OKLAHOMA
Office of Management
& Enterprise Services

# FIRST AMENDMENT TO OKLAHOMA STATEWIDE CONTRACT NO. 1044 WITH DELOITTE LLP

This First Amendment to Oklahoma Statewide Contract No. 1044 (the "First Amendment") is effective as of the date of the last signature below, between the State of Oklahoma by and through the Office of Management and Enterprise Services ("State") and Deloitte Transactions and Business Analytics LLP ("Supplier"). This First Amendment supplements and amends the State of Oklahoma Contract with Deloitte LLP. entered into by the parties and effective on November 17, 2021, (the "Contract"), including all supplements and amendments thereto. Unless otherwise indicated, capitalized terms used in this First Amendment without definition shall have the respective meanings specified in the Contract.

For good and valuable consideration, the parties agree as follows:

1. Supplier and State desire to amend the Contract (as defined in the Contract) to amend the Cover Page to add the following terms and conditions:
    a. To the extent any term or condition in any Contract Document, including via a hyperlink or uniform resource locator, conflicts with an applicable Oklahoma and/or United States law or regulation, such term or condition is void and unenforceable. By executing any Contract Document which contains a conflicting term or condition, the State or Customer makes no representation or warranty regarding the enforceability of such term or condition and the State or Customer does not waive the applicable Oklahoma and/or United States law or regulation which conflicts with the term or condition.

2. Supplier and State desire to amend the Contract (as defined in the Contract) to amend Attachment E – Supplier Pricing to remove terms and conditions regarding travel costs. The following section shall be deleted in its entirety:
    a. Travel and Other Direct Costs (ODO's) – Deloitte has not included any travel or ODC's 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.

3. Supplier and State desire to amend the Contract (as defined in the Contract) to amend Attachment A. Attachment A shall be deleted in its entirety and replaced by Attachment A attached hereto.

4. Supplier and State desire to amend the Contract (as defined in the Contract) to amend Attachment F. Attachment F shall be deleted in its entirety and replaced by Attachment F attached hereto.

5. Supplier and State desire to amend the Contract (as defined in the Contract) to add Attachment D-1 attached hereto.

6. Supplier and State agree that this First Amendment shall be applied retroactively beginning November 17, 2021.

7. Except as expressly modified by this First Amendment, all terms or provisions of the Contract not addressed herein remain as executed by the parties and in full force and effect.

8. This First Amendment may be executed in multiple counterparts, each of which will be an original and together will constitute the same instrument.

**SIGNATURES**

The undersigned represent and warrant that they are authorized, as representatives of the Party on whose behalf they are signing, to sign this First Amendment and to bind their respective Party thereto.

| **STATE:** | **SUPPLIER:** |
|---|---|
| Joe McIntosh (Apr 3, 2024 11:19 CDT) | Christopher Knox (Apr 2, 2024 17:50 EDT) |
| **Authorized Signature** | **Authorized Signature** |
| Joe McIntosh | Christopher Knox |
| **Printed Name** | **Printed Name** |
| Chief Information Officer | Managing Director |
| **Title** | **Title** |
| Apr 3, 2024 | Apr 2, 2024 |
| **Date** | **Date** |

# ATTACHMENT A

# SOLICIATION 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 7 Safeguarding Contract Language

### I. PERFORMANCE

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

(1) All work will be performed under the supervision of the contractor.

(2) The contractor and contractor's officers or employees to be authorized access to FTI must meet background check requirements defined in IRS Publication 1075. The contractor will maintain a list of officers or employees authorized access to FTI. Such list will be provided to the agency and, upon request, to the IRS.

(3) FTI in hardcopy or electronic format shall be used only for the purpose of carrying out the provisions of this contract. FTI in any format shall be treated as confidential and shall not be divulged or made known in any manner to any person except as may be necessary in the performance of this contract. Inspection or disclosure of FTI to anyone other than the contractor or the contractor's officers or employees authorized is prohibited.

(4) FTI will be accounted for upon receipt and properly stored before, during, and after processing. In addition, any related output and products require the same level of protection as required for the source material.

(5) The contractor will certify that FTI processed during the performance of this contract will be completely purged from all physical and electronic data storage with no output to be retained by the contractor at the time the work is completed. If immediate purging of physical and electronic data storage is not possible, the contractor will certify that any FTI in physical or electronic storage will remain safeguarded to prevent unauthorized disclosures.

(6) Any spoilage or any intermediate hard copy printout that may result during the processing of FTI will be given to the agency. When this is not possible, the contractor will be responsible for the destruction of the spoilage or any intermediate hard copy printouts and will provide the agency with a statement containing the date of destruction, description of material destroyed, and the destruction method.

(7) All computer systems receiving, processing, storing, or transmitting FTI must meet the requirements in IRS Publication 1075. To meet functional and assurance requirements, the security features of the environment must provide for the managerial, operational, and technical controls. All security features must be available and activated to protect against unauthorized use of and access to FTI.

(8) No work involving FTI furnished under this contract will be subcontracted without the prior written approval of the IRS.

(9) Contractor will ensure that the terms of FTI safeguards described herein are included, without modification, in any approved subcontract for work involving FTI.

(10) To the extent the terms, provisions, duties, requirements, and obligations of this contract apply to performing services with FTI, the contractor shall assume toward the subcontractor all obligations, duties and responsibilities that the agency under this contract assumes toward the contractor, and the subcontractor shall assume toward the contractor all the same obligations, duties and responsibilities which the contractor assumes toward the agency under this contract.

(11) In addition to the subcontractor's obligations and duties under an approved subcontract, the terms and conditions of this contract apply to the subcontractor, and the subcontractor is bound and obligated to the contractor hereunder by the same terms and conditions by which the contractor is bound and

obligated to the agency under this contract.

(12) For purposes of this contract, the term “contractor” includes any officer or employee of the contractor with access to or who uses FTI, and the term “subcontractor” includes any officer or employee of the subcontractor with access to or who uses FTI.

(13) The agency will have the right to void the contract if the contractor fails to meet the terms of FTI safeguards described herein.

**II. CRIMINAL/CIVIL SANCTIONS**

(1) Each officer or employee of a contractor to whom FTI is or may be disclosed shall be notified in writing that FTI disclosed to such officer or employee can be used only for a purpose and to the extent authorized herein, and that further disclosure of any FTI for a purpose not authorized herein constitutes a felony punishable upon conviction by a fine of as much as $5,000 or imprisonment for as long as 5 years, or both, together with the costs of prosecution.

(2) Each officer or employee of a contractor to whom FTI is or may be accessible shall be notified in writing that FTI accessible to such officer or employee may be accessed only for a purpose and to the extent authorized herein, and that access/inspection of FTI without an official need-to-know for a purpose not authorized herein constitutes a criminal misdemeanor punishable upon conviction by a fine of as much as $1,000 or imprisonment for as long as 1 year, or both, together with the costs of prosecution.

(3) Each officer or employee of a contractor to whom FTI is or may be disclosed shall be notified in writing that any such unauthorized access, inspection or disclosure of FTI may also result in an award of civil damages against the officer or employee in an amount equal to the sum of the greater of $1,000 for each unauthorized access, inspection, or disclosure, or the sum of actual damages sustained as a result of such unauthorized access, inspection, or disclosure, plus in the case of a willful unauthorized access, inspection, or disclosure or an unauthorized access/inspection or disclosure which is the result of gross negligence, punitive damages, plus the cost of the action. These penalties are prescribed by IRC sections 7213, 7213A and 7431 and set forth at 26 CFR 301.6103(n)-1.

(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 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.

(4) Granting a contractor access to FTI must be preceded by certifying that each officer or employee understands the agency’s security policy and procedures for safeguarding FTI. A contractor and each officer or employee must maintain their authorization to access FTI through annual recertification of their understanding of the agency’s security policy and procedures for safeguarding FTI. The initial certification and recertifications must be documented and placed in the agency's files for review. As part of the certification and at least annually afterwards, a contractor and each officer or employee must be advised of the provisions of IRC sections 7213, 7213A, and 7431 (see Exhibit 4, *Sanctions for Unauthorized Disclosure*, and Exhibit 5, *Civil Damages for Unauthorized Disclosure*). The training on the agency’s security policy and procedures provided before the initial certification and annually thereafter must also cover the incident response policy and procedure for reporting unauthorized disclosures and data breaches. (See Section 10) For the initial certification and the annual recertifications, the contractor and each officer or employee must sign, either with ink or electronic signature, a confidentiality statement certifying their understanding of the security requirements.

## III. INSPECTION

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

**Attachment 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 B, General Terms, Scope and Contract Renewal (Section 1.2)** | **This section is hereby deleted in its entirety and is replaced with the following:**<br><br>**"**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 Contract Renewal (Section 1.3)** | **This section is hereby deleted in its entirety and is replaced with the following:**<br><br>"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." |

| | |
|---|---|
| **Attach B, General Terms, Scope and Contract Renewal (Section 1.4)** | **This section is hereby deleted in its entirety and is replaced with the following:**<br><br>**"**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." |
| **Attach B, General Terms, Modification of Contract Terms and Contract Documents (Section 3.1)** | **This section is hereby deleted in its entirety and is replaced with the following:**<br><br>**"**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." |
| **Attach B, General Terms, Definitions (Section 4.18)** | **This section is hereby deleted in its entirety and is replaced with the following:**<br><br>**"**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." |
| **Attach B, General Terms, Definitions (Section 4.21, page 6)** | **This section is hereby deleted in its entirety and is replaced with the following:**<br><br>**"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 (vii) all Intellectual Property Rights in any of the foregoing, and which are or were created,<br>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. |
| **Attach B, General Terms, Ordering, Inspection, and Acceptance (Section 6.2, pages 7-8)** | **Item 6.2 of Section 6 is hereby deleted in its entirety and replaced with the following:**<br><br>"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.<br><br>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<br><br>exclusive remedy." |
| **Attach B, General Terms, Maintenance of Insurance, Payment of Taxes, and Workers' Compensation (Section 8.1)** | The following section is deleted in its entirety and is replaced with the following:<br><br>"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).<br><br>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 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:<br><br>A. Workers' Compensation and Employer's Liability Insurance in accordance with and to the extent required by applicable law;<br>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;<br>C. Automobile Liability Insurance with limits of liability of not less than $1,000,000 combined single limit each accident;<br>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;<br>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<br>Additional coverage required in writing in connection with a particular Acquisition." |
| **Attach B, General Terms, Compliance with Applicable Laws (Section 9.2)** | **This section is hereby deleted in its entirety and is replaced with the following:**<br><br>**"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.**"** |
| **Attach B, General Terms, Audits and Records Clause (Section 10.3)** | **This section is hereby deleted in its entirety and is replaced with the following:**<br><br>**"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." |
| **Attach B, General Terms, Confidentiality, Section 11.1)** | **This section is hereby deleted in its entirety and is replaced with the following:**<br><br>**"**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." |
| **Attach B, General Terms, Confidentiality, Section 11.3** | **This section is hereby deleted in its entirety and is replaced with the following:**<br><br>**"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." |
| **Attach B, General Terms, Confidentiality, Section 11.5)** | **This section is hereby deleted in its entirety and is replaced with the following:**<br><br>**"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." |
| **Attach B, General Terms,** | **This section is hereby deleted in its entirety and replaced with the following:** |

| | |
|---|---|
| **Confidentiality (Section 11.6, page 16)** | "**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." |
| **Attach B, General Terms, Patents and Copyrights (Section 15, pages 19-20)** | **This section is hereby removed in its entirety and is replaced with the following:**<br><br>**"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 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)** | **This section is hereby deleted in its entirety and replaced with the following:**<br><br>"**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." |
| **Attach B, General Terms, Indemnification (Section 16.2)** | **This section is hereby deleted in its entirety and replaced with the following:**<br><br>"**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 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** | **This section is hereby deleted in its entirety and replaced with the following :**<br>"**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." |
| **Attach B, General Terms, Indemnification (Section 16.5.B – Limitation of Liability, pages 21-22)** | **This section is hereby deleted in its entirety and replaced with the following:**<br><br>**"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." |
| **Attach B, General Terms, Termination for Funding Insufficiency (Section 17.2,)** | **This section is hereby deleted in its entirety and is replaced with the following:**<br><br>"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." |
| **Attach B, General Terms, Termination for Funding Insufficiency (Section 17.1)** | **This section is hereby deleted in its entirety and is replaced with the following:**<br>**"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.**"** |
| **General Terms, Termination for Cause (Section 18.4)** | **This section is hereby deleted in its entirety and is replaced with the following:**<br><br>**"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." |
| **General Terms, Suspension of Supplier (Section 20.2)** | **This section is hereby deleted in its entirety and is replaced with the following:**<br><br>**"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." |
| **Attach C, Statewide Contract Terms, Termination for Cause (Section 4)** | **This section is hereby deleted in its entirety and is replaced with the following:**<br><br>"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 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)** | **This section is hereby deleted in its entirety and is replaced with the following:**<br><br>**"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." |
| **Attach B, General Terms, Security of Property and Personnel (Section 24)** | **This section is hereby deleted in its entirety and is replaced with the following:**<br><br>**"**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.<br>**"** |
| **Attach B, General Terms, Miscellaneous (Section 26.4 Transition** | **This section is hereby deleted in its entirety and is replaced with the following:**<br><br>"**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 |

| | |
|---|---|
| **Services)** | 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." |
| **Attach B, General Terms, Miscellaneous (Section 26.5 - Publicity** | **This section is hereby deleted in its entirety and is replaced with the following:**<br><br>**"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 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** | **Item (D) of Section 26.8 is hereby deleted in its entirety and is replaced with the following:**<br><br>**"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." |
| **Attach C, Statewide Contract Terms,** | **The following section is included in the Contract as an additional Customer term:**<br><br>**Auto-Deletion of State Data hosted by Supplier:**<br>The Supplier shall automatically delete any Customer's data hosted by the Supplier or in the Supplier's platform 30 calendar days after acceptance of the applicable deliverable for which Customer's data was utilized. The Supplier shall not retain any Customer data longer than 30 calendar days after acceptance of the applicable deliverable for which Customer's data was utilized unless a longer retention period is requested by the Customer. |
| **Information Technology Terms (Introduction Paragraph, page 1)**<br>**Information Technology Terms, Definitio ns (Section 1.2)** | **This section is hereby deleted in its entirety and is replaced by the following:**<br><br>"**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." |
| **Attach D, Information Technology Terms, Termination of Maintenance and Support Services (Section 2, page 3)** | **This section is hereby deleted in its entirety and is replaced by the following:**<br><br>**"2.** If applicable, 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;<br><br>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).<br><br>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." |
| **Attach D, Information Technology Terms, Compliance with Technology Policies (Section 6.1)** | **This section is hereby deleted in its entirety and is replaced by the following:**<br><br>**"6.1.**<br><br>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 policy does not conflict with the terms of the Contract or Supplier's own policies.<br><br>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 to the extent that (i) such policies are applicable to Supplier in performance of the Services, and<br>(ii) such policies do not conflict with the terms of the Contract or Supplier's own policies." |
| **Information Technology Terms, Emerging Technologies (Section 7, page 5)** | **This section is hereby deleted in its entirety and is replaced with the following:**<br><br>**"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." |
| **Attach D, Information Technology Terms, Extension Right (Section 8, page 5)** | **This section is hereby deleted in its entirety and is replaced with the following:**<br><br>**"**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." |
| **Attach D, Information Technology Terms, Source** | **This section is hereby deleted in its entirety** |

| | |
|---|---|
| **Code Escrow (Section 9)** | |
| **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 Rights (Section 11)** | **This section is hereby deleted in its entirety** |
| **Attach D, Information Technology Terms, Intellectual Property Ownership (Section 12.1, page 7)** | **This section is hereby deleted in its entirety and is replaced with the following:**<br><br>"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. |
| **Attach D, Information Technology Terms, Intellectual Property Ownership (Section 12.2)** | **This section is hereby deleted in its entirety and is replaced with the following:**<br><br>**"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." |

| | |
|---|---|
| **Attach D, Information Technology Terms, Intellectual Property Ownership (Section 12.5,)** | **This section is hereby deleted in its entirety and is replaced with the following:**<br><br>**"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 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." |
| **Attach D, Information Technology Terms, Intellectual Property Ownership (Section 12.8,)** | **This section is hereby deleted in its entirety and is replaced with the following:**<br><br>**"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." |
| **Attach D, Information Technology Terms, Intellectual Property Ownership (Section 12.9)** | **This section is hereby deleted in its entirety and is replaced with the following:**<br><br>**"**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." |

| | |
|---|---|
| **Attach D, Information Technology Terms, Intellectual Property Ownership (Section 12.11)** | **This section is hereby deleted in its entirety and is replaced with the following:**<br>**"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." |
| **Attach D, Information Technology Terms, Hosting Services (Section 13.2, page 10)** | **This section is hereby deleted in its entirety and is replaced with the following:**<br><br>**"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." |
| **Information Technology Terms, Service Level Deficiency (Section 15)** | **Attachment D, Section 15 shall be deleted in its entirety and replaced with the following:**<br>**"15 Service Level Deficiency**<br>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.**"** |
| **Attach D, Appendix 1 to Information Technology Terms, Customer Data (Section A.1** | **This section is hereby deleted in its entirety and is replaced with the following:**<br>**"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." |
| **Attach D, Appendix 1 to Information Technology Terms, Customer Data (Section A.2)** | **This section is hereby deleted in its entirety and is replaced with the following:**<br><br>**"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 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." |
| **Appendix 1 to Information Technology Terms, Data Security Section B.1** | **This section is hereby deleted in its entirety and is replaced with the following:**<br><br>**"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." |
| **Appendix 1 to Information Technology Terms, Data Security (Section B.5)** | **The following section is hereby deleted in its entirety and is replaced with the following:**<br><br>"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.." |
| **Appendix 1 to Information Technology Terms, Data Security (Section B.6)** | **The following section is hereby deleted in its entirety and is replaced with the following:**<br><br>**"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. |
| **Attach D, Appendix 1 to Information Technology Terms, Security Incident or Data Breach Notification (Section D)** | **The introductory sentence to section D of Appendix 1 is hereby modified as follows:**<br><br>**"D. Security Incident or Data Breach Notification:** Supplier shall inform Customer of its awareness of any Security Incident or Data Breach." |
| **Attach D, Appendix 1 to Information Technology Terms, Security Incident or Data Breach** | **This section is hereby deleted in its entirety and is replaced with the following:**<br><br>**"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, |

| | |
|---|---|
| **Notification (Section D.1, page 15)** | 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." |
| **Attach D, Appendix 1 to Information Technology Terms, Security Incident or Data Breach Notification (Section D.2, page 15)** | **This section is hereby deleted in its entirety and is replaced with the following:**<br><br>"**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)." |
| **Attach D, Appendix 1 to Information Technology Terms, Security Incident or Data Breach Notification (Section D.3.c page 15)** | **This section is hereby deleted in its entirety and is replaced with the following:**<br><br>"**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." |
| **Attach D, Appendix 1 to Information Technology Terms, Security Incident or Data Breach Notification (Section D.4 page 15)** | **This section is hereby deleted in its entirety and is replaced with the following:**<br><br>"**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." |
| **Attach D, Appendix 1 to Information Technology Terms, Termination, Expiration and Suspension of Service (Section I.2)** | **The second sentence of Section I.2 shall be modified as follows:**<br><br>**"I, 2.** Supplier shall implement an orderly return of Customer Data in a reasonable format specified by Customer and as determined by the Customer:**"** |
| **Attach D, Appendix 1 to Information Technology Terms, Termination, Expiration and Suspension of Service (Section I.4)** | **This section is hereby deleted in its entirety.** |
| **Appendix 1 to Information Technology Terms, Security Assessment** | **This section is hereby deleted in its entirety and is replaced with the following:**<br><br>**"C.1** The State requires any entity or third-party Supplier Hosting Oklahoma Customer Data to submit to a State Certification and Accreditation Review |

| | |
|---|---|
| **(Section C.1)** | 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." |
| **Appendix 1 to Information Technology Terms, Breach Responsibilities (Section E.2)** | **This section is hereby deleted in its entirety and is replaced with the following:**<br><br>"**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 |
| **Appendix 1 to Information Technology Terms, Breach Responsibilities (Section E.3)** | **This section is hereby deleted in its entirety.** |
| **Additional Bidder Term** | **The following section is included in the Contract as an additional Supplier term:**<br>**"**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." |

# Attachment D-1
# Information Security Requirements

## 1. General Information Security Requirements

a. No employee of Contractor or its subcontractors will be granted access to State of Oklahoma agency information systems without the prior completion and approval of applicable logon authorization and acceptable use requests.

b. Contractor or its subcontractors will notify applicable State of Oklahoma agencies when employees who have access to agency information systems are terminated.

c. Contractor or its subcontractors will disclose to Client any suspected breach of the security of the information system or the data contained therein in the most expedient time possible and without unreasonable delay and will cooperate with Client during the investigation of any such incident.

d. Contractor or its subcontractors agree to adhere to the State of Oklahoma "Information Security Policy, Procedures, and Guidelines" available at: https://oklahoma.gov/content/dam/ok/en/omes/documents/InfoSecPPG.pdf

## 2. HIPAA Requirements

a. Contractor shall agree to use and disclose Protected Health Information in its possession or control in compliance with the Standards for Privacy of Individually Identifiable Health Information (Privacy Rule) (45 C.F.R. Parts 160 and 164) under the Health Insurance Portability and Accountability Act (HIPAA) of 1996. The definitions set forth in the Privacy Rule are incorporated by reference into this Contract (45 C.F.R. §§ 160.103 and 164.501).

b. If applicable, Contractor will sign and adhere to a Business Associate Agreement (BAA). The Business Associate Agreement provides for satisfactory assurances that Contractor will use the information only for the purposes for which it was engaged. Contractor agrees it will safeguard the information from misuse, and will comply with HIPAA as it pertains to the duties stated within the contract. Failure to comply with the requirements of this standard may result in funding being withheld from Contractor, and/or full audit and inspection of Contractor's security compliance as it pertains to this contract.

c. Business Associate Terms Definitions:

   i. Unless otherwise defined in this BAA, all capitalized terms used in this BAA have the meanings ascribed in the HIPAA Regulations, provided; however, that "PHI" and "ePHI" shall mean Protected Health Information and Electronic Protected Health Information, respectively, as defined in 45 C.F.R. § 160.103, limited to the information Business Associate received from or created or received on behalf of the applicable State of Oklahoma agency as a Business Associate. "Administrative Safeguards" shall have the same meaning as the term "administrative safeguards in 45 C.F.R. § 164.304, with the exception that it shall apply to the management of the conduct of Business

Associate's workforce, not the State of Oklahoma agency workforce, in relation to the protection of that information.

ii. Business Associate. "Business Associate" shall generally have the same meaning as the term "Business Associate" at 45 C.F.R. 160.103, and in reference to the party to this agreement, shall mean the entity whose name appears below.

iii. Covered Entity. "Covered Entity" shall generally have the same meaning as the term "Covered Entity" at 45 C.F.R. 160.103.

iv. HIPAA Rules. "HIPAA Rules" shall mean the Privacy, Security, Breach Notification, and Enforcement Rules at 45 C.F.R. Part 160 and Part 164, all as may be amended.

v. The following terms used in this Agreement shall have the same meaning as those terms in the HIPAA Rules: Breach, Data Aggregation, Designated Record Set, Disclosure, Health Care Operations, Individual, Minimum Necessary, Notice of Privacy Practices, Protected Health Information, required by law, Secretary, Security Incident, Sub-Contractor, Unsecured PHI, and Use.

d. Obligations of Business Associate: Business Associate may use Electronic PHI and PHI (collectively, "PHI") solely to perform its duties and responsibilities under this Agreement and only as provided in this Agreement. Business Associate acknowledges and agrees that PHI is confidential and shall not be used or disclosed, in whole or in part, except as provided in this Agreement or as required by law. Specifically, Business Associate agrees it will, as applicable:

i. use or further disclose PHI only as permitted in this Agreement or as Required by Law, including, but not limited to the Privacy and Security Rule;

ii. use appropriate safeguards, and comply with Subpart C of 45 C.F.R. Part 164 with respect to Electronic PHI, to prevent use or disclosure of PHI other than as provided for by this Agreement;

iii. implement and document appropriate administrative, physical, and technical safeguards to protect the confidentiality, integrity, and availability of PHI that it creates, receives, maintains, or transmits for or on behalf of Covered Entity in accordance with 45 C.F.R. 164;

iv. implement and document administrative safeguards to prevent, detect, contain, and correct security violations in accordance with 45 C.F.R. 164;

v. make its applicable policies and procedures required by the Security Rule available to Covered Entity solely for purposes of verifying BA's compliance and the Secretary of the Department of Health and Human Services (HHS);

vi. not receive remuneration from a third party in exchange for disclosing PHI received from or on behalf of Covered Entity;

vii. in accordance with 45 C.F.R. 164.502(e)(1) and 164.308(b), if applicable, require that any Sub-Contractors that create, receive, maintain or transmit PHI on behalf of the Business Associate agree to the same restrictions, conditions, and requirements that apply to the Business Associate with respect to such information; this shall be in the

form of a written HIPAA Business Associate Contract and a fully executed copy will be provided to the Contract Monitor;

viii. report to Covered Entity in writing any use or disclosure of PHI that is not permitted under this Agreement as soon as reasonably practicable but in no event later than five calendar days from becoming aware of it and mitigate, to the extent practicable and in cooperation with Covered Entity, any harmful effects known to it of a use or disclosure made in violation of this Agreement;

ix. promptly report to Covered Entity in writing and without unreasonable delay and in no case later than five calendar days any successful Security Incident, as defined in the Security Rule, with respect to Electronic PHI;

x. with the exception of law enforcement delays that satisfy the requirements of 45 C.F.R. 164.412, notify Covered Entity promptly, in writing and without unreasonable delay and in no case later than five calendar days, upon the discovery of a breach of Unsecured PHI. Such notice shall include, to the extent possible, the name of each individual who's Unsecured PHI has been, or is reasonably believed by Business Associate to have been, accessed, acquired, or disclosed during such Breach. Business Associate shall also, to the extent possible, furnish Covered Entity with any other available information that Covered Entity is required to include in its notification to Individuals under 45 C.F.R. § 164.404(c) at the time of Business Associate's notification to Covered Entity or promptly thereafter as such information becomes available. As used in this Section, "breach" shall have the meaning given such term at 45 C.F.R. 164.402;

xi. to the extent allowed by law, for any PHI breach arising out of the unauthorized disclosure by Business Associate of any PHI resulting from the negligent acts or omissions of Business Associate or the breach by Business Associate of any applicable obligation hereunder related to PHI, Contractor will pay for the cost incurred by the Covered Entity to notify impacted individuals and credit monitoring for them for up to one year, if the nature of the information that is subject to the breach is of the type to reasonably necessitate credit monitoring, without limiting the Covered Entity's rights or remedies;

xii. provide access to PHI it maintains in a Designated Record Set to Covered Entity, or if directed by Covered Entity to an Individual in order to meet the requirements of 45 C.F.R. 164.524. In the event that any Individual requests access to PHI directly from Business Associate, Business Associate shall forward such request to Covered Entity within five working days of receiving a request. This shall be in the form of a written HIPAA Business Associate Contract and a fully executed copy will be provided to the Contract Monitor. Any denials of access to the PHI requested shall be the responsibility of Covered Entity;

xiii. make PHI it maintains in a Designated Record Set available to Covered Entity for amendment and incorporate any amendments to PHI in accordance with 45 C.F.R. 164.526;

xiv. document disclosure of PHI it maintains in a Designated Record Set and

information related to such disclosure as would be required for Covered Entity to

respond to a request by an Individual for an accounting of disclosures of PHI, in accordance with 45 C.F.R. 164.528, and within five working days of receiving a request from Covered Entity, make such disclosure documentation and information available to Covered Entity. In the event the request for an accounting is delivered directly to Business Associate, Business Associate shall forward within five working days of receiving a request such request to Covered Entity;

xv. make its internal practices, books, and records related to the use and disclosure of PHI received from or created or received by Business Associate on behalf of Covered Entity available to the Secretary of the Department of HHS, authorized governmental officials, and Covered entity for the purpose of determining Business Associate's compliance with the Privacy Rule. Business Associate shall give Covered Entity advance written notice of requests from HHS or government officials and provide Covered Entity with a copy of all documents made available; and

xvi. require that all of its Sub-Contractors, vendors, and agents to whom it provides PHI or who create, receive, use, disclose, maintain, or have access to Covered Entity's PHI shall agree in writing to requirements, restrictions, and conditions at least as stringent as those that apply to Business Associate under this Agreement, including but not limited to implementing reasonable and appropriate safeguards to protect PHI, and shall require that its Sub-Contractors, vendors, and agents agree to indemnify and hold harmless Covered Entity for their failure to comply with each of the provisions of this Agreement.

e. Permitted Uses and Disclosures of PHI by Business Associate: Except as otherwise provided in this Agreement, Business Associate may use or disclose PHI on behalf of or to provide services to Covered Entity for the purposes specified in this Agreement, if such use or disclosure of PHI would not violate the Privacy Rule if done by Covered Entity. Unless otherwise limited herein, Business Associate may:

i. use PHI for its proper management and administration or to fulfill any present or future legal responsibilities of Business Associate;

ii. disclose PHI for its proper management and administration or to fulfill any present or future legal responsibilities of Business Associate, provided that; (i) the disclosures required by law; or (ii) Business Associate obtains reasonable assurances from any person to whom the PHI is disclosed that such PHI will be kept confidential and will be used or further disclosed only as Required by Law or for the purpose(s) for which it was disclosed to the person, and the person commits to notifying Business Associate of any instances of which it is aware in which the confidentiality of the PHI has been breached;

iii. disclose PHI to report violations of law to appropriate federal and state authorities; or

iv. aggregate the PHI with other data in its possession for purposes of Covered Entity's Health Care Operations;

v. make uses and disclosures and requests for protected health information consistent with Covered Entity's minimum necessary policies and procedures;
vi. de-identify any and all PHI obtained by Business Associate under this BAA, and use such de-identified data, all in accordance with the de-identification requirements of the Privacy Rule [45 C.F.R. § (d)(1)].

f. Obligations of Covered Entity
   i. Covered Entity shall notify Business Associate of any changes in, or revocation of, the permission by an individual to use or disclose his or her PHI, to the extent that such changes may affect Business Associate's use or disclosure of PHI.
   ii. Covered Entity shall notify Business Associate of any restriction on the use or disclosure of PHI that Covered Entity has agreed to or is required to abide by under 45 C.F.R. 164.522, to the extent that such restriction may affect Business Associate's use or disclosure of protected health information.
   iii. Covered Entity shall not request Business Associate use or disclose PHI in any manner that would violate the Privacy Rule if done by Covered Entity.
   iv. Covered Entity agrees to timely notify Business Associate, in writing, of any arrangements between Covered Entity and the Individual that is the subject of PHI that may impact in any manner the use and/or disclosure of the PHI by Business Associate under this BAA.
   v. Covered Entity shall provide the minimum necessary PHI to Business Associate.

g. Term and Termination:
   i. Obligations of Business Associate upon Termination. Upon termination of this Agreement for any reason, Business Associate, with respect to PHI received from Covered Entity, or created, maintained, or received by Business Associate on behalf of Covered Entity, shall as applicable:
      (1) retain only that PHI that is necessary for Business Associate to continue its proper management and administration or to carry out its legal responsibilities;
      (2) return to Covered Entity (or, if agreed to by Covered Entity, destroy) the remaining PHI that the Business Associate still maintains in any form;
      (3) continue to use appropriate safeguards and comply with Subpart C of 45 C.F.R. Part 164 with respect to PHI to prevent use or disclosure of the PHI, other than as provided for in this Section, for as long as Business Associate retains the PHI;
      (4) not use or disclose the PHI retained by Business Associate other than for the purposes for which such PHI was retained and subject to the same conditions set out at above under "Permitted Uses and Disclosures By Business Associate" that applied prior to termination; and
      (5) return to Covered Entity (or, if agreed to by Covered Entity, destroy) the PHI retained by Business Associate when it is no longer needed by Business Associate for its proper management and administration or to carry out its legal responsibilities.

ii. All other applicable obligations of Business Associate under this Agreement shall survive termination.

iii. Should the applicable State of Oklahoma agency become aware of a pattern of activity or practice that constitutes a material breach of a material term of this BAA by Business Associate, the agency shall provide Business Associate with written notice of such a breach in sufficient detail to enable Contractor to understand the specific nature of the breach. The Client shall be entitled to terminate the Underlying Contract associated with such breach if, after the applicable State of Oklahoma agency provides the notice to Business Associate, Business Associate fails to cure the breach within a reasonable time period not less than thirty (30) days specified in such notice; provided, however, that such time period specified shall be based on the nature of the breach involved per 45 C.F.R. §§ 164.504(e)(1)(ii)(A),(B) & 164.314 (a)(2)(i)(D).

h. Miscellaneous Provisions:

i. No Third Party Beneficiaries: Nothing in this Agreement shall confer upon any person other than the parties and their respective successors or assigns, any rights, remedies, obligations, or liabilities whatsoever.

ii. Business Associate recognizes that any incurable material breach of this Business Associate Terms section or breach of confidentiality or misuse of PHI may result in the termination of this Agreement and/or legal action. Said termination may be immediate and need not comply with any termination provision in the parties' underlying agreement, if any.

iii. The parties agree to amend this Agreement from time to time as is necessary for Covered Entity or Business Associate to comply with the requirements of the Privacy Rule and related laws and regulations.

iv. The applicable State of Oklahoma agency shall make available its Notice of Privacy Practices.

v. Any ambiguity in this Agreement shall be resolved in a manner that causes this Agreement to comply with HIPAA.

vi. If Business Associate maintains a designated record set in an electronic format on behalf of Covered Entity, then Business Associate agrees that within 30 calendar days of expiration or termination of the parties' agreement, Business Associate shall provide to Covered Entity a complete report of all disclosures of and access to the designated record set covering the three years immediately preceding the termination or expiration. The report shall include patient name, date and time of disclosures/access, description of what was disclosed/accessed, purpose of disclosure/access, name of individual who received or accessed the information, and, if available, what action was taken within the designated record set.

vii. Amendment: To the extent that any relevant provision of the HIPAA Regulations is materially amended in a manner that changes the obligations of Business Associates or Covered Entities, the Parties agree to negotiate in good faith appropriate amendment(s)

to this Agreement to give effect to these revised obligations. The parties agree to amend this Agreement from time to time as is necessary for Covered Entity or to comply with the requirements of the Privacy Rule and related laws and regulations.

**3. 42 C.F.R. Part 2 Related Provisions**

a. Confidentiality of Information. Contractor's employees and agents shall have access to private data to the extent necessary to carry out the responsibilities, limited by the terms of this Agreement. Contractor accepts the responsibilities for providing adequate administrative supervision and training to their employees and agents to ensure compliance with relevant confidentiality, privacy laws, regulations and contractual provisions. No private or confidential data collected, maintained, or used shall be disseminated except as authorized by statute and by terms of this Agreement, whether during the period of the Agreement or thereafter. Furthermore, Contractor:

i. Acknowledges that in receiving, transmitting, transporting, storing, processing, or otherwise dealing with any information received pursuant to this agreement that identifies or otherwise relates to the individuals under the care of or in the custody of a State of Oklahoma agency, it is fully bound by the provisions of the federal regulations governing the confidentiality of Alcohol and Drug Abuse Patient Records, 42 C.F.R. Part 2 and the HIPAA, 45 C.F.R. 45 Parts 142, 160, and 164, Title 43 A § 1-109 of Oklahoma Statutes, and may not use or disclose the information except as permitted or required by this Agreement or by law;

ii. Acknowledges that pursuant to 43A O.S. §1-109, all mental health and drug or alcohol treatment information and all communications between physician or psychotherapist and patient are both privileged and confidential and that such information is available only to persons actively engaged in treatment of the client or consumer or in related administrative work. Contractor agrees that such protected information shall not be available or accessible to staff in general and shall not be used for punishment or prosecution of an kind;

iii. Agrees to resist any efforts in judicial proceedings to obtain access to the protected information except as expressly provided for in the regulations governing the Confidentiality of Alcohol and Drug Abuse Patient Records, 42 C.F.R. Part 2;

iv. Agrees to, when applicable and to the extent within Contractor's control, use appropriate administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of the electronic protected health information that it creates, receives, maintains, or transmits on behalf of the State of Oklahoma agency and to use appropriate safeguards to prevent the unauthorized use or disclosure of the protected health information, and agrees that protected information will not be placed in the Child Protective Services (CPS) record of any individual involved with the Oklahoma Department of Human Services (DHS).

v. Agrees to report to the State of Oklahoma agency any use or disclosure or any security incident involving protected information not provided for by this Agreement. Such a report shall be made immediately when an employee becomes aware of such a disclosure, use, or security incident.

vi. Agrees to provide access to the protected information at the request of the State of Oklahoma agency or to an authorized individual as directed by the State of Oklahoma agency, in order to meet the requirement of 45 C.F.R. §164.524 which provides clients with the right to access and copy their own protected information;

vii. Agrees to make any amendments to the protected information as directed or agreed to by the State of Oklahoma agency, pursuant to 45 C.F.R. §164.526;

viii. Agrees to make available its internal practices, books, and records, including policies and procedures, relating to the use and disclosure of protected information received from the State of Oklahoma agency or created or received by the Contractor on behalf of the State of Oklahoma agency, to the State of Oklahoma agency and to the Secretary of the Department of Health and Human Services for purpose of the Secretary determining the giving party's compliance with HIPAA;

ix. Agrees to provide the State of Oklahoma agency, or an authorized individual, information to permit the State of Oklahoma agency to respond to a request by an individual for an accounting of disclosures in accordance with 45 C.F.R. §164.528.

b. Data Security. The Contractor agrees to, when applicable and to the extent within Contractor's control, maintain the data in a secure manner compatible with the content and use. The Contractor will, when applicable to the extent within Contractor's control, control access to the data in Contractor's possession or control compliance with the terms of this Agreement. Only the Contractor's personnel whose duties require the use of such information, will have regular access to the data. The Contractor's employees will be allowed access to the data only for the purpose set forth in this Agreement.

c. Data Destruction. Contractor agrees to, when applicable and to the extent within Contractor's control, follow State of Oklahoma agency policies regarding secure data destruction.

d. Use of Information. Contractor agrees that the information received or accessed through this Agreement shall not be used to the detriment of any individual nor for any purpose other than those stated in this Agreement.

e. Redisclosure of Data. The Contractor agrees not to redisclose any information to a third party not covered by the Agreement unless written permission by the State of Oklahoma agency is received and redisclosure is permitted under applicable law.

**4. RESERVED.**

5. **SSA Requirements (If applicable)**
    a. PERFORMANCE: If Contractor takes possession or control of in SSA provided information in the performance of this contract, the contractor agrees to, where applicable and to the extent within Contractor's control comply with and assume responsibility for compliance by his or her employees with the following requirements:
        i. All work will be done under the supervision of the State of Oklahoma.
        ii. Any SSA provided information made available shall be used only for carrying out the provisions of this Agreement. Information contained in such material shall be treated as confidential and shall not be divulged or made known in any manner to any person except as may be necessary in the performance of this contract. Inspection by or disclosure to anyone other than an officer or employee of the Contractor is prohibited.
        iii. All SSA provided information shall be accounted for upon receipt and properly stored before, during, and after processing. In addition, all related output and products will be given the same level of protection as required for the source material.

iv. No work involving SSA provided information furnished under this contract shall be subcontracted without prior written approval by the applicable State of Oklahoma agency and the SSA.
v. The Contractor shall maintain a list of employees authorized access. Such list shall be provided upon request to the applicable State of Oklahoma agency or the SSA.
vi. Contractor or agents may not legally process, transmit, or store SSA-provided information in a cloud environment without explicit permission from SSA's Chief Information Officer. Proof of this authorization shall be provided to the Contractor by the applicable State of Oklahoma agency prior to accessing SSA provided information.
vii. Contractor shall provide security awareness training to all employees, contractors, and agents who access SSA-provided information. The training should be annual, mandatory, and certified by the personnel who receive the training. Contractor is also required to certify that each employee, contractor, and agent who views SSA-provided information certify that they understand the potential criminal, civil, and administrative sanctions or penalties for unlawful assess and/or disclosure.
viii. Contractor shall require employees, contractors, and agents to sign a non-disclosure agreement, attest to their receipt of Security Awareness Training, and acknowledge the rules of behavior concerning proper use and security in systems that process SSA-provided information. Contractor shall retain non-disclosure attestations for at least five (5) to seven (7) years for each employee who processes, views, or encounters SSA-provided information as part of their duties.
ix. The applicable State of Oklahoma agency shall provide the Contractor a copy of the SSA exchange agreement and all related attachments before initial disclosure of SSA data. Contractor is required to follow the terms of the applicable State of Oklahoma agency's data exchange agreement with the SSA. Prior to signing this Agreement, and thereafter at SSA's request, the applicable State of Oklahoma agency shall obtain from the Contractor a current list of the employees of such Contractor with access to SSA data and provide such list to the SSA.
x. Where the Contractor processes, handles, or transmits information provided to the applicable State of Oklahoma agency by SSA or has authority to perform on the agency's behalf, the applicable State of Oklahoma agency shall clearly state the specific roles and functions of the Contractor within the Agreement.
xi. SSA requires all parties subject to this Agreement to exercise due diligence to avoid hindering legal actions, warrants, subpoenas, court actions, court judgments, state or Federal investigations, and SSA special inquiries for matters pertaining to SSA-provided information.
xii. SSA requires all parties subject to this Agreement to agree that any Client-owned or subcontracted facility involved in the receipt, processing, storage, or disposal of SSA-provided information operate as a "de facto" extension of the Client and is subject to onsite inspection and review by the Client or SSA with prior notice.

xiii. If the Contractor must send a Contractor computer, hard drive, or other computing or storage device offsite for repair, the Contractor must have a non-disclosure clause in their contract with the vendor. If the Contractor used the item in a business process that involved SSA-provided information and the vendor will retrieve or may view SSA-provided information during servicing, SSA reserves the right to inspect the Contractor's vendor contract. The Contractor must remove SSA-provided information from electronic devices before sending it to an external vendor for service. SSA expects the Contractor to render SSA-provided information unrecoverable or destroy the electronic device if they do not need to recover the information. The same applies to excessed, donated, or sold equipment placed into the custody of another organization.

xiv. In the event of a suspected or verified data breach involving SSA provided information, the Contractor shall notify the Client immediately.

xv. The Client shall have the right to void the contract if the contractor fails to provide the safeguards described above.

b. CRIMINAL/CIVIL SANCTIONS: The Act specifically provides civil remedies, 5 U.S.C. Sec. 552a(g), including damages, and criminal penalties, 5 U.S.C. Sec. 552a(i), for violations of the Act. The civil action provisions are premised violations of the Act committed by parties subject to this Agreement or regulations promulgated thereunder. An individual claiming such a violation by parties subject to this Agreement may bring civil action in a federal district court. If the individual substantially prevails, the court may assess reasonable attorney fees and other litigation costs. In addition, the court may direct the parties subject to this Agreement to grant the plaintiff access to his/her records, and when appropriate direct an amendment or correction of records subject to the Act. Actual damages may be awarded to the plaintiff for intentional or willful refusal by parties subject to this Agreement to comply with the Act.

i. Civil Remedies.

(1) In any suit brought under the provisions of 5 U.S.C. § 552a(g)(1)(C) or (D) in which the court determines that the parties subject to this Agreement acted in a manner which was intentional or willful, shall be liable in an amount equal to the sum of —

(a) actual damages sustained by the individual because of the refusal or failure, but in no case, shall a person entitled to recovery receive less than the sum of $1,000; and

(b) the costs of the action together with reasonable attorney fees as determined by the court.

(2) An action to enforce any liability created under 5 U.S.C. § 552a may be brought in the district court of the United States in the district in which the complainant resides, or has his principal place of business, or in which the records are situated, or in the District of Columbia, without regard to the amount in controversy, within two years from the date on which the cause of action arises, except that where

parties subject to this Agreement have materially and willfully misrepresented any information required under this section to be disclosed to an individual and the information so misrepresented is material to establishment of the liability of the agency to the individual under 5 U.S.C. § 552a, the action may be brought at any time within two years after discovery by the individual of the misrepresentation. Nothing in this section shall be construed to authorize any civil action because of any injury sustained as the result of a disclosure of a record prior to September 27, 1975.

ii. Criminal Penalties

(1) Any officer or employee of an agency, who by virtue of his employment or official position, has possession of, or access to, agency records which contain individually identifiable information the disclosure of which is prohibited by this section or by rules or regulations established thereunder, and who knowing that disclosure of the specific material is so prohibited, willfully discloses the material in any manner to any person or agency not entitled to receive it, shall be guilty of a misdemeanor and fined not more than $5,000. See 5 U.S.C. § 552a(i)(1).

(2) Any officer or employee of any agency who willfully maintains a system of records without meeting the notice requirements of subsection (e)(4) of this section shall be guilty of a misdemeanor and fined not more than $5,000. See 5 U.S.C. § 552a(i)(2).

(3) Any person who knowingly and willfully requests or obtains any record concerning an individual from an agency under false pretenses shall be guilty of a misdemeanor and fined not more than $5,000. See 5 U.S.C. § 552a(i)(3).

**6. Child Support FPLS Requirements (If applicable)**

a. Contractor, when applicable and to the extent within Contractor's control, and the applicable State of Oklahoma agency must comply with the security requirements established by the Social Security Act, the Privacy Act of 1974, the Federal Information Security Management Act of 2002 (FISMA), 42 United States Code (USC) 654(26), 42 UCS 654a(d)(1)-(5), the U.S. Department of Health and Human Services (HHS), the U.S. Department of Health and Human Services Administration of Children and Families Office of Child Support Enforcement Security Agreement and the Automated Systems for Child Support Enforcement: A Guide for States Section H Security and Privacy. Contractor and applicable State of Oklahoma agency also agree to use Federal Parent Locator Service (FPLS) information and Child Support (CS) program information solely for the authorized purposes in accordance with the terms in this agreement. The information exchanged between state Child Support agencies and all other state program information must be used for authorized purposes and protected against unauthorized access to reduce fraudulent activities and protect the privacy rights of individuals against unauthorized disclosure of confidential information.

i. This is applicable to the personnel, facilities, documentation, data, electronic and physical records and other machine-readable information systems of the applicable State of Oklahoma agency and Contractor, including, but not limited to, state employees and contractors working with FPLS information and CS program information and state CS agency data centers, statewide centralized data centers, contractor data centers, state Health and Human Services' data centers, comprehensive tribal agencies, data centers serving comprehensive tribes, and any other individual or entity collecting, storing, transmitting or processing FPLS information and CS program information. This is applicable to all FPLS information, which consists of the National Directory of New Hires (NDNH), Debtor File, and the Federal Case Registry (FCR). The NDNH, Debtor File and FCR are components of an automated national information system.

ii. This is also applicable to all CS program information, which includes the state CS program information, other state and tribal program information, and confidential information. Confidential information means any information relating to a specified individual or an individual who can be identified by reference to one or more factors specific to him or her, including but not limited to the individual's Social Security number, residential and mailing addresses, employment information, and financial information. Ref. 45 Code of Federal Regulations (CFR) 303.21(a).

**7. FERPA Requirements (If applicable)**

a. If Contractor takes possession or control of Information covered by FERPA in performance of this Agreement, Contractor agrees to, when applicable and to the extent within Contractor's control comply with and assume responsibility for compliance by its employees with the Family Educational Rights and Privacy Act; (20 U.S.C. § 1232g; 34 CFR Part 99) ("FERPA") and the Oklahoma Student Data Accessibility, Transparency, and Accountability Act of 2013; (70 O.S. § 3-168), where personally identifiable student education data is exchanged.

**8. CJIS Requirements (If applicable)**

a. INTRODUCTION

This section shall be applicable to the extent that Contractor takes possession or control of CJIS data. The use and maintenance of all items of software or equipment offered for purchase herein must be in compliance with the most current version of the U.S. Department of Justice, Federal Bureau of Investigation ("FBI"), Criminal Justice Information Services (CJIS) Division's CJIS Security Policy ("CJIS Security Policy" or "Security Policy" herein).

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

b. CJIS SECURITY POLICY REQUIREMENTS GENERALLY

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

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

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

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

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

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

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

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

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