,000 per occurrence and \$2,000,000 in the aggregate;</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. 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 claim; the coverage may be included within the Professional Liability coverage form;</p> <p>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 claim for wrongful acts; the coverage may be included within the Professional Liability coverage form; and</p> <p>F. Additional coverage required in writing in connection with a particular Acquisition."</p>
<p>Attach B, General Terms, Compliance with Applicable Laws (Section 9.2)</p>	<p>This section is hereby deleted in its entirety and is replaced with the following:</p> <p>"9.2 The Supplier's employees, agents and subcontractors performing Services hereunder shall adhere to applicable Customer policies to the extent that (i) such policies are applicable to Supplier in performance of the Services, and (ii) such policies do not conflict with the terms of the Contract or Supplier's own policies. Such policies including, but are 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."</p>
<p>Attach B, General Terms, Audits and Records Clause (Section 10.3)</p>	<p>This section is hereby deleted in its entirety and is replaced with the following:</p>

RFP Section	Exception
	<p>“10.3 Pursuant to 74 O.S. §85.41, if applicable, 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.”</p>
<p>Attach B, General Terms, Confidentiality, Section 11.1)</p>	<p>This section is hereby deleted in its entirety and is replaced with the following:</p> <p>“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. If an agency requires Supplier to adhere to policies that are not publicly available, it will apprise Supplier of the same in writing and in advance. 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.”</p>
<p>Attach B, General Terms, Confidentiality, Section 11.3</p>	<p>This section is hereby deleted in its entirety and is replaced with the following:</p> <p>“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 reasonable efforts to assist the Customer in investigating or preventing the reoccurrence of such event in the future. The Supplier shall reasonably 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 reasonable out-of-pocket costs associated with the investigation, response and recovery in connection with any breach of State or citizen data or records caused by Supplier or its representatives 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, subject to the limitation on liability contained herein.”</p>

RFP Section	Exception
Attach B, General Terms, Confidentiality, Section 11.5)	<p>This section is hereby deleted in its entirety and is replaced with the following:</p> <p>“11.4 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 seek 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.”</p>
Attach B, General Terms, Confidentiality (Section 11.6, page 16)	<p>This section is hereby deleted in its entirety and replaced with the following:</p> <p>“11.6 The Supplier shall promptly 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 reasonably cooperate with all efforts to protect the security and confidentiality of such data or records in response to a third party request. Notwithstanding anything to the contrary in this section, the Supplier shall provide the aforementioned Notice to the State Purchasing Director no less than two (2) days upon receipt of any request for data or records in possession of the Supplier.”</p>
Attach B, General Terms, Patents and Copyrights (Section 15, pages 19-20)	<p>This section is hereby removed in its entirety and is replaced with the following:</p> <p>“15. Without exception, the price for the Work Products 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 Work Product 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 Work Product 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 Work Product 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</p>

RFP Section	Exception
	to operate as a waiver of legal or equitable remedies because of acceptance of relief provided by Supplier."
Attach B, General Terms, Indemnification (Section 16.1.B - Acts or Omissions, page 20)	<p>This section is hereby deleted in its entirety and replaced with the following:</p> <p>"16.1(B) To the extent Supplier is found liable for loss, damage, or destruction of any personal 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."</p>
Attach B, General Terms, Indemnification (Section 16.2)	<p>This section is hereby deleted in its entirety and replaced with the following:</p> <p>"16.2 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 the following: (I) alleged infringement of any patent, intellectual property, copyright or other intellectual property right in connection with a product or service provided under the Contract. Supplier's duty under this subsection (I) 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; (II) any bodily injury, death, or damage to real or tangible personal property arising from the negligent acts or omissions of Supplier, its employees or agents, officers or subcontractors in the performance of work under this Contract; (III) disclosure of Confidential Information in violation of Attachment B, Section 11, by Supplier, its employees or agents, officers or subcontractors; (IV) disclosure of PHI by the Supplier, its employees or agents, officers or subcontractors in violation of the Business Associate Agreement which is agreed to in writing by Supplier and an applicable Customer; (V) violations by Supplier, its employees or agents, officers or subcontractors of laws applicable to Supplier in its performance of its obligations hereunder; (VI) recklessness by Supplier, its employees or agents, officers or subcontractors in the performance of work under this Contract; (VII) violations by Supplier, its employees or agents, officers or subcontractors of the Freedom of Information Act or other similar customer law resulting from Supplier's claim that Supplier confidential information is exempt from disclosure under such laws; (VIII) claims brought against a Customer by any personnel of Supplier performing work hereunder for employment benefits or employment compensation, in each case for which Supplier is</p>

RFP Section	Exception
	responsible and has failed to pay, except to the extent that such claim results from acts or omissions of Customer; and (IX) claims brought against Customer by any Supplier subcontractor performing a portion of the work hereunder for payment of its fees to the extent caused by Supplier's failure to pay such fees."
Attach B, General Terms, Indemnification, Section 16.5 A	<p>This section is hereby deleted in its entirety and replaced with the following :</p> <p>"16.5A To the extent permitted by applicable law, and subject to Section 16.5.B, Supplier shall not be liable to the State or Customer for any claims, liabilities, or expenses arising under or related to this Contract for an aggregate amount in excess of four times (4x) fees paid by the State to Supplier for the statement of work, work order, or other similar ordering document in place at the time a claim or cause of action arises. With respect to any claim or cause of action arising under or related to the Contract, neither the State nor any Customer nor Supplier shall be liable to the other 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."</p>
Attach B, General Terms, Indemnification (Section 16.5.B – Limitation of Liability, pages 21-22)	<p>This section is hereby deleted in its entirety and replaced with the following:</p> <p>"16.5(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 arising from any negligent act, omission, or willful misconduct of by Supplier or its employees, agents or subcontractors in the execution or performance of the Contract; indemnity, security or confidentiality obligations under the Contract; or the bad faith, negligence, intentional misconduct or other acts in each case for which applicable law does not allow exemption from liability of Supplier or its employees, agents or subcontractors."</p>
Attach B, General Terms, Termination for Funding Insufficiency (Section 17.2,)	<p>This section is hereby deleted in its entirety and is replaced with the following:</p> <p>"Upon receipt of notice of a termination, Supplier shall immediately comply with the notice terms and take all reasonably 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."</p>
Attach B, General Terms, Termination for Funding	<p>This section is hereby deleted in its entirety and is replaced with the following:</p> <p>"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</p>

RFP Section	Exception
Insufficiency (Section 17.1)	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."
General Terms, Termination for Cause (Section 18.4)	<p>This section is hereby deleted in its entirety and is replaced with the following:</p> <p>"18.4 The Supplier's repeated failure to provide an acceptable product or service in accordance with the acceptance provisions herein; 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 material 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."</p>
General Terms, Suspension of Supplier (Section 20.2)	<p>This section is hereby deleted in its entirety and is replaced with the following:</p> <p>"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 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."</p>
Attach C, Statewide Contract Terms, Termination for Cause (Section 4)	<p>This section is hereby deleted in its entirety and is replaced with the following:</p> <p>"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 cure period upon written notice to Supplier if cure is not possible, such</p>

RFP Section	Exception
	as 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."
Attach B, General Terms, Attach B, General Terms, Certification Regarding Debarment, Suspension, and Other Responsibility Matters (Section 21)	<p>This section is hereby deleted in its entirety and is replaced with the following:</p> <p>"21. 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>
Attach B, General Terms, Security of Property and Personnel (Section 24)	<p>This section is hereby deleted in its entirety and is replaced with the following:</p> <p>"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.</p> <p>"</p>
Attach B, General Terms, Miscellaneous (Section 26.4 Transition Services)	<p>This section is hereby deleted in its entirety and is replaced with the following:</p> <p>"26.4 If transition services are needed at the time of Contract expiration or termination, to the extent not in conflict with law, or independence or professional rules, 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 written request, and reasonably cooperate with any successor supplier and with establishing a mutually agreeable transition plan."</p>
Attach B, General Terms, Miscellaneous (Section 26.5 - Publicity)	<p>This section is hereby deleted in its entirety and is replaced with the following:</p> <p>"26.5 "The utilization of this Contract by Customer is not in any way an endorsement by the Customer of Vendor or the Products and shall not be so construed by Vendor in any advertising or publicity materials. Vendor agrees to submit to the Customer all advertising, sales promotion, and other publicity matters relating to this Contract wherein the Customer's name is</p>

RFP Section	Exception
	mentioned or language used from which the connection of the Customer's name therewith may, in the Customer's judgment, be inferred or implied as an endorsement. Vendor 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 this Contract without obtaining the prior written approval of the Customer."
Attach B, General Terms, Miscellaneous (Section 26.8(D) – Mutual Responsibilities	<p>Item (D) of Section 26.8 is hereby deleted in its entirety and is replaced with the following:</p> <p>"D. The Customer and Supplier shall reasonably cooperate with each other and any Supplier to which the provision of a product and/or service under the Contract may be transitioned after termination or expiration of the Contract to the extent such transition services are agreed to under the Contract."</p>
<p>Information Technology Terms (Introduction Paragraph, page 1)</p> <p>Information Technology Terms, Definitions (Section 1.2)</p>	<p>This section is hereby deleted in its entirety and is replaced by the following:</p> <p>"1.2 Customer Data means all data supplied by or on behalf of a Customer to Supplier in connection with the Contract that is under Supplier's custody, excluding any confidential information of Supplier."</p>
<p>Attach D, Information Technology Terms, Termination of Maintenance and Support Services (Section 2, page 3)</p>	<p>This section is hereby deleted in its entirety and is replaced by the following:</p> <p>"2. If applicable, Customer may terminate maintenance or support services without an adjustment charge, provided any of the following circumstances occur:</p> <p>2.1 Customer removes the product for which the services are provided, from productive use or;</p> <p>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).</p> <p>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."</p>
<p>Attach D, Information Technology Terms, Compliance with Technology Policies (Section 6.1)</p>	<p>This section is hereby deleted in its entirety and is replaced by the following:</p> <p>"6.1.</p> <p>The Supplier agrees to adhere to the State of Oklahoma "Information Security Policy, Procedures, and Guidelines" to the extent that (i) such policy is applicable to Supplier in performance of the Services, and (ii) such</p>

RFP Section	Exception
	<p>policy does not conflict with the terms of the Contract or Supplier's own policies.</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 http://eclipse.omes.ok.gov, to the extent that (i) such policies are applicable to Supplier in performance of the Services, and (ii) such policies do not conflict with the terms of the Contract or Supplier's own policies."</p>
Information Technology Terms, Emerging Technologies (Section 7, page 5)	<p>This section is hereby deleted in its entirety and is replaced with the following:</p> <p>"7. The State of Oklahoma reserves the right to enter into an Addendum to the Contract with Customer 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. The parties agree to discuss such proposed changes in good faith, including the implementation requirements and the applicable cost allocation between the parties, and execute any agreed-to changes in an Addendum to the Contract."</p>
Attach D, Information Technology Terms, Extension Right (Section 8, page 5)	<p>This section is hereby deleted in its entirety and is replaced with the following:</p> <p>"In addition to extension rights of the State set forth in the Contract, the State CIO reserves the right to extend any Contract in accordance with the extension terms in the Contract if the State CIO determines such extension to be in the best interest of the State."</p>
Attach D, Information Technology Terms, Source Code Escrow (Section 9)	This section is hereby deleted in its entirety
Attach D, Information Technology Terms, Off-the-Shelf Software (Section 10)	This section is hereby deleted in its entirety
Attach D, Information Technology Terms, Ownership	This section is hereby deleted in its entirety

RFP Section	Exception
Rights (Section 11)	
Attach D, Information Technology Terms, Intellectual Property Ownership (Section 12.1, page 7)	<p>This section is hereby deleted in its entirety and is replaced with the following:</p> <p>“As between Supplier and Customer, the Work Product and Intellectual Property Rights therein, other than any Supplier Intellectual Property included therein, are and shall, upon payment to Supplier hereunder, and subject to the terms herein, be owned exclusively by Customer, and not Supplier. Supplier specifically agrees that, except with respect to Supplier Intellectual Property included therein, the Work Product shall be considered “works made for hire” and that the Work Product, except with respect to Supplier Intellectual Property included therein, 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, other than any Supplier Intellectual Property included therein, is hereby effectively transferred, granted, conveyed, assigned and relinquished exclusively to Customer upon payment to Supplier hereunder, and subject to the terms herein, 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 such 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.</p>
Attach D, Information Technology Terms, Intellectual Property Ownership (Section 12.2)	<p>This section is hereby deleted in its entirety and is replaced with the following:</p> <p>“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.”</p>
Attach D, Information Technology Terms, Intellectual Property Ownership (Section 12.5.)	<p>This section is hereby deleted in its entirety and is replaced with the following:</p> <p>“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 may cause substantial and irreparable harm to Customer’s business. Therefore, Supplier acknowledges and stipulates that Customer may seek a court of competent jurisdiction to immediately</p>

RFP Section	Exception
	<p>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."</p>
<p>Attach D, Information Technology Terms, Intellectual Property Ownership (Section 12.8,)</p>	<p>This section is hereby deleted in its entirety and is replaced with the following:</p> <p>"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, upon payment to Supplier hereunder, and subject to the terms herein, 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."</p>
<p>Attach D, Information Technology Terms, Intellectual Property Ownership (Section 12.9)</p>	<p>This section is hereby deleted in its entirety and is replaced with the following:</p> <p>"Supplier agrees that it shall require consistent compliance with the provisions hereof related to Work Product and Intellectual Property Rights of 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 requirement 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."</p>
<p>Attach D, Information Technology Terms,</p>	<p>This section is hereby deleted in its entirety and is replaced with the following:</p>

RFP Section	Exception
Intellectual Property Ownership (Section 12.11)	<p>“12.11 If applicable, to the extent any Acquisition pursuant to the Contract is funded wholly or in part with federal funds, any source code which is created or customized for the State by Supplier, and all its associated software and related documentation and materials 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.”</p>
Attach D, Information Technology Terms, Hosting Services (Section 13.2, page 10)	<p>This section is hereby deleted in its entirety and is replaced with the following:</p> <p>“13.2 If the Hosting of Customer Data by Supplier or its subcontractor, affiliate or any other person or entity engaged by Supplier to 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.”</p>
Information Technology Terms, Service Level Deficiency (Section 15)	<p>Attachment D, Section 15 shall be deleted in its entirety and replaced with the following:</p> <p>“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. Notwithstanding the foregoing, Supplier and individual agencies seeking a release under the Contract may negotiate specific service level requirements for their release. Any agreed upon service level requirements shall be memorialized in a formal release document reflecting the agreement of the parties.”</p>
Attach D, Appendix 1 to Information Technology Terms, Customer Data (Section A.1)	<p>This section is hereby deleted in its entirety and is replaced with the following:</p> <p>“A.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). Customer shall limit disclosures of Customer Data to Supplier or its subcontractors to the minimum necessary for Supplier or its subcontractors to perform the Services.”</p>
Attach D, Appendix 1 to Information Technology Terms, Customer Data (Section A.2)	<p>This section is hereby deleted in its entirety and is replaced with the following:</p> <p>“2. Supplier shall, unless prohibited by law, 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 reasonably fastest means available and also in writing pursuant to Contract</p>

RFP Section	Exception
	<p>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."</p>
<p>Appendix 1 to Information Technology Terms, Data Security Section B.1</p>	<p>This section is hereby deleted in its entirety and is replaced with the following:</p> <p>"B.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. Except for damage or malfunction caused by Supplier or Supplier's contractors, or as otherwise expressly agreed in this contract or an applicable statement of work, Supplier is not responsible for any equipment or information systems of Customer or its vendors or other service providers."</p>
<p>Appendix 1 to Information Technology Terms, Data Security (Section B.5)</p>	<p>The following section is hereby deleted in its entirety and is replaced with the following:</p> <p>"Supplier shall allow the Customer to audit conformance to the Contract terms upon agreement as to timing and scope. The Customer may perform this audit or contract with a third party at its discretion subject to Supplier's prior written approval (acting reasonably) and the execution of a confidentiality agreement with such third party and at Customer's expense.."</p>
<p>Appendix 1 to Information Technology Terms, Data Security (Section B.6)</p>	<p>The following section is hereby deleted in its entirety and is replaced with the following:</p> <p>"B.6 Supplier shall perform or engage 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. Customer shall not disclose such audit reports, or refer to such audit reports in any communication, to any person or entity other than Customer."</p>
<p>Attach D, Appendix 1 to Information Technology Terms, Security Incident or Data Breach</p>	<p>The introductory sentence to section D of Appendix 1 is hereby modified as follows:</p> <p>"D. Security Incident or Data Breach Notification: Supplier shall inform Customer of its awareness of any Security Incident or Data Breach."</p>

RFP Section	Exception
Notification (Section D)	
Attach D, Appendix 1 to Information Technology Terms, Security Incident or Data Breach Notification (Section D.1, page 15)	<p>This section is hereby deleted in its entirety and is replaced with the following:</p> <p>“D.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, unless otherwise required by applicable law.”</p>
Attach D, Appendix 1 to Information Technology Terms, Security Incident or Data Breach Notification (Section D.2, page 15)	<p>This section is hereby deleted in its entirety and is replaced with the following:</p> <p>“D.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 regarding Supplier’s notification requirement (i.e. HIPAA requires notice to be provided within 24 hours).”</p>
Attach D, Appendix 1 to Information Technology Terms, Security Incident or Data Breach Notification (Section D.3.c page 15)	<p>This section is hereby deleted in its entirety and is replaced with the following:</p> <p>“D.3 Mitigate, to the extent practicable, the cause of the harmful effects of Security Incidents that are known to Supplier; and Document all Security Incidents and their outcomes.”</p>
Attach D, Appendix 1 to Information Technology Terms, Security Incident or Data Breach Notification (Section D.4 page 15)	<p>This section is hereby deleted in its entirety and is replaced with the following:</p> <p>“D.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 from becoming aware, unless shorter time is required by applicable law regarding Supplier’s notification requirement, and (2) take commercially reasonable measures to address the Data Breach in a timely manner.”</p>
Attach D, Appendix 1 to Information Technology Terms, Termination, Expiration and Suspension of Service (Section I.2)	<p>The second sentence of Section I.2 shall be modified as follows:</p> <p>“I, 2. Supplier shall implement an orderly return of Customer Data in a reasonable format specified by Customer and as determined by the Customer:”</p>
Attach D, Appendix 1 to Information Technology Terms,	This section is hereby deleted in its entirety.

RFP Section	Exception
Termination, Expiration and Suspension of Service (Section I.4)	
Appendix 1 to Information Technology Terms, Security Assessment (Section C.1)	<p>This section is hereby deleted in its entirety and is replaced with the following:</p> <p>“C.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, may constitute 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 agrees that during the course of performing the Services, it shall not make changes to its security 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 may constitute a material breach by Supplier and may result in a whole or partial termination of the Contract.”</p>
Appendix 1 to Information Technology Terms, Breach Responsibilities (Section E.2)	<p>This section is hereby deleted in its entirety and is replaced with the following:</p> <p>“E.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 other breach of Supplier’s obligations in this Attachment D, Supplier shall bear the costs associated with (1) Supplier’s investigation and resolution of the Data Breach; (2) Customer’s reasonable, out-of-pocket costs in providing notifications to individuals, regulators or others required by state law; (3) Customer’s reasonable, out-of-pocket costs in obtaining credit monitoring services from a nationally-recognized supplier of such services as required by state or federal law; (4) Customer’s reasonable, out-of-pocket costs in establishing 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; provided that the costs associated with (1) – (5) are subject to the limitation on liability contained in the Contract</p>
Appendix 1 to Information Technology Terms, Breach Responsibilities (Section E.3)	<p>This section is hereby deleted in its entirety.</p>

RFP Section	Exception
Additional Bidder Term	<p>The following section is included in the Contract as an additional Supplier term:</p> <p>“All Customer users requiring access to Deloitte’s systems will be required to complete the Rules of Behavior and Computer User Agreement prior to being granted access.”</p>









Request for Signature - State of OK SW1044 Deloitte eDiscovery

Final Audit Report

2021-11-17

Created:	2021-11-16
By:	Sean Tolbert (Sean.Tolbert@omes.ok.gov)
Status:	Signed
Transaction ID:	CBJCHBCAABAAwzG30svufVVqimGVx3XobjMzq-l5SIIW

"Request for Signature - State of OK SW1044 Deloitte eDiscover y" History

-  Document created by Sean Tolbert (Sean.Tolbert@omes.ok.gov)
2021-11-16 - 8:50:32 PM GMT- IP address: 165.225.216.87
-  Document emailed to Christopher Knox (csknox@deloitte.com) for signature
2021-11-16 - 8:51:27 PM GMT
-  Email viewed by Christopher Knox (csknox@deloitte.com)
2021-11-16 - 8:52:43 PM GMT- IP address: 163.116.129.117
-  Document e-signed by Christopher Knox (csknox@deloitte.com)
Signature Date: 2021-11-16 - 9:03:01 PM GMT - Time Source: server- IP address: 163.116.129.117
-  Document emailed to Jerry Moore (jerry.moore@omes.ok.gov) for signature
2021-11-16 - 9:03:05 PM GMT
-  Email viewed by Jerry Moore (jerry.moore@omes.ok.gov)
2021-11-16 - 11:12:15 PM GMT- IP address: 166.137.115.10
-  Document e-signed by Jerry Moore (jerry.moore@omes.ok.gov)
Signature Date: 2021-11-17 - 5:49:04 PM GMT - Time Source: server- IP address: 165.225.216.87
-  Agreement completed.
2021-11-17 - 5:49:04 PM GMT