OKLAHOMA
Office of Management
& Enterprise Services

State of Oklahoma

Office of Management and Enterprise Services

STATE OF OKLAHOMA CONTRACT
WITH EQUIFAX WORKFORCE SOLUTIONS LLC

This State of Oklahoma Contract ("Contract") is entered into between the State of Oklahoma by and through the Oklahoma Employment Security Commission ("State") and Equifax Workforce Solutions LLC ("Supplier") and is effective as of the effective date set forth on a properly issued purchase order or, if no effective date is listed, the date of last signature to this Contract. The initial term of the Contract shall be for one (1) year with four (4) one-year options to renew.

Purpose

The State is awarding this Contract to Supplier for the purchase of access to recent incarceration information obtained from jails and correctional facilities across the country, as more particularly described in certain Contract Documents. Supplier submitted a proposal containing exceptions to the Solicitation and Supplier requested confidential matters to be considered. This Contract memorializes the agreement of the parties with respect to negotiated terms of the Contract that is being awarded to Supplier.

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

1. The parties agree that Supplier has not yet begun performance of work under this Contract. Issuance of a purchase order is required prior to payment to a Supplier.

2. The following Contract Documents are attached hereto and incorporated herein:

   2.1. Solicitation #EV00000579, Attachment A;
   2.2. Non-Negotiable Terms, Attachment A-1;
   2.3. General Terms, Attachment B;
   2.4. Reserved, Attachment C;
   2.5. Information Technology Terms, Attachment D;
   2.6. Pricing, Attachment E-1;
   2.7. Reserved, Attachment E-2;
   2.8. Universal Membership Agreement & Schedule A, Attachment E-3
   2.9. IT Security Standards, Attachment E-4;
   2.10. Value Add, Attachment E-5;
   2.11. Reserved, Attachment F;
   2.12. Federal Funding Terms, Attachment G.

3. The parties additionally agree:

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

3.3. To the extent any term or condition in any Contract Document, including via a hyperlink or uniform resource locator, conflicts with an applicable Oklahoma and/or United States law or regulation, such term or condition is void and unenforceable. By executing any Contract Document which contains a conflicting term or condition, the State or Customer makes no representation or warranty regarding the enforceability of such term or condition and the State or Customer does not waive the applicable Oklahoma and/or United States law or regulation which conflicts with the term or condition.

4. The parties recognize that while the State of Oklahoma is executing this contract, payment obligations rest solely with the Oklahoma Employment Security Commission, and OMES shall not be responsible for such. Please send invoices and billing inquiries to:

Oklahoma Employment Security Commission
Attn: Accounts Payable
P.O. Box 52003,
Oklahoma City, OK 73152-2003
Invoice Email: AccountsPayable@oesc.ok.gov

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

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

6. The undersigned Agency hereby attests that any required terms and conditions based on a Federal Award applicable to this Contract are included herein.

[THE REMAINDER OF THIS PAGE IS INTENTIONALLY LEFT BLANK]

SIGNATURES

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

STATE OF OKLAHOMA
by and through the OKLAHOMA
EMPLOYMENT SECURITY COMMISSION

By: Trae Rahill
Trae Rahill (Jul 7, 2026 13:56:57 CDT)

Name: Trae Rahill

Title: CEO

Date: Jul 7, 2026

EQUIFAX WORKFORCE SOLUTIONS LLC

By: _____
David Turner (May 26, 2026 14:44:04 EDT)

Name: David Turner

Title: SVP & General Manager

Date: May 26, 2026

The Chief Information Officer is signing solely to approve the Contract pursuant to 62 O.S., § 34.11.1 concerning procurement of Information Technology and/or Telecommunications.

By: _____
Dan Cronin (Jul 7, 2026 14:20:16 CDT)

Name: Dan Cronin

Title: Chief Information Officer/Chief Transformation Officer

Date: Jul 7, 2026

Attachment A

Solicitation No. EV00000579

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.

I. PURPOSE

The Office of Management and Enterprise Services (OMES), Central Purchasing Division, is seeking responses on behalf of Oklahoma's Employment Security Commission (OESC) from potential Suppliers to provide a contract for the purchase of access via File Transfer Protocol (FTP) and the internet to recent incarceration information obtained from jails and correctional facilities across the country. A Contract resulting from this Solicitation may be designated for use as a Statewide Contract.[1]

1. Contract Term and Renewal Options:

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

2. Contract Specifications

2.1. Certain Contract requirements and terms are attached hereto as Exhibit 1 and incorporated herein.

3. Solicitation Criterion:

3.1. The Bid will be evaluated using a best value criterion, based on the following:

i. Mandatory Requirement -Exhibit#1
ii. Price- Exhibit#2
iii. Supplier Requirements and References (Meet or Do not Meet-Score will be Yes or No)

[1] 74 O.S. 85.5(G)(3)

Exhibit 1

EV00000579

1. SOLICITATION SPECIFICATIONS

The Office of Management and Enterprise Services (OMES), on behalf of the Oklahoma Employment Security Commission (OESC) is seeking the services of a vendor to provider access via File Transfer Protocol (FTP) and the Internet to recent (OESC) is seeking the services of a vendor to provide access via File Transfer Protocol (FTP) and the internet to recent incarceration information obtained from jails and correctional facilities across the country. This procurement is being sought in order to identify and prevent Unemployment Insurance (UI) claimants being paid benefits while incarcerated. Oklahoma envisions a weekly process that would enable a data set of the last four (4) weeks of Oklahoma UI claimants to be transferred via FTP to a vendor. The vendor would use OESC's file to search for matches in the file of incarcerated individuals for the requested time frame and return the file of UI claimant matches or hits via FTP to OESC. Oklahoma investigators would access, via the internet, the database that houses the incarceration data to verify booking dates and perform identification validation. The object of this service is to provide OESC the ability to perform nationwide searched to determine whether Oklahoma UI claimants are or were incarcerated during the weeks for which benefits were claimed.

2. Mandatory Specifications/Requirements

2.1. Mandatory requirements are the minimum capabilities, features, and/or technical standards that must be met by proposed solution to be determined response. Supplier shall provide a brief narrative, describing any installation and configuration requirements and the proposed method to meet the requirements of the RFP. Supplier should provide examples, samples, and or screenshots as applicable to the proposed solution.

2.2 Functionality

The proposed solution must be fully capable of the following.

2.2.1 Solution must include Web Based access to a database that houses the criminal information for the majority of the incarcerated person in the United States, including those in local jails as well as correctional facilities.

2.2.2 Access to the information must be web-bases and must allow authorized registered subscribers the ability to view current offender data as well as historical data for offenders that have been released. Vendor must specify how long the historical information for an offender is maintained in the database.

2.2.3 Batch processing capabilities are required with formatting in PDF or Word.

2.2.4 OESC will provide a Payment Data Set via FTP containing Social Security Number, Name, Date of Birth, Beginning Date and Ending Date for between 25,000 and 100,000 records weekly to the vendor for matching with incarceration information. Vendor will return a "Hit" Data Set back to OESC via FTP containing but not limited incarceration Dates, Correctional Facility, Facility State, and the Facility Telephone number of matched records where 3 or more days of incarceration occurred during and between the Beginning and Ending Dates supplied by OESC. Vendor will

2.3 Web and Database Access

2.3.1 Solution must provide proper execution using Microsoft Internet Explorer 6 or higher.

2.3.2 Bandwidth must be provided to support timely response to all users.

2.4. Queries

2.4.1 Solution must include online web-based query. Supplier shall provide a brief narrative for the proposed solution's Query capabilities and any applicable examples, samples and/or screenshots.

3. Additional Features/Functions

Supplier should provide detailed information for additional features/functions, describe how each of these items will be proved or accomplished. Supplier's response must state if the feature/function is available or unavailable and include any associated cost. Additional points may be given for response to this section.

3.1. Vendor should provide justification which proves that the proposed solution contains information for the 'majority" (stated in a percentage) of incarcerated persons in the United States.

3.2. Vendor should also provide a list of the correctional/local facilities by State that are not currently available in the database.

3.3. Because offenders are often processed and released within a 24-hour period, it is important that the data in the central database be kept current via hourly updates, at a minimum. Vendor should describe their data refresh policy.

3.4. OESC prefers a solution that will maintain four (4) weeks of the "Hit" Data Sets that were returned to OESC. Vendor would match weekly Hit records to be returned to OESC against those already sent in order to eliminate duplicate Hits being returned for the same incarceration dates and facilities. Describe the method used to insure against duplicate Hit records.

4. Implementation/Work plan

Supplier shall submit a proposed implementation and support plan solutions and processes

i. As a part of the proposal, Vendor should include a preliminary Project Work Plan and timeline. A mutually agreed upon Project Plan and Timeline will be finalized after award.

5. Staffing Plan

The successful: contractor will provide the necessary personnel, facilities, supplies, equipment, and/or related resources and skills to accomplish the requirements of a contract. All of the work and services required shall be performed by the Contractor or Sub-Contractor staff and must be fully qualified and authorized under State and Local law to perform such work and/or services.

6. Training Plan

Within the proposal, vendor, should define a Training Plan and Schedule for the training being offered as part of the base package, including up to 10 participate. Training location should be held in Oklahoma City.

7. Maintenance/Support

The proposed solution must provide Ongoing Maintenance-Support during the performance of the contract. Support is required for ongoing maintenance, including but not limited to, standards and process updates.

7.1. OESC expects the maintenance and support service to include all application software upgrades, patches, and customizations.

7.2. Describe Helpdesk description and availability.

7.3. Describe regular maintenance schedules and any downtime required for maintenance.

7.4. Ongoing maintenance shall be quoted both monthly and quarterly, although it shall be invoiced/paid quarterly.

8. Project Management

Kickoff Meeting- The project schedule/work plan will include a kickoff meeting to be help with OESC within 14 days of award. The minimum participate from the Contractor's team at this kickoff meeting will be the OESC Project Manager, the Contractor's Manger/Account Executive providing corporate oversight of the project, and at least one Lead Developer. In the event that a component of the system is provided through a subcontractor, the subcontractor's Project Manager and technical representative will be at the kickoff meeting. OESC will provide similar representation. The Contractor shall provide a written report to the OESC Project Manager within 5 working

days documenting all discussions and decisions conducted at the kickoff meeting.

Project Schedule- The final Project Schedule, Implementation/Work Plan, will be developed by the Contractor with input and final approval by OESC. The agreed-upon project schedule may not be modified without the mutual written consent of the OESC Project Manager and the Contractor's Project Manager.

Addition Project Management Support- If the project encounters difficulty; OESC may require additional meetings or progress/status reports. The Contractor shall maintain and support such additional project management support in the format and the frequency deemed necessary by OESC, at no additional cost. At the discretion of OESC, such support may take the form of written reports, conference call, and/or face-to-face meetings, as required.

ATTACHMENT A1: NON-NEGOTIABLE TERMS
STATE OF OKLAHOMA LOCKDOWN GENERAL TERMS

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

1 Scope and Contract Renewal

1.1 Supplier may not add products or services to its offerings under the Contract without the State's prior written approval. Such request may require a competitive bid of the additional products or services. If the need arises for goods or services outside the scope of the Contract, Supplier shall contact the State.

1.2 At no time during the performance of the Contract shall the Supplier have the authority to obligate any Customer for payment for any products or services (a) when a corresponding encumbering document is not signed or (b) over and above an awarded Contract amount. Likewise, Supplier is not entitled to compensation for a product or service provided by or on behalf of Supplier that is neither requested nor accepted as satisfactory.

1.3 If applicable, prior to any Contract renewal, the State shall subjectively consider the value of the Contract to the State, the Supplier's performance under the Contract, and shall review certain other factors, including but not limited to the: a) terms and conditions of Contract documents to determine validity with current State and other applicable statutes and rules; b) current pricing and discounts offered by Supplier; and c) current products, services and support offered by Supplier. If the State determines changes to the Contract are required as a condition precedent to renewal, the State and Supplier will cooperate in good faith to evidence such required changes in an Amendment. Further, any request for a price increase in connection with a renewal or otherwise will be conditioned on the Supplier providing appropriate documentation supporting the request.

1.4 Upon mutual agreement, the Parties may extend the Contract for ninety (90) days beyond a final renewal term. The Parties may to the extent allowable by law, choose to exercise subsequent ninety (90) day extensions.

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

2 Contract Effectiveness

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

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

3 Modification of Contract Terms and Contract documents

3.1 The Contract may only be modified, amended, or expanded by an Amendment. Any change to the Contract, including the addition of work or materials, the revision of payment terms, or the substitution of work or materials made unilaterally by the Supplier, is a material breach of the Contract. Unless otherwise specified by applicable law or rules, such changes, including without limitation, any unauthorized written Contract modification, shall be void and without effect and the Supplier shall not be entitled to any claim under the Contract based on those changes. No oral statement of any person shall modify or otherwise affect the terms, conditions, or specifications stated in the Contract.

3.2 Any additional terms on an ordering document provided by Supplier are of no effect and are void unless mutually executed. OMES bears no liability for performance, payment or failure thereof by the Supplier or by a customer other than OMES in connection with an Acquisition.

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

3.4 Unless mutually agreed to in writing by the State of Oklahoma by and through the Office of Management and Enterprise Services, no Contract document or other terms and conditions or clauses, including via a hyperlink or uniform resource locator, shall supersede or conflict with the terms of this Contract or expand the State's or OMES's liability or reduce the rights of OMES or the State.

3.5 To the extent any term or condition in any Contract document, including via a hyperlink or uniform resource locator, conflicts with an applicable state or federal law or regulation, such term or condition is void and

unenforceable. By executing any Contract document which contains a conflicting term or condition, neither makes a representation or warranty regarding the enforceability of such term or condition and the neither party waives the state or federal law or regulation which conflicts with the term or condition.

4 Pricing

4.1 Pursuant to 68 O.S. §§ 1352, 1356, and 1404, State agencies are exempt from the assessment of State sales, use, and excise taxes. Further, State agencies and political subdivisions of the State are exempt from Federal Excise Taxes pursuant to Title 26 of the United States Code. Any taxes of any nature whatsoever payable by the Supplier shall not be reimbursed.

4.2 Pursuant to 74 O.S. §85.40, all travel expenses of Supplier must be included in the total Acquisition price.

4.3 The price of a product offered under the Contract shall include and Supplier shall prepay all shipping, packaging, delivery and handling fees. All product deliveries will be free on board Customer's Destination. No additional fees shall be charged by Supplier for standard shipping and handling. If Customer requests expedited or special delivery, Customer may be responsible for any charges for expedited or special delivery

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

4.5 Pursuant to OAC 260:115-9-1, 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 the Acquisition at Supplier's expense or, if unable to replace, shall issue a refund to Customer. Refund under this section shall not be an exclusive remedy.

5 Invoices and Payments

5.1 Supplier shall be paid upon submission of a proper invoice(s) at the prices

stipulated in the Contract in accordance with 74 O.S. §85.44B which requires that payment be made only after products have been provided and accepted or services rendered and accepted. This section shall not prohibit the payment of membership dues or payment for subscriptions to magazines, periodicals or books or for payment to vendors providing subscription services under 74 O.S. 85.44B.
The following terms additionally apply:

A. An invoice shall contain the purchase order number, description of products or services provided and the dates of such provision.

B. Failure to provide a timely and proper invoice may result in delay of processing the invoice for payment. Proper invoice is defined at OAC 260:10-1-2.

C. Payment of all fees under the Contract shall be due NET 30 days, but shall not be deemed late until 45 days. Payment and interest on late payments are governed by 62 O.S. §34.72. Such interest is the sole and exclusive remedy for late payments by a State agency and no other late fees are authorized to be assessed pursuant to Oklahoma law.

D. The date from which an applicable early payment discount time is calculated shall be from the receipt date of a proper invoice. There is no obligation, however, to utilize an early payment discount.

E. If an overpayment or underpayment has been made to Supplier any subsequent payments to Supplier under the Contract may be adjusted to correct the account. A written explanation of the adjustment will be issued to Supplier.

F. If the Supplier accepts payment by Purchase Card they shall do so according to Oklahoma law.

6 Oklahoma Open Records Act

Supplier acknowledges that all State agencies and certain other Customers are subject to the Oklahoma Open Records Act set forth at 51 O.S. §24A-1 et seq. Supplier also acknowledges that compliance with the Oklahoma Open Records Act and all opinions of the Oklahoma Attorney General concerning the Act is required. Customer may be provided access to Supplier Confidential Information. State agencies are subject to the Oklahoma Open Records Act and Supplier acknowledges information marked confidential information will be disclosed to the extent permitted under the Open Records Act and in accordance with this section.

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

7 Conflict of Interest

In addition to any requirement of law or of a professional code of ethics or conduct, the Supplier, its employees are required to disclose any outside activity or interest that conflicts or may conflict with the best interest of the State. Prompt disclosure is required under this section if the activity or interest is related, directly or indirectly, to any person or entity currently under contract with or seeking to do business with the State, its employees or any other third-party individual or entity awarded a contract with the State. Further, as long as the Supplier has an obligation under the Contract, any plan, preparation or engagement in any such activity or interest shall not occur without prior written approval of the State. Any conflict of interest shall, at the sole discretion of the State, be grounds for partial or whole termination of the Contract.

8 State Shall Not Indemnify

The State of Oklahoma cannot lawfully agree to indemnify a private contractor. The credit of the State shall not be given, pledged, or loaned to any individual, company, corporation, or association, municipality, or political subdivision of the State pursuant to Oklahoma Constitution article 10, Section 15, OAC 260:115-7-32(k)(3)(A) and Attorney General Opinion 2012-18.

9 Indemnification Coordination of Defense

9.1 In connection with indemnification obligations under the Contract, when a

State agency is a named defendant in any filed or threatened lawsuit, the defense of the State agency shall be coordinated by the Attorney General of Oklahoma, or the Attorney General may authorize the Supplier to control the defense and any related settlement negotiations; provided, however, Supplier shall not agree to any settlement of claims against the State without obtaining advance written concurrence from the Attorney General. If the Attorney General does not authorize sole control of the defense and settlement negotiations to Supplier, Supplier shall have authorization to equally participate in any proceeding related to the indemnity obligation under the Contract and shall remain responsible to indemnify the applicable Indemnified Parties.

10 Termination for Funding Insufficiency

10.1 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.

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

10.3 The State's exercise of its right to terminate the Contract under this section shall not be considered a default or breach under the Contract or relieve the Supplier of any liability for claims arising under the Contract.

11 Suspension Certification Regarding Debarment, Suspension, and Other Responsibility Matters

The certification made by Supplier with respect to Debarment, Suspension, certain

indictments, convictions, civil judgments and terminated public contracts is a material representation of fact upon which reliance was placed when entering into the Contract. A determination that Supplier knowingly rendered an erroneous certification, in addition to other available remedies, may result in whole or partial termination of the Contract for Supplier's default. Additionally, Supplier shall promptly provide written notice to the State Purchasing Director if the certification becomes erroneous due to changed circumstances.

12 Certification Regarding State Employees Prohibition From Fulfilling Services

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

13 Notices

All notices, approvals or requests allowed or required by the terms of any Contract shall be in writing, reference the Contract with specificity and deemed delivered upon receipt or upon refusal of the intended party to accept receipt of the notice. Notice information may be updated in writing to the other party as necessary.
In addition to other notice requirements in the Contract and the designated Supplier contact provided in a successful Bid, notices shall be sent to the State at the email address set forth below.

Notwithstanding any other provision of the Contract, confidentiality, breach and termination-related notices shall be delivered to the address below in addition to e-mail.

If sent to the State:
State Purchasing Director
2401 North Lincoln Blvd., Second Floor
Oklahoma City, Oklahoma 73105

With a copy, which shall not constitute notice, to:
Purchasing Division Deputy General Counsel
2401 North Lincoln Blvd., Second Floor
Oklahoma City, Oklahoma 73105

14 Miscellaneous

14.1 Choice of Law and Venue

Any claim, dispute, or litigation relating to the Contract documents, in the

singular or in the aggregate, shall be governed by the laws of the State of Oklahoma without regard to application of choice of law principles. Pursuant to 74 O.S. §85.7(F), where Federal awards are involved, applicable federal laws, rules and regulations shall govern to the extent necessary to insure ensure compliance with the terms of the Federal award. Venue for any action, claim, dispute, or litigation relating in any way to the Contract documents, shall be in Oklahoma County, Oklahoma. The State expressly declines any terms that minimize its rights under Oklahoma Law, including but not limited to, Statutes of Limitations.

14.2 Employment Relationship

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

14.3 Failure to Enforce

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

14.4 Invalid Term or Condition

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

14.5 Severability

If any provision of a Contract document, or the application of any term or

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

14.6 Section Headings

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

14.7 Sovereign Immunity

Notwithstanding any provision in the Contract, the Contract is entered into subject to the State's Constitution, statutes, common law, regulations, and the doctrine of sovereign immunity, none of which are waived by the State nor any other right or defense available to the State; provided, however, that the parties hereby agree that the doctrine of sovereign immunity does not apply to actions grounded in contract and therefore does not prohibit Supplier from pursuing claims arising under the Contract against the State and Customers.

14.8 Survival

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

14.9 Gratuities

The Contract may be immediately terminated, in whole or in part, by written notice if it is determined that the Supplier, its authorized employee, agent, or another representative acting within the scope of their authority violated any federal, State or local law, rule or ordinance by offering or giving a

gratuity to any State employee directly involved in the Contract. In addition, Suspension or Debarment of the Supplier may result from such a violation.

14.10 Import/Export Controls

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

ATTACHMENT B

STATE OF OKLAHOMA NEGOTIABLE GENERAL TERMS

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

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

1 Contract Order of Priority

1.1 Contract documents shall be read to be consistent and complementary. Any conflict among the Contract documents shall be resolved by giving priority to Contract documents in the following order of precedence:

A. any Amendment.

B. Attachments A-D, Attachment E-3, and Attachment G (as and if provisions of Attachment G are applicable to Supplier or Suppliers Services, Data, and Information) in this Contract document (taking precedence in alphabetical order).

C. Pricing T&Cs Attachments E-1 through E-4.

D. any other statement of work, work order, or other mutually agreed Contract documents.

1.2 Both parties acknowledge that Equifax Workforce Solutions LLC will not include any click wrap or shrink wrap terms in this contract. However, the following language will be applicable if Equifax Workforce Solutions LLC does include click wrap or shrink wrap terms in the future: If there is a conflict between the terms contained in this Contract document or in Contract-specific terms and an agreement provided by or on behalf of Supplier including but not limited to linked or supplemental documents which alter or diminish the rights of Customer or the State, the conflicting terms provided by Supplier shall not take priority over this Contract document or Acquisition-specific terms. In no event will any linked document alter or override such referenced terms except as specifically agreed in an Amendment.

2 Definitions

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

2.1 **Acquisition** means items, products, materials, supplies, services and equipment acquired by purchase, lease purchase, lease with option to purchase, value provided or rental under the Contract. The Services, Data, and information are explicitly not included under the Definition of an Acquisition**.**

2.2 **Amendment** means any mutually executed, written modification to a Contract document or a written change, addition, correction or revision to a Solicitation.

2.3 **Bid** means an offer a Bidder submits in response to the Solicitation.

2.4 **Bidder** means an individual or business entity that submits a Bid in response to the Solicitation.

2.5 **Contract** means the written, mutually agreed and binding legal relationship resulting from the Contract documents and an appropriate encumbering document as may be amended from time to time, which evidences the final agreement between the parties with respect to the subject matter of the Contract. May also be referred to as the "Agreement."

2.6 **Customer** means the entity receiving goods or services contemplated by the Contract. May also be referred to as the "Agency".

2.7 **Debarment** means action taken by a debarring official under federal or state law or regulations to exclude any business entity from inclusion on the Supplier list; bidding; offering to bid; providing a quote; receiving an award of contract with the State and may also result in cancellation of existing contracts with the State.

2.8 **Destination** means delivered to the receiving dock or other point specified in the applicable Contract document.

2.9 **Federal Award** means the Federal financial assistance that a recipient receives directly from a Federal awarding agency or indirectly from a pass-through entity

2.10 **Governmental Entity** means any governmental entity specified as a political subdivision of the State pursuant to the Governmental Tort Claim Act including any associated institution, instrumentality, board, commission, committee, department, or other entity designated to act on behalf of the state.

2.11 **Indemnified Parties** means the State and Customer and/or its officers, directors, agents, employees, representatives, contractors, assignees and designees thereof.

2.12 **Inspection** means the physical examining and testing an Acquisition (including, when appropriate, raw materials, hardware components, and physical assemblies) to determine whether the Acquisition meets Contract requirements. For the avoidance of doubt, "Inspection" is limited to tangible items and does not include any audit, assessment, or testing of software, Information Assets, technology systems, or security protocols.

2.13 **Moral Rights** means any and all rights of paternity or integrity of the Work Product and the right to object to any modification, translation or use of the Work Product and any similar rights existing under the judicial or statutory law of any country in the world or under any treaty, regardless of whether or not such right is denominated or referred to as a moral right. Supplier (and its licensors) shall at all times retain all right, title, and interest in and to the Servies, Data (excluding Customer and State Data), and Information, including all such Moral Rights. Nothing in this Agreement shall be construed as granting to the Customer any license, waiver, title or consent in or to the same, all of which are expressly reserved by the Suppler.

2.14 **OAC** means the Oklahoma Administrative Code.

2.15 **OMES** means the Office of Management and Enterprise Services.

2.16 **Solicitation** means the document inviting Bids for the Acquisition referenced in the Contract and any amendments thereto.

2.17 **State** means the government of the state of Oklahoma, its employees and authorized representatives, including without limitation any department, agency, or other unit of the government of the state of Oklahoma.

2.18 **Supplier** means the Bidder with whom the State enters into the Contract awarded pursuant to the Solicitation or the business entity or individual that is a party to the Contract with the State.

2.19 **Suspension** means action taken by a suspending official under federal or state law or regulations to suspend a Supplier from inclusion on the Supplier list; be eligible to submit Bids to State agencies and be awarded a contract by a State agency subject to the Central Purchasing Act and as used under Section 11 of Attachment A1.

2.20 **Supplier Confidential Information** means certain confidential and proprietary information of Supplier that is clearly marked as confidential and other certain information asserted and defined as Confidential Information under Section 8, Confidentiality, agreed by the State Purchasing Director or Customer, as applicable. Notwithstanding the foregoing, Supplier Confidential Information shall not include: 1. Information expressly excluded from confidentiality by other provisions of this Contract; or 2. information that is deemed a public record and subject to disclosure under the Oklahoma Open Records Act, unless such information falls under a specific statutory exemption (such as a trade secret) and has been properly asserted as such in accordance with this Contract and applicable law.

2.21 **Work Product** means any and all deliverables produced by Supplier under a statement of work or similar Contract document issued pursuant to this Contract, including any and all tangible or intangible items or things that have been or will be prepared, created, developed, invented or conceived at any time following the Contract effective date including but not limited to any (i) works of authorship (such as manuals, instructions, printed material, graphics, artwork, images, illustrations, photographs, computer programs, computer software, scripts, object code, source code or other programming code, HTML code, flow charts, notes, outlines, lists, compilations, manuscripts, writings, pictorial materials, schematics, formulae, processes, algorithms, data, information, multimedia files, text web pages or web sites, other written or machine readable expression of such works fixed in any tangible media, and all other copyrightable works), (ii) trademarks, service marks, trade dress, trade names, logos, or other indicia of source or origin, (iii) ideas, designs, concepts, personality rights, methods, processes, techniques, apparatuses, inventions, formulas, discoveries, or improvements, including any patents, trade secrets and know-how, (iv) domain names, (v) any copies, and similar or derivative works to any of the foregoing, (vi) all documentation and materials related to any of the foregoing, (vii) all other goods, services or deliverables to be provided by or on behalf of Supplier under the Contract and (vii) all Intellectual Property Rights in any of the foregoing, and which are or were created, prepared, developed, invented or conceived for the use of benefit of Customer in connection with this Contract or with funds appropriated by or for Customer or Customer's benefit (a) by any Supplier personnel or Customer personnel or (b) any Customer personnel who then became personnel to Supplier or any of its affiliates or subcontractors, where, although creation or reduction-to-practice is completed while the person is affiliated with Supplier or its personnel, any portion of same was created, invented or conceived by such person while affiliated with Customer. All Work Product, excluding the Work Product, or portions thereof, containing Customer or State Data, shall be the

sole and exclusive property of Supplier. To the extent that any Work Product is deemed to be "work made for hire" or ownership otherwise vests in the Customer by operation of law, Customer hereby irrevocably assigns to Supplier all right, title, and interest in and to such Work Product, including all Intellectual Property Rights therein.

3 Additional Pricing

3.1 If products are provided under this Contract, the price of a product offered under the Contract shall include and Supplier shall prepay all shipping, packaging, delivery and handling fees. All product deliveries will be free on-board Customer's Destination. No additional fees shall be charged by Supplier for standard shipping and handling. If Customer requests expedited or special delivery, Customer may be responsible for any charges for expedited or special delivery.

4 Ordering, Inspection, and Acceptance

4.1 **Purchase Orders**. Any product or service furnished under the Contract shall be ordered by issuance of a valid purchase order or other appropriate payment mechanism, including a pre-encumbrance, or by use of a valid Purchase Card. All orders and transactions are governed by the terms and conditions of the Contract. Any purchase order or other applicable payment mechanism dated prior to termination or expiration of the Contract shall be performed unless mutually agreed in writing otherwise.

4.2 The following information must be provided as part of the Contract. Failure to include this information reflects Agency's agreement that a PO shall not be required by Agency. Agency shall provide notice of any PO changes no less than thirty (30) days prior to the expiration of the current PO. No additional terms and conditions shall be included in the PO unless expressly agreed to in writing by the Parties. If there is a conflict between language in the PO and the Contract, the Contract shall control. The PO Amount or dollar limit, if applicable, of initial PO does not limit or otherwise impact any minimum ordering obligations or purchase commitments specified herein. The PO effective dates (as defined below) does not impact the Effective Date(s) or Term(s) specified herein.

PO Number (or similar):		PO Amount:	
PO Start Date:		PO End Date:	
PO Contact Name:		PO Contact Email:	

4.3 Services will be performed in accordance with industry standard practices and are subject to acceptance by the Customer. Supplier may invoice the Customer for Services or associated deliverables upon delivery or provision. Notwithstanding any other provision in the Contract, and to the extent permitted by applicable law, receipt of an invoice by the Customer shall constitute deemed acceptance of the applicable Services or deliverables; provided however that nothing in this section shall be construed to waive or limit any inspection or acceptance rights required under applicable law, including OAC 260:115-9, Deemed acceptance shall not apply automatically solely upon receipt of a deliverable or upon provision of a service absent an invoice.

4.4 WARRANTY. Supplier warrants that the Service will be performed in all material respects in a reasonable and workmanlike manner and in compliance with laws and regulations applicable to EVS's performance thereof. Agency acknowledges that the ability of EVS to provide accurate information is dependent upon receipt of accurate information from employers. EVS does not warrant that the Service will be error free. EXCEPT FOR THE EXPRESS WARRANTIES SET FORTH HEREIN, EVS MAKES NO OTHER WARRANTIES AS TO THE SERVICE OR THE DATA, EXPRESSED OR IMPLIED, INCLUDING ANY IMPLIED WARRANTY OF GOOD TITLE, MERCHANTABILITY, AND/OR FITNESS FOR A PARTICULAR PURPOSE EVEN IF EVS KNOWS OF SUCH PURPOSE

4.5 If products are provided under this Contract, any product to be delivered pursuant to the Contract shall be subject to final inspection and acceptance by the Customer at Destination.

Pursuant to OAC 260:115-9-1 and the terms of this Agreement, if the Services provided do not meet the express warranties set forth herein, Supplier shall be notified in writing within thirty (30) days of the delivery of the Service. Supplier shall, at its option, either re-perform the Service or issue a refund of the fees paid for the specific Service giving rise to the claim. The foregoing states Supplier's entire liability and Customer's sole and exclusive remedy for any breach of warranty. In no event shall Equifax's aggregate liability for any such claim exceed the amounts actually paid by Customer for the specific service connected with the event giving rise to the liability.

4.6 Supplier shall deliver services on or before the required date specified in a Contract document, for clarity, no Services shall be provided prior to the Effective Date of the Contract. Deviations, substitutions, or changes in a product or service, including changes of personnel directly providing services, shall not be made unless expressly authorized. Any substitution of personnel

directly providing services shall be a person of comparable or greater skills, education and experience for performing the services as the person being replaced. Additionally, Supplier shall utilize staff sufficiently experienced and able to perform with respect to any reasonable transitional services provided by Supplier in connection with termination or expiration of the Contract.

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

5.1 As a condition of this Contract, Supplier shall procure at its own expense, and provide proof of, insurance coverage with the applicable liability limits set forth below and any approved subcontractor of Supplier shall procure and provide proof of the same coverage. The required insurance shall be underwritten by an insurance carrier with an A.M. Best rating of A- or better.

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

A. Workers' Compensation and Employer's Liability Insurance in accordance with and to the extent required by applicable law.

B. Commercial General Liability Insurance covering the risks of personal injury, bodily injury (including death) and property damage, including coverage for contractual liability, with a limit of liability of not less than $2,000,000 per occurrence and in the aggregate.

C. Automobile Liability Insurance with limits of liability of not less than $2,000,000 combined single limit each accident.

D. If the Supplier will access, process, or store state data, then Security and Privacy Liability insurance, including coverage for failure to protect confidential information and failure of the security of Supplier's computer systems that results in unauthorized access to Customer data with limits $5,000,000 per occurrence and in the aggregate; and

E. Additional coverage required in writing in connection with a particular Acquisition if mutually agreed upon.

5.2 Supplier shall be entirely responsible during the existence of the Contract for the liability and payment of taxes payable by or assessed to Supplier or its employees, agents and subcontractors of whatever kind, in connection with the Contract. Supplier further agrees to comply with all state and federal laws applicable to any such persons, including laws regarding wages, taxes, insurance, and Workers' Compensation. Neither Customer nor the State shall be liable to the Supplier, its employees, agents, or others for the payment of taxes or the provision of unemployment insurance and/or Workers' Compensation or any benefit available to a State or Customer employee. Agency shall provide Contractor with a copy of its tax-exemption certificate, and update this certificate from time to time as so required.

5.3 To the extent permitted by laws applicable to the parties, Supplier agrees to indemnify Customer, the State, and its employees, agents, representatives, contractors, and assignees for any and all liability, actions, claims, demands, or suits, and all related costs and expenses (including without limitation reasonable attorneys' fees and expenses) brought by third parties against Customer and arising from Supplier's: (i) breach of this Agreement; (ii) negligent or intentional, wrongful act or omission; (iii) infringement on third party proprietary rights; or (iv) violation of law. Notwithstanding the indemnification obligations under this contract, Customer shall not be liable for tax liability based upon Supplier's net income, or any state or local privilege or franchise taxes, as well as any unemployment insurance and/or Workers' Compensation obligations in connection with Supplier's employees and its performance under the Contract.

6 Compliance with Applicable Laws

6.1 As long as Supplier has an obligation under the terms of the Contract and in connection with performance of its obligations, the Supplier represents its present compliance, and shall have an ongoing obligation to comply, with all applicable federal, State, and local laws, rules, regulations, ordinances, and orders, as amended, including but not limited to the following if and as they

apply to Supplier, the Service, and/or Information and Data received therefrom:

A. Drug-Free Workplace Act of 1988 set forth at 41 U.S.C. §81.

B. Section 306 of the Clean Air Act, Section 508 of the Clean Water Act, Executive Order 11738, and Environmental Protection Agency Regulations which prohibit the use of facilities included on the EPA List of Violating Facilities under nonexempt federal contracts, grants or loans.

C. Prospective participant requirements set at 45 C.F.R. part 76 in connection with Debarment, Suspension and other responsibility matters.

D. 1964 Civil Rights Act, Title IX of the Education Amendment of 1972, Section 504 of the Rehabilitation Act of 1973, Americans with Disabilities Act of 1990, and Executive Orders 11246 and 11375.

E. Anti-Lobbying Law set forth at 31 U.S.C. §1325 and as implemented at 45 C.F.R. part 93.

F. Requirements of Internal Revenue Service Publication 1075 regarding use, access and disclosure of Federal Tax Information (as defined therein).

G. Obtaining certified independent audits conducted in accordance with Government Auditing Standards and Office of Management and Budget Uniform Guidance, 2 CFR 200 Subpart F §200.500 et seq. with approval and work paper examination rights of the applicable procuring entity.

H. Requirements of the Oklahoma Taxpayer and Citizen Protection Act of 2007, 25 O.S. §1312 and applicable federal immigration laws and regulations and be registered and participate in the Status Verification System. The Status Verification System is defined at 25 O.S. §1312, includes but is not limited to the free Employment Verification Program (E-Verify) through the Department of Homeland Security, and is available at **Home | E-Verify**;

I. Requirements of the Health Insurance Portability and Accountability Act of 1996; Health Information Technology for Economic and Clinical Health Act; Payment Card Industry Security Standards;

Criminal Justice Information System Security Policy and Security Addendum; and Family Educational Rights and Privacy Act; and

J. Be registered as a business entity licensed to do business in the State, have obtained a sales tax permit, and be current on franchise tax payments to the State, as applicable.

6.2 The Supplier, its employees, and subcontractors agree to adhere to the State of Oklahoma Data Security Standard, Acceptable Use Standard, System Acceptable Use Standard, and Personal Device Standard, as attached hereto as Attachment E-4.

6.3 At no additional cost to Customer, the Supplier shall maintain all applicable licenses and permits required in association with its obligations under the Contract.

6.4 In addition to compliance under subsection 6.1 above, Supplier shall have a continuing obligation to comply with applicable Customer-specific mandatory contract provisions, which have been provided and agreed to by Supplier and required in connection with the receipt of federal funds or other funding source.

6.5 The Supplier is responsible to for its employees, agents, and subcontractors who provide a product or perform the Service under the Contract and will ensure such employees, agents, and subcontractor perform in such a manner as to enable Supplier to meet Supplier's obligations under the Contract.

6.6 As applicable, Supplier agrees to comply with the Governor's Executive Orders related to the use of any tobacco product, electronic cigarette or vaping device on any and all properties owned, leased, or contracted for use by the State, including but not limited to all buildings, land and vehicles owned, leased, or contracted for use by agencies or instrumentalities of the State.

6.7 The execution, delivery and performance of the Contract and any ancillary documents by Supplier will not, to the best of Supplier's knowledge, violate, conflict with, or result in a breach of any provision of, or constitute a default (or an event which, with notice or lapse of time or both, would constitute a default) under, or result in the termination of, any written contract or other instrument between Supplier and any third party.

6.8 Supplier represents that it has the ability to pay its debts when due and it does not anticipate the filing of a voluntary or involuntary bankruptcy petition or appointment of a receiver, liquidator or trustee.

6.9 Supplier represents that, to the best of its knowledge as of the effective date of this Agreement, any litigation or claim or any threat thereof involving Supplier that could reasonably be expected to have a material adverse effect on Supplier's ability to perform its obligations under the Contract, has been disclosed in writing to the State and Supplier is not aware of any other such litigation, claim or threat thereof.

6.10 If Services provided by Supplier include delivery of an electronic communication, Supplier shall ensure such communication and any associated support documents are compliant with, or are working towards compliance with, Section 508 of the Federal Rehabilitation Act and with State standards regarding accessibility. Should any communication or associated support documents be non-compliant, Supplier shall correct and re-deliver such communication immediately upon discovery or notice, at no additional cost to the State. Additionally, as part of compliance with accessibility requirements where documents are only provided in non-electronic format, Supplier shall promptly provide such communication and any associated support documents in an alternate format usable by individuals with disabilities upon request and at no additional cost, which may originate from an intended recipient or from the State.

7 Audits and Records Clause

7.1 As used in this clause and pursuant to 67 O.S. §203, "Record" includes a document, book, paper, photograph, microfilm, computer tape, disk, record, sound recording, film recording, video record, accounting procedures and practices, and other data, regardless of type and regardless of whether such items are in written form, in the form of computer data, or in any other form.

7.2 Supplier agrees any pertinent federal or State agency or governing entity of a Customer shall have the right to examine and audit, at no additional cost to a Customer, all specific Records relevant to the invoices, payments, execution, and performance of the Contract specific to the relevant Customer and its Contract except, unless otherwise agreed, costs of Supplier that comprise pricing under the Contract. Such examinations and audits shall be conducted in accordance with Supplier's policies and procedures and not include information or Records otherwise exempt as confidential, proprietary, trade secret information, or otherwise protected or exempt under other applicable laws.

7.3 The Supplier is required to retain records relative to the Contract for the duration of the Contract and for a period of seven (7) years following completion or termination of an Acquisition unless otherwise indicated in the

Contract terms , provided, however, that Supplier shall only be required to maintain such records for seven (7) years following the individual creation of such records by Vendor, or as otherwise required by law. If a claim, audit, litigation or other action involving such records is started before the end of the seven-year period, the records are required to be maintained for two (2) years from the date that all issues arising out of the action are resolved, or until the end of the seven (7) year retention period, whichever is later. For the avoidance of doubt, the record retention requirements set forth in this Section do not apply to audit logs or regulatory items that Supplier is required to maintain under applicable law, which shall be governed by their respective regulatory retention schedules.

7.4 Pursuant to 74 O.S. §85.41, if professional services are provided hereunder, all items of the Supplier that relate to the professional services are subject to examination by the State agency, State Auditor and Inspector and the State Purchasing Director. Professional services are not provided hereunder.

8 Confidentiality

8.1 Subject to federal and state law, rule, or regulation including but not limited to the Oklahoma Open Records Act, as applicable, each party acknowledges that materials and information disclosed by a party ("Disclosing Party") to another party ("Recipient") in connection with performance of this Agreement, including Data and Information obtained from the Service, the negotiated of this Agreement and the pricing terms provided to a specific Customer consist of confidential and proprietary data ("Confidential Information"). Each Recipient will hold those materials and that information in strict confidence, and will restrict its use of those materials and that information to the purposes anticipated in this Agreement. If the law or legal process requires Recipient to disclose confidential and proprietary data, Recipient will notify the Disclosing Party of the request. Thereafter, the Disclosing Party may seek a protective order or waive the confidentiality requirements of this Agreement, provided that Recipient may only disclose the minimum amount of information necessary to comply with the requirement. Recipient will not be obligated to hold confidential any information from the Disclosing Party which (a) is or becomes publicly known, (b) is received from any person or entity who, to the best of Recipient's knowledge, has no duty of confidentiality to the Disclosing Party, (c) was already known to Recipient prior to the disclosure, and that knowledge was evidenced in writing prior to the date of the other party's disclosure, or (d) is developed by the Recipient without using any of the Disclosing Party's information. The rights and obligations of this Section, with respect to (i) confidential and proprietary data that constitutes a "trade secret" (as defined by applicable law), will survive termination of this Agreement for

so long as such confidential and proprietary information remains a trade secret under applicable law; and (ii) all other confidential and proprietary data, will survive the termination of this Agreement for the longer of two (2) years from termination, or the confidentiality period required by applicable law.

8.2 Additionally, the Supplier shall maintain strict security of all State and citizen data and records provided to it by the State ("State Confidential Information"), in accordance with and subject to applicable federal and State laws, rules, regulations, and policies and shall use State Confidential Information only as necessary for Supplier to perform its obligations under the Contract. Supplier shall not sell, release, or otherwise disclose Confidential Information of the State without written permission, except as to Supplier's Affiliates, subcontractors, and Service Providers (including cloud service providers) as necessary to perform the Services or as otherwise permitted under this Agreement and in order to comply with applicable law. The Supplier agrees that State Confidential Information provided under this Agreement 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 State 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 represents that it has a tested and proven system in effect designed to protect all State Confidential Information.

8.3 Each party shall establish, maintain and enforce agreements with all such persons and entities that have access to the other's Confidential Information to fulfill their duties and obligations under the Contract and to specifically prohibit any sale, assignment, conveyance, provision, release, dissemination or other disclosure of any State or citizen data or records except as required by law or allowed by written prior approval of the other party.

8.4 A party shall immediately report to the other any and all unauthorized use, appropriation, sale, assignment, conveyance, provision, release, access, acquisition, disclosure or other dissemination of any Confidential Information 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 party providing notice shall also promptly furnish to the other full details of the unauthorized use, appropriation, sale, assignment, conveyance, provision, release, access, acquisition, disclosure or other

dissemination, or attempt thereof, and use its best efforts to assist the other party in investigating or preventing the reoccurrence of such event in the future. The Supplier shall cooperate with the Customer in connection with any investigation regarding a Security Incident/Data Breach involving Confidential Information and shall promptly remediate any findings. In the event of a third-party claim arising from Supplier's breach of its data security obligations, Supplier shall indemnify Customer for resulting losses and costs to the extent provided in the Indemnity section of this Agreement.

8.5 Each party further agrees to promptly prevent a reoccurrence of any unauthorized use, appropriation, sale, assignment, conveyance, provision, release, access, acquisition, disclosure or other dissemination of Confidential Information.

8.6 Each party acknowledges that any improper use, appropriation, sale, assignment, conveyance, provision, release, access, acquisition, disclosure or other dissemination of any Confidential Information to others may cause immediate and irreparable harm to the other party and certain beneficiaries and may violate state or federal laws and regulations. If a party 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, that party will immediately be entitled to injunctive relief and/or any other rights or remedies available under this Contract, at equity or pursuant to applicable statutory, regulatory, and common law without a cure period.

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

9 Assignment and Permitted Subcontractors

9.1 Except as permitted below, Supplier's obligations under the Contract may not be assigned or transferred to any other person or entity without the prior written consent of the State which may be withheld at the State's sole discretion, however, such consent shall not be unreasonably withheld. Should Supplier assign its rights to payment, in whole or in part, under the Contract, Supplier shall provide the State and affected Customer(s) with written notice of the

assignment. Such written notice shall be delivered timely and contain details sufficient for affected Customer(s) to perform payment obligations without any delay caused by the assignment.

9.2 Notwithstanding the foregoing, the Contract may be freely assigned by Supplier to, and shall inure to the benefit of and be binding upon, any corporation or other entity in connection with a merger, consolidation, sale of all equity interests of the Supplier, or a sale of all or substantially all of the assets of the Supplier to which the Contract relates, or to an entity within Supplier's family of companies or an entity with common ownership and control. In any such case, said corporation or other entity shall by operation of law or expressly in writing assume all obligations of the Supplier as fully as if it had been originally made a party to the Contract. Supplier shall give the State and all affected Customers prior written notice of said assignment unless such advance notice is not permitted under applicable law. Any assignment or delegation in violation of this subsection shall be void.

9.3 If the Supplier is permitted to utilize subcontractors in support of the Contract, the Supplier shall remain solely responsible for its obligations under the terms of the Contract, for its actions and omissions and those of its agents, employees and subcontractors and for payments to such persons or entities. Prior to a subcontractor being utilized by the Supplier to provide material work under this Contract, the Supplier shall obtain written approval of the State of such subcontractor and each employee, as applicable to a particular Acquisition, of such subcontractor proposed for use by the Supplier. Any proposed subcontractor shall be identified by entity name, if required by the particular Acquisition, in the applicable proposal and shall include the nature of the services to be performed by that subcontractor. As part of the approval request, the Supplier shall provide a copy of a written agreement outlining the relevant flow downs to be executed by the Supplier and subcontractor setting forth that such subcontractor is bound by and agrees, as applicable, to perform the same covenants and be subject to the same conditions and make identical certifications to the same facts and criteria, as the Supplier under the terms of all applicable Contract documents. Supplier agrees that maintaining such agreement with any subcontractor and obtaining prior written approval by the State of any subcontractor and associated employees shall be a continuing obligation. If a subcontractor or any employee fails to meet service requirements, Supplier will notify the State and take commercially reasonable steps to replace such Subcontractor. If Supplier fails to replace such Subcontractor in a reasonable amount of time, the State retains the right to proceed with revocation of Agreement or the parties may mutually agree to an alternative arrangement via amendment.

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

9.5 This Agreement may not be assigned or transferred by Agency without EVS's prior written consent.

10 Background Checks and Criminal History Investigations

Supplier performs background checks at the time of hire and every five years thereafter. Prior to the commencement of any services, performance of background checks and criminal history investigations of the Supplier's employees and subcontractors who will be providing services may be required. If required, the Suppler agrees to provide the State with a description of the background check process to include any vendor's used to gather information. Supplier maintains a standard background check policy and, upon request, will provide a description of its screening process. Supplier will further attest that each employee and subcontractor providing services has passed Supplier's standard background check in accordance with Supplier's policy. Supplier's access to facilities, data and information may be withheld prior to completion of background verification acceptable to the State. The costs of additional background checks beyond Supplier's normal hiring practices shall be the responsibility of the Customer unless such additional background checks are required solely because Supplier will not provide verification of results of its otherwise acceptable normal background checks; in such an instance, Supplier shall pay for the additional background checks. Supplier will coordinate with the State and its employees to complete the necessary background checks and criminal history investigations. Supplier will not provide results of screens to Customers nor allow Customer to conduct its own screens of Supplier employees. Supplier requires its service suppliers to conduct background checks of their employees who will have access to Supplier or have a Supplier ID to access Supplier's systems. Should any employee or subcontractor of the Supplier who will be providing services under the Contract not be incompliance with Supplier's background check policy and acceptable as a result of the background check or criminal history investigation, the Customer may require replacement of the employee or subcontractor in question and, if no suitable replacement is made within a reasonable time, terminate the purchase order or other payment mechanism associated with the project or services.

11 Patents and Copyrights

Without exception, a product or deliverable price shall include all royalties or costs owed by the Supplier to any third party arising from the use of a patent, intellectual property, copyright or other property right held by such third party. Should an

Infringement Claim (as defined in Section 1.1) be made that any portion of a product or service provided by Supplier under the Contract infringes any United States patent or copyright in effect as of the date of this Agreement, Supplier shall enable each affected Customer to legally continue to use, or modify for use, the portion of the product or service at issue or replace such potentially infringing product, or re-perform or redeliver in the case of a service, with at least a functional non-infringing equivalent at its option and expense, either: (i) procure for Customer the right to continue using the Services; (ii) replace or modify the Services so that Customer's use becomes non-infringing, without materially impairing the functionality of the Services; or (iii) terminate Customer's use of the Services. Supplier's duty under this section shall extend to include any other product or service rendered materially unusable as intended due to replacement or modification of the product or service at issue. If the Supplier determines that none of these alternatives are reasonably available, the State shall return such portion of the product or deliverable at issue to the Supplier, upon written request, in exchange for a refund of the price paid for such returned goods as well as a refund or reimbursement, if applicable, of the cost of any other product or deliverable rendered materially unusable as intended due to removal of the portion of product or deliverable at issue. Any remedy provided under this section is not an exclusive remedy and is not intended to operate as a waiver of legal or equitable remedies because of acceptance of relief provided by Supplier. Supplier's obligations under this Section shall not apply with respect to an Infringement Claim which arises from: (1) unauthorized modification of the Services; (2) use of the Services in combination with data or software not provided by Supplier; or (3) materials or specifications provided by Customer.

12 Indemnification

12.1 Agency and EVS recognize that every business decision represents an assumption of risk and that neither party in furnishing Confidential Information, Data, or the Service to the other, underwrites or assumes the other's risk in any manner. To the extent not prohibited by laws applicable to the parties, such as Oklahoma Constitution article 10, Section 15 or any other applicable Oklahoma law, rule, or regulation, and others as referenced in Section 8 of Attachment A1, each party agrees to indemnify, defend and hold harmless ("Indemnify") the other party and its affiliates, and their directors, officers and employees (each, an "Indemnified Party"), from and against claims, demands, liabilities, suits, damages, expenses and costs, including reasonable attorneys', experts' and investigators' fees and expenses ("Claims") brought by third parties against the Indemnified Party and arising from the indemnifying party's, or its affiliates', directors', officers' or employees' ("Indemnifying Party") (i) any breach of the sections of this Agreement relating to confidentiality (including as a result of a Security Incident or Data Breach impacting State or Customer data), which shall not be subject to the

Limitation of Liability set forth in Section 12.4 ; (ii) breach of this Agreement, (iii) negligent or intentional, wrongful act or omission, (iv) subject to the requirements of subsection (c) below, any claim that the Services, when used for their intended purposes, infringe any third-party intellectual property rights, including any United States patent, copyright, trademark, or trade secret in effect as of the date of this Agreement (an "Infringement Claim"), or (iv) violation of applicable law.

12.2 Infringement

Should all or any part of the Services become, or in EVS' opinion be likely to become, the subject of an Infringement Claim, then Agency will permit EVS, at EVS' option and expense, to either: (i) procure for Agency the right to continue using the Services; (ii) replace or modify the Services so that Agency's use becomes non-infringing, without materially impairing the functionality of the Services; or (iii) terminate Agency's use of the Services. Upon any such termination, EVS shall return to Agency a prorated amount of any Fees prepaid by Agency with respect to the affected Services for the period after such termination takes effect. EVS' obligations shall not apply with respect to an Infringement Claim which arises from any of the following: (1) the use of the Services in a manner other than as permitted in this Agreement or as otherwise designed or intended; (2) any modification of, or connection to, the Services made by Agency that are not authorized by EVS; (3) the use, operation, or combination of the Services with software, data, equipment, or materials not provided by EVS; (4) Agency's continuance of allegedly infringing activity after being informed of the infringement and provided with modifications that would avoid the alleged infringement; or (5) any modifications to the Services in compliance with materials, data, information, directions, or specifications provided by, or on behalf of, Agency to EVS.

12.3 Notice and Cooperation

A. In connection with indemnification obligations under the Contract, the parties agree to furnish prompt written notice to each other of any third-party claim.

B. An Indemnifying Party will provide Indemnification only if: (i) the Indemnified Party notifies the Indemnifying Party promptly upon learning that the Claim might be asserted, provided that failure to timely provide such notice shall not diminish the Indemnifying Party's Indemnification obligations except to the extent the Indemnifying Party's ability to defend such claim is materially prejudiced by such failure or delay; (ii) the Indemnifying Party has sole control over the

defense of the Claim subject to the prior approval of the State Attorney General if the Supplier is the Indemnifying Party; and (iii) the Indemnified Party provides the Indemnifying Party with all reasonable assistance, information, and authority necessary for the Indemnifying Party to fulfill its obligations pursuant to this section.

C. As it relates to the State, any Customer affected by the Claim will reasonably cooperate with Supplier and defense of the claim to the extent its interests are aligned with Supplier should the Supplier take on defense of the third-party Claim as it relates to the Customer. Supplier shall use counsel reasonably experienced in the subject matter at issue and will not settle a claim without the written consent of the Customer being defended and where applicable for that Customer and Claim, the Attorney General of Oklahoma, which consent will not be unreasonably withheld or delayed.

13 Limitation of Liability

In no event shall Supplier or its officers, agents or employees be liable for loss of profits, or for indirect, special, incidental, punitive, or consequential damages arising out of or related to the Service or this Agreement, even if it has been advised of the possibility of such damages. Except for the indemnification obligations found herein, damages of any kind payable by Supplier shall not exceed the total amount paid by the Customer for the item of Service provided during the twelve (12) months immediately preceding the loss which causes the Customer's claim. Additionally, the Supplier will not be responsible for failure to provide software or Services if due to any cause or condition beyond the Supplier's control.

14 Termination for Cause

14.1 Supplier may terminate the Contract if (i) it has provided the State with written notice of material breach and (ii) the State fails to cure such material breach within thirty (30) days of receipt of written notice. If there is more than one Customer, material breach by a Customer does not give rise to a claim of material breach as grounds for termination by Supplier of the Contract as a whole. The State may terminate the Contract in whole or in part if (i) it has provided Supplier with written notice of material breach, and (ii) Supplier fails to cure such material breach within thirty (30) days of receipt of written notice. If there is more than one Customer, material breach by Supplier related to one Customer does not give rise to a claim of material breach as grounds for termination by Customer or other Customers of the Contract as a whole. 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.

14.2 Either party may terminate the Contract in whole or in part immediately without a thirty (30) day written notice to the alleged breaching party if (i) the alleged breaching party fails to comply with confidentiality, privacy, security, environmental or safety requirements applicable to that party's performance or obligations under the Contract and an opportunity to cure is not reasonably possible under the circumstances; (ii) that party's material breach is reasonably determined to be an impediment to the function of the State and detrimental to the State or to cause a condition precluding the thirty (30) day notice; or (iii) when the non-breaching party determines that an administrative error in connection with award of the Contract occurred prior to Contract performance.

14.3 The State may terminate the Contract if the scope includes PR Vendor services and the Supplier, or Supplier's employee, violate the lobbying clause. PR Vendor services is defined to include a contract for public relations (PR), marketing or communication services. The State may immediately terminate the Contract with no more than 10-day notice under this section.

14.4 If Supplier believes that Agency has breached an obligation of this Agreement impacting data, data or information treatment, privacy, security, confidentiality, or other similar critical provisions the Supplier may, at its option and reserving all other rights and remedies, terminate or suspend – indefinitely or otherwise – this Agreement and/or any Schedules, Exhibits, Addenda, or Attachments immediately upon notice to Agency.

14.5 Upon receipt of notice of a termination, Supplier shall promptly 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 Service 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 aside from those provided for elsewhere in this Contract. Such termination is not an exclusive remedy but is in addition to any other rights and remedies provided for by law. Any amount paid to Supplier in the form of prepaid fees that are unused when the Contract or certain obligations are terminated shall be refunded. Termination of the Contract under this section, in whole or in part, shall not relieve the Supplier of liability for claims arising under the Contract.

14.6 Supplier's actual failure to perform its obligations under the Contract; Supplier's inability to pay its debts when due; assignment for the benefit of Supplier's creditors; or voluntary or involuntary appointment of a receiver or filing of bankruptcy of Supplier shall constitute a material breach of the Supplier's obligations, which may result in partial or whole termination of the Contract. This subsection is not intended as an exhaustive list of material breach conditions. Termination may also result from other instances of failure to adhere to the Contract provisions and for other reasons provided for by applicable law, rules or regulations; without limitation, OAC 260:115-9-1 is an example.

15 Termination for Convenience

15.1 EVS may suspend or terminate this Agreement or any Addenda, Exhibit, Attachment, or Schedule(s), at any time upon twelve (12) months prior written notice to the State.

15.2 The State may terminate the Contract, in whole or in part, for convenience if it is determined that termination is in the State's best interest. In the event of a termination for convenience, Supplier will be provided at least thirty (30) days' written notice of termination. Any partial termination of the Contract shall not be construed as a waiver of, and shall not affect, the rights and obligations of any party regarding portions of the Contract that remain in effect.

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

16 Suspension of Supplier

16.1 Supplier may be subject to Suspension without advance notice and may additionally be suspended from activities under the Contract if Supplier fails

to comply with confidentiality, privacy, security, environmental or safety requirements applicable to Supplier's performance or obligations under the Contract.

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

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

17 Certification Regarding State Employees Prohibition From Fulfilling Services

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

18 Force Majeure

18.1 Either party shall not be liable to the other for any delay, or interruption in performance, as to any obligations hereunder resulting from fire or other similar casualty, act of God, strike or labor dispute, war or other violence, governmental emergency orders, judicial or governmental action, emergency regulations, sabotage, riots, vandalism, electrical failure, major computer hardware or software failures, equipment delivery delays, acts of third parties, delays or interruptions in performance beyond its reasonable control, or any law, order or requirement of any governmental agency or authority provided the party experiencing the force majeure event has prudently and promptly acted to take any and all steps within the party's control to ensure continued performance and to shorten duration of the event. If a party's performance of its obligations is materially hindered as a result of a force majeure event, such

party shall promptly notify the other party of its best reasonable assessment of the nature and duration of the force majeure event and steps it is taking, and plans to take, to mitigate the effects of the force majeure event. The party shall use commercially reasonable best efforts to continue performance to the extent possible during such event and resume full performance as soon as reasonably practicable.

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

18.3 Notwithstanding the foregoing or any other provision in the Contract, (i) the following are not a force majeure event under the Contract: (a) shutdowns, disruptions or malfunctions in Supplier's system or any of Supplier's telecommunication or internet services to the extent such events are within Supplier's reasonable control or result from Supplier's failure to maintain commercially reasonable business continuity measures or (b) the delay or failure of Supplier or subcontractor personnel to perform any obligation of Supplier hereunder unless such delay or failure to perform is itself by reason of a force majeure event and (ii) no force majeure event modifies or excuses Supplier's obligations related to confidentiality, indemnification, data security or breach notification obligations set forth herein.

19 Security of Property and Personnel

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

20 Miscellaneous

20.1 Transition Services

If transition services are needed at the time of Contract expiration or termination, Supplier shall provide such services on a month-to-month basis, at the contract rate or other mutually agreed rate as formally agreed upon in a mutual signed amendment to the Contract. Such amendment shall outline transition duties, expectations, terms and conditions, length of performance, and costs that may be associated with such a transition or wrap-up. Supplier shall provide a proposed transition plan, upon reasonable request, and reasonably cooperate with any successor supplier and with establishing a mutually agreeable transition plan. Failure to cooperate may be documented as poor performance of Supplier. Nothing in this Section shall require Supplier to provide Services out of Scope of Contract, for free, or to disclose or shared Supplier's Confidential Information, other proprietary business information, Data, Information, or the Services to any successor supplier.

20.2 Publicity

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

20.3 Mutual Responsibilities

A. No party to the Contract grants the other the right to use any trademarks, trade names, other designations in any promotion or publication without the express written consent by the other party.

B. The Contract is a non-exclusive contract and each party is free to enter into similar agreements with others.

C. The Customer and Supplier each grant the other only the licenses and rights explicitly specified in the Contract and all other rights and interests are expressly reserved.

D. The Customer and Supplier shall reasonably cooperate with each other during a transition up until termination or expiration of the Contract. Nothing in this provision shall require Supplier to provide free Services to Customer or any other supplier nor shall it require Supplier to provide Services, Data, Information, or its own Confidential Information to any other supplier, nor shall Customer be permitted to share such items with any other supplier. Notwithstanding the foregoing, upon termination or expiration of the Contract and request from Customer, Supplier shall promptly return to Customer or destroy in compliance with Attachment D, or at Customer's direction provide in a commercially reasonable and commonly used electronic format, all Customer Data in Supplier's possession, custody, or control, and shall not withhold such Customer Data due to any dispute between the parties. The foregoing shall not be construed as to prevent Supplier from retaining the minimum amount of Customer Data necessary to comply with applicable audit or regulatory requirements.

E. Except as otherwise set forth herein, where approval, acceptance, consent, or similar action by a party is required under the Contract, such action shall not be unreasonably delayed or withheld.

20.4 Entire Agreement

The Contract documents taken together as a whole constitute the entire agreement between the parties. The Contract documents include this Contract, any Amendments to this Contract, and any successful bid as may be amended or limited through negotiation, Addenda, Schedules, Exhibits, Attachments, Statements of Work, or Purchase Orders. No statement, promise, condition, understanding, inducement or representation, oral or written, expressed or implied, which is not contained in a Contract document shall be binding or valid. The Supplier's certifications, including any completed electronically, are incorporated by reference into the Contract. For the convenience of the parties, copies of this Agreement and Schedules hereof may be executed in two or more counterparts and signature pages exchanged by facsimile, email or other means of electronic transmission. The parties intend that counterpart copies signed and exchanged as provided in the preceding sentence shall be fully binding as an original handwritten executed copy hereof and thereof and all of such copies together shall constitute one instrument.

20.5 Failure to Enforce.

In addition to Section 14.3 in Attachment A1, failure by the Supplier at any time to enforce a provision of, or exercise a right under, the Contract shall not

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

ATTACHMENT C

AGENCY TERMS

Intentionally left blank

ATTACHMENT D

STATE OF OKLAHOMA INFORMATION TECHNOLOGY TERMS

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

1 DEFINITIONS

1.1 **Customer Data** means all data supplied by or on behalf of a Customer in connection with the Contract, excluding any Confidential Information of Supplier, the Services, Data, or Information. Customer Data includes both Non-Public Data and Personal Data.

1.2 **Data Breach** means the unauthorized access or the reasonable suspicion of unauthorized access, by an unauthorized person that results in the use, destruction, loss, alteration, disclosure, or theft of Customer Data.

1.3 **Host** includes the terms Hosted or Hosting and means the accessing, processing or storing of Customer Data.

1.4 **Intellectual Property Rights** means the worldwide legal rights or interests evidenced by or embodied in any idea, design, concept, personality right, method, process, technique, apparatus, invention, discovery or improvement including any patents, trade secrets and know-how; any work of authorship including any copyrights, neighboring rights; any trademark, service mark, trade dress, trade name or other indicia of source or origin; domain name registrations; and any other proprietary or similar rights. Intellectual Property Rights of a party also includes all worldwide legal rights or interests that the party may have acquired by assignment or license with the right to grant sublicenses. Foregoing. For the avoidance of doubt the Service and Data are proprietary to Supplier and all rights to the Service and Data are proprietary to and reserved by Supplier and shall only ever be considered or treated as Supplier's Intellectual Property and Supplier shall be the only party under this Contract with Intellectual Property Rights thereto.

1.5 **Non-Public Data** means Customer Data, other than Personal Data, that is not subject to distribution to the public as public information. It is deemed to be sensitive and confidential by Customer because it contains information that is exempt by statute, ordinance or administrative rule from access by the general public as public information. Non-Public Data includes any data deemed confidential pursuant to the Contract, otherwise identified by Customer as Non-Public Data, or that a reasonable person would deem confidential.

1.6 **Personal Data** means Customer Data that contains 1) any combination of an individual's name, social security numbers, driver's license, state/federal identification number, account number, credit or debit card number and/or 2) data subject to protection under a federal, state or local law, rule, regulation or ordinance.

1.7 **Security Incident** means the attempted or successful unauthorized access, use, disclosure, modification, loss, theft, or destruction of information or interference with the Hosted environment used to perform the services.

1.8 **Supplier** means the Bidder with whom the State enters into the Contract awarded pursuant to the Solicitation or the business entity or individual that is a party to the Contract with the State. A Supplier with whom the State enters into an awarded Contract shall also be known as a Contractor.

Supplier Intellectual Property means all tangible or intangible items or things, including the Intellectual Property Rights therein, created or developed by Supplier in relation to the Services, Data, Information, and Supplier Confidential Information.

1.9 **Third Party Intellectual Property** means the Intellectual Property Rights of any third party that is not a party to the Contract, and that is not directly or indirectly providing any goods or services to a Customer under the Contract

2 TERMINATION OF MAINTENANCE AND SUPPORT SERVICES

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

2.1 Customer removes the product for which the services are provided, from productive use; or,

2.2 The location at which the services are provided is no longer controlled by Customer (for example, because of statutory or regulatory changes or the sale or closing of a facility).

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

3 COMPLIANCE AND ELECTRONIC AND INFORMATION TECHNOLOGY ACCESSIBILITY

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

including but not limited to a statement of work, riders, agreement, purchase order or Addendum.

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

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

4.1 Any disk drives and memory cards purchased with or included for use in leased or purchased products under the Contract remain the sole and exclusive property of the Customer.

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

5 OFFSHORE SERVICES

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

6 COMPLIANCE WITH TECHNOLOGY POLICIES

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

Supplier's employees and subcontractors shall adhere to the applicable State IT Standards, policies, procedures and architectures as set forth at https://oklahoma.gov/omes/services/information-services.html or as otherwise provided by the State.

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

7 EMERGING TECHNOLOGIES

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

8 EXTENSION RIGHT

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

9 SOURCE CODE ESCROW

For the avoidance of doubt, the Parties acknowledge and agree that this Agreement does not contemplate Supplier custom building products for the State and therefore this provision is not applicable to the current Agreement. Pursuant to 62 O.S. § 34.31, if customized computer software is developed or modified exclusively for a State agency, the Supplier has a continuing obligation to comply with such law and place the source code for such software and any modifications thereto into escrow with an independent third-party escrow agent. Supplier shall pay all fees charged by the escrow agent and enter into an escrow agreement, the terms of which are subject to the prior written approval of the State, including terms that provide the State receives ownership of all escrowed source code upon the occurrence of any of the following:

9.1 A bona fide material default of the obligations of the Supplier under the agreement with the applicable Customer;

9.2 An assignment by the Supplier for the benefit of its creditors;

9.3 A failure by the Supplier to pay, or an admission by the Supplier of its inability to pay, its debts as they mature;

9.4 The filing of a petition in bankruptcy by or against the Supplier when such petition is not dismissed within sixty (60) days of the filing date;

9.5 The appointment of a receiver, liquidator or trustee appointed for any substantial part of the Supplier's property;

9.6 The inability or unwillingness of the Supplier to provide the maintenance and support services in accordance with the agreement with the agency;

9.7 Supplier's ceasing of maintenance and support of the software; or Such other condition as may be statutorily imposed by the future amendment or enactment of applicable Oklahoma law.

10 COMMERCIAL OFF THE SHELF SOFTWARE OR SUPPLIER TERMS

If Supplier specifies terms and conditions or clauses in an electronic license, subscription, maintenance, support or similar agreement, including via a hyperlink or uniform resource locator address to a site on the internet, that conflict with the terms of this Contract, the additional terms and conditions or conflicting clauses shall not be binding on the State and the provisions of this

Contract shall prevail. Further, no such terms and conditions or clauses shall expand the State's or Customer's liability or reduce the rights of Customer or the State.

11 OWNERSHIP RIGHTS

The Service and the Data are proprietary to Supplier; and all rights to the Service and Data are proprietary to and reserved by Supplier. The parties mutually agree the State r does not make a claim of ownership to the existing Intellectual Property of Supplier or Third Party Intellectual Property.

12 INTELLECTUAL PROPERTY OWNERSHIP TO WORK PRODUCT

12.1 Terms related to the development of new or customized software are not included in this Master Agreement. At such time as Supplier and Customer agree to work involving such development, the parties agree to negotiate applicable intellectual property provisions.

13 HOSTING SERVICES

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

14 CHANGE MANAGEMENT

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

15 SERVICE LEVEL DEFICIENCY

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

16 OWNERSHIP OF IT AND TELECOMMUNICATION ASSETS

Notwithstanding any other provision in the Contract and pursuant to the Oklahoma Information Technology Consolidation and Coordination Act, all information technology and telecommunication assets and contracts on behalf of appropriated agencies of the State belong to OMES-IS. OMES-IS allows other State agencies to use the assets while retaining ownership and the right to reassign the assets, at no additional cost, upon written notification to Supplier. For the avoidance of doubt, this provision applies to the relationship between OMES and OESC and ownership of its agency's technology or telecommunication assets, and shall in no way apply to Supplier or ownership or use of, or rights to reassign, Supplier's Services or Data, and Supplier's Services and Data - including the use of or access to such Services and Data - shall not be considered 'assets' under this provision.

17 CUSTOMER DATA

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

17.2 Customer will be responsible for the accuracy and completeness of all Customer Data provided to Supplier by Customer. Customer shall retain exclusive ownership of rights, title, and interest in Customer Data. Non-Public Data and Personal Data shall be deemed to be Customer's confidential information. Supplier shall restrict access to Customer Data to their employees with a need to know (and advise such employees of the confidentiality and non-disclosure obligations assumed herein).

17.3 Supplier shall promptly notify the Customer upon receipt of any requests from unauthorized third parties which in any way might reasonably require access to Customer Data or Customer's use of the Hosted environment. Supplier shall notify the Customer by the fastest means available and also in writing pursuant to Contract notice provisions and the notice provision herein. Except to the extent required by law, Supplier shall not respond to subpoenas, service or process, Freedom of Information Act or other open records requests, and other legal request related to Customer without first notifying the Customer and obtaining the Customer's prior approval, which shall not be unreasonably withheld, of Supplier's proposed responses. Supplier agrees to provide its completed responses to the Customer with adequate time for Customer review, revision and approval.

17.4 Supplier will use commercially reasonable efforts to prevent the loss of or damage to Customer Data in its possession and will maintain commercially reasonable back-up procedures and copies to facilitate the reconstruction of any Customer Data that may be lost or damaged by Supplier. Supplier will promptly notify Customer of any loss, damage to, or unauthorized access of Customer Data. Supplier will use commercially reasonable efforts to reconstruct any Customer Data that has been lost or damaged by Supplier as a result of its negligence or willful misconduct. If Customer Data is lost or damaged for reasons other than as a result of Supplier's negligence or willful misconduct, Supplier, at

the Customer's expense, will, at the request of the State, use commercially reasonable efforts to reconstruct any Customer Data lost or damaged.

18 DATA SECURITY

18.1 Supplier will use commercially reasonable efforts, consistent with industry standards, to provide security for the Hosted environment and Customer Data and to protect against both unauthorized access to the Hosting environment, and unauthorized communications between the Hosting environment and the Customer's browser. Supplier shall implement and maintain appropriate administrative, technical and organizational security measures to safeguard against unauthorized access, disclosure or theft of Personal Data and Non-Public Data. Such security measures shall be in accordance with recognized industry practice and not less stringent than the measures the service provider applies to its own personal data and non-public data of similar kind.

18.2 All Personal Data and Non-public Data shall be encrypted at rest and in transit with controlled access. Unless otherwise stipulated, the service provider is responsible for encryption of Personal Data. All Personal Data and Non-Public Data shall be subject to controlled access. Any stipulation of responsibilities shall be included in a Statement of Work and will identify specific roles and responsibilities.

18.3 Supplier represents and warrants to the Customer that the Hosting equipment and environment will be routinely checked with a commercially available, industry standard software application with up-to-date virus definitions. Supplier will regularly update the virus definitions to ensure that the definitions are as up-to-date as is commercially reasonable. Supplier will promptly purge all viruses discovered during virus checks. If there is a reasonable basis to believe that a virus may have been transmitted to Customer by Supplier, Supplier will promptly notify Customer of such possibility in a writing that states the nature of the virus, the date on which transmission may have occurred, and the means Supplier has used to remediate the virus. Should the virus propagate to Customer's IT infrastructure, Supplier is responsible for costs incurred by Customer for Customer to remediate the virus.

18.4 At no time shall any Customer Data or processes – that either belong to or are intended for the use of the State - be copied, disclosed, or retained by Supplier or any party related to Supplier for subsequent use in any transaction that does not include the State unless otherwise agreed to by the State.

18.5 Supplier shall provide its services to Customer and its users solely from data centers in the U.S. Storage of Customer Data at rest shall be located solely in data centers in the U.S. Supplier shall not allow its personnel or contractors to store Customer Data on portable devices, including personal computers, except for devices that are used and kept only at its U.S. data centers. Supplier shall permit its personnel and contractors to access Customer Data remotely only as required to fulfill Supplier's obligations under the Contract.

18.6 Supplier shall allow the Customer to audit conformance to the Contract terms. The Customer may perform this audit or contract with a third party at its discretion and at Customer's expense. Notice will be provided to the Supplier to allow for at a minimum 2 weeks to accommodate Customer.

18.7 Supplier shall perform an independent audit of its data centers at least annually at its expense and provide a redacted version of the audit report upon request. Supplier may remove its proprietary information from the redacted version. A Service Organization Control (SOC) 2 audit report or approved equivalent sets the minimum level of a third-party audit.

18.8 Any remedies provided are not exclusive and are in addition to other rights and remedies available under the terms of the Contract, at law or in equity.

19 SECURITY ASSESSMENT

19.1 The State requires any entity or third-party Supplier Hosting Oklahoma Customer Data to submit to a State Certification and Accreditation Review process to assess initial security risk. Supplier submitted to the review and met the State's minimum security standards at time the Contract was executed. Failure to maintain the State's minimum security standards during the term of the contract, including renewals, constitutes a material breach. Upon request, the Supplier shall provide updated data security information in connection with a potential renewal. If information provided in the security risk assessment changes, Supplier shall promptly notify the State and include in such notification the updated information; provided, however, Supplier shall make no change that results in lessened data protection or increased data security risk. Failure to provide the notice required by this section or maintain the level of security required in the Contract constitutes a material breach by Supplier and may result in a whole or partial termination of the Contract.

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

20 SECURITY INCIDENT OR DATA BREACH NOTIFICATION

20.1 Supplier shall inform Customer of any Security Incident or Data Breach.

20.2 Supplier may need to communicate with outside parties regarding a Security Incident, which may include contacting law enforcement, fielding media inquiries and seeking external expertise as mutually agreed upon, defined by law or contained in the Contract. If a Security Incident involves Customer Data, Supplier will coordinate with Customer prior to any such communication.

20.3 Supplier shall report a Security Incident to the Customer identified contact set forth herein within five (5) days of discovery of the Security Incident or within a shorter notice

period required by applicable law or regulation (i.e., HIPAA requires notice to be provided within 24 hours).

20.4 Supplier shall maintain processes and procedures to identify, respond to and analyze Security Incidents; (ii) make summary information regarding such procedures available to Customer at Customer's request, (iii) mitigate, to the extent practicable, harmful effects of Security Incidents that are known to Vendor; and (iv) documents all Security Incidents and their outcomes.

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

21 DATA BREACH NOTIFICATION AND RESPONSIBILITIES

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

21.1 Supplier shall (1) cooperate with Customer as reasonably requested by Customer to investigate and resolve the Data Breach, (2) promptly implement necessary remedial measures, if necessary, and (3) document responsive actions taken related to the Data Breach, including any post-incident review of events and actions taken to make changes in business practices in providing the services, if necessary.

21.2 Unless otherwise stipulated, if a Data Breach is a direct result of Supplier's breach of its obligation to encrypt Personal Data and Non-Public Data or otherwise prevent its release, Supplier shall bear the costs associated with (1) the investigation and resolution of the Data Breach; (2) notifications to individuals, regulators or others required by state law; (3) credit monitoring services required by state or federal law; (4) a website or toll-free numbers and call center for affected individuals required by state law – all not to exceed the agency per record per person cost calculated for data breaches in the United States on the most recent Cost of Data breach Study: Global Analysis published by the Ponemon Institute at the time of the data breach; and (5) complete all corrective actions as reasonably determined by Supplier based on root cause.

21.3 If a Data Breach is a direct result of Supplier's breach of its obligations to encrypt Personal Data and Non-Public Data or otherwise prevent its release, Supplier shall indemnify and hold harmless the Customer against all penalties assessed to Indemnified Parties by governmental authorities in connection with the Data Breach.

22 SUPPLIER REPRESENTATIONS AND WARRANTIES

Supplier represents and warrants the following, to the best of its knowledge:

22.1 The product and services provided in connection with Hosting services do not infringe a third party's patent or copyright or other intellectual property rights.

22.2 Supplier will protect Customer's Non-Public Data and Personal Data from unauthorized dissemination and use with the same degree of care that each such party uses to protect its own confidential information and, in any event, will use no less than a reasonable

degree of care in protecting such confidential information.

22.3 The execution, delivery and performance of the Contract and any ancillary documents and the consummation of the transactions contemplated by the Contract or any ancillary documents by Supplier will not violate, conflict with, or result in a breach of any provision of, or constitute a default (or an event which, with notice or lapse of time or both, would constitute a default) under, or result in the termination of, any written contract or other instrument between Supplier and any third parties retained or utilized by Supplier to provide goods or services for the benefit of the Customer.

22.4 Supplier shall not knowingly upload, store, post, e-mail or otherwise transmit, distribute, publish or disseminate to or though the Hosting environment any material that contains software viruses, malware or other surreptitious code designed to interrupt, destroy or limit the functionality of any computer software or hardware or telecommunications equipment or circumvent any "copy-protected" devices, or any other harmful or disruptive program.

23 INDEMNITY

Refer to Attachment B, Section 12.

24 TERMINATION, EXPIRATION AND SUSPENSION OF SERVICE

24.1 During any period of service suspension, Supplier shall not take any action to intentionally disclose, alter or erase any Customer Data unless otherwise required by Customer or applicable law.

24.2 Supplier shall not take any action to intentionally erase any Customer Data for a period of thirty (30) days after the effective date of termination or expiration. After such thirty (30) day period, Supplier shall, unless legally prohibited or otherwise required by applicable law, regulation, court order, company policies or procedures, or internal audit/backup requirements, delete all Customer Data in its systems or otherwise in its possession or under its control. Notwithstanding the foregoing, Supplier may retain one copy of such data to the extent required to comply with applicable legal, regulatory, or audit requirements, provided such retained data remains subject to the confidentiality and security obligations of this Agreement. If the services involve prescreen data, Customer may be allowed to retain one (1) copy for up to three (3) years solely for audit and regulatory purposes, after which it must be securely destroyed.

24.3 The State shall be entitled to any post-termination or expiration assistance generally made available by Supplier with respect to the services, subject to mutually agreed fees for any custom or non-standard support.

24.4 Disposal by Supplier of Customer Data in all of its forms shall be performed in a secure manner. Data shall be permanently deleted and shall not be recoverable, using commercially reasonable procedures consistent with those issued by the Federal Trade Commission (FTC) in connection with the disposal of consumer report information and/or NIST-approved methods. Certificates of destruction shall be provided to Customer

within thirty (30) calendar days of Supplier's receipt of a written request for disposal of data, provided such data is classified as Class 5 (Consumer Protected). Notwithstanding the foregoing, Supplier may retain one copy of such data to the extent required to comply with applicable legal, regulatory, or audit requirements, provided such retained data remains subject to the confidentiality and security obligations of this Agreement.

25 GENERAL INFORMATION SECURITY REQUIREMENTS

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

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

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

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

26 HIPAA REQUIREMENTS (if applicable)

26.1 In the event that Contractor in the performance of the Services under the Agreement receives from or on behalf of Consumer protected health information, including electronic protected health information (collectively, "**PHI**" unless the context provides otherwise) or such PHI is used, accessed, maintained or transmitted by EVS on Client's behalf, the parties agree to protect the confidentiality of such PHI in accordance with the Health Insurance Portability and Accountability Act of 1996 ("**HIPAA**"), the Health Information Technology for Economic and Clinical Health Act in Public Law 111-5 (the "**HITECH Act**"), and the regulations promulgated thereto (collectively, the "**HIPAA Rules**"), which include, as amended from time to time, (i) the privacy standards, requirements and specifications promulgated by the Secretary at 45 C.F.R. Parts 160 and 164 subparts A and E (the "**Privacy Rule**"), and (ii) the security standards, requirements and specifications promulgated by the Secretary at 45 C.F.R. Parts 160, 162 and 164 subparts A and C (the "**Security Rule**").

26.2

26.3 If applicable, Contractor will sign and adhere to a Business Associate Agreement (BAA) as negotiated by the parties. 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, as applicable. Failure to comply with the requirements of this standard may result in funding being withheld from Contractor, and/or full audit and inspection of Contractor's security compliance as it pertains to this contract.

26.4 Business Associate Terms Definitions:

a. Terms used, but not otherwise defined, in this BAA shall have the same meaning as those terms in 45 CFR 160.103, 164.304 and 164.501 and shall be deemed to be modified to reflect any changes made to such terms from time to time as defined in the HIPAA Rules.

26.5 Obligations of Business Associate: In connection with the performance of its obligations under the Agreement, EVS agrees to:

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

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

c. report to Covered Entity any use or disclosure of PHI not provided for by the Agreement of which EVS becomes aware, including any security incident;

d. in accordance with 45 C.F.R. 164.502(e)(1) and 164.308(b), if applicable, require that any agents, including subcontractors to whom Contractor provides PHI received from, or created or received by Contractor on behalf of Covered Entity agrees to the same restrictions, conditions, and requirements that apply to the Contractor with respect to such PHI;

e. report to Covered Entity any use or disclosure of PHI that is not permitted under this Agreement of which Contractor becomes aware, including any security incident, as soon as reasonably practicable;

f. make available any PHI it maintains in a Designated Record Set in accordance with 45 C.F.R. 164.524;

g. make amendments to any PHI it maintains in a Designated Record Set in accordance with 45 C.F.R. 164.526;

h. Make available the information required to provide an accounting of disclosures, in accordance with 45 C.F.R. 164.528; make its internal practices, books, and records related to the use and disclosure of PHI received from or created or received by Contractor on behalf of Covered Entity available to the Secretary, for the purpose of determining Contractor's compliance with the HIPAA Rules.

26.6 Permitted Uses and Disclosures of PHI by Business Associate: Except as otherwise limited in a BAA, Contractor may:

a. use PHI for its proper management and administration of Contractor or to carry out the legal responsibilities of Contractor;

b. use or disclose PHI for its proper management and administration of Contractor, provided that; (i) the disclosures required by law; or (ii) Contractor 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 notifies Contractor of any instances of which it is aware in which the confidentiality of the PHI has been breached; and

c. use or disclose PHI to perform functions, activities, or services for, or on behalf of, Covered Entity as specified in the Agreement, provided that such use or disclosure would not violate the Privacy Rule if done by Client.

26.7 Obligations of Covered Entity

a. Covered Entity shall notify Contractor 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 Contractor's use or disclosure of PHI.

b. Covered Entity shall notify Contractor 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 Contractor's use or disclosure of PHI.

c. Covered Entity shall promptly notify Contractor of any limitation(s) in the notice of privacy practices of Covered Entity under 45 CFR 164.520, as well as any changes to such notice, to the extent that such limitation may affect Contractor's use or disclose PHI.

26.8 Permissible Requests by Covered Entity. Except as otherwise permitted herein, Covered Entity shall not request Contractor to use or disclose PHIU in any manner that would not be permissible under the Privacy Rule if done by the Covered Entity.

26.9 Term and Termination:

a. Term. The BAA shall be effective as of the relevant effective date, and shall terminate either: (i) when all of the PHI provided by Covered Entity to Contractor, or created or received by Contractor on behalf of Covered Entity, is destroyed or returned to Covered Entity, or, if it is infeasible to return or destroy PHI, protections are extended to such information; or (ii) upon the termination of the Agreement for any reason, whichever is sooner.

b. Termination for Cause. Upon Covered Entity's knowledge of a material breach of the BAA by Contractor, Covered Entity shall provide a reasonable opportunity for Contractor to cure the breach or end the violation, and shall terminate the Agreement if Contractor fails to cure the breach or end the violation within the time specified by Covered Entity, or immediately terminate the Agreement if Contractor has breached a material term of the BAA and cure is not possible.

c. Effect of Termination. Except as provided herein, upon termination of the BAA Contractor shall, if feasible, return or destroy all PHI received from Covered Entity, or created or received by Contractor on behalf of Covered Entity. This provision

shall apply to PHI that is in the possession of subcontractors or agents of Contractor. Contractor shall retain no copies of the PHI. Notwithstanding, if Contractor determines that returning or destroying the PHI is not feasible, Contractor shall provide to Covered Entity notification of the same, and shall extend the protections of the BAA to such PHI and limit further uses and disclosures of such PHI to those purposes that make the return or destruction of the PHI infeasible, for so long as Contractor maintains such PHI. The respective rights and obligations of Contractor under this section shall survive the termination of the BAA.

27 42 C.F.R. PART 2 RELATED PROVISIONS

27.1 In the event that Contractor in the performance of the Services under the Agreement receives from or on behalf of Consumer protected health information, including electronic protected health information (collectively, "**PHI**" unless the context provides otherwise) or such PHI is used, accessed, maintained or transmitted by EVS on Client's behalf, such that Section 26 is triggered the parties also agree to comply with the following laws outlined below, as applicable, in addition to those in Section 20.

27.2 Confidentiality of Information. Contractor's employees and agents shall have access to private data to the extent necessary to carry out the responsibilities, limited by the terms of this Agreement. Contractor accepts the responsibilities for providing adequate administrative supervision and training to their employees and agents to ensure

compliance with relevant confidentiality, privacy laws, regulations and contractual provisions. No private or confidential data collected, maintained, or used shall be disseminated except as authorized by statute and by terms of this Agreement, whether during the period of the Agreement or thereafter. Furthermore, Contractor:

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

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

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

27.6 Agrees to, when applicable and to the extent within Contractor's control, use appropriate

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

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

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

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

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

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

28 DATA SECURITY

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

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

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

28.3 Redisclosure of Data. The Contractor agrees not to redisclose any information to a third

party not covered by the Agreement unless written permission by the State of Oklahoma agency is received and redisclosure is permitted under applicable law.

29 FEDERAL TAX INFORMATION REQUIREMENTS IRS PUBLICATION 1075

29.1 The provisions of Section 29 are inapplicable to the Services or parties under this Contract, however, in the event the Contract is modified to require such provisions, the following shall apply unless otherwise amended at that time.

29.2 PERFORMANCE: If Contractor takes possession or control of Federal Tax Information in performance of this contract, the Contractor agrees to, when applicable and to the extent within Contractor's control, comply with and assume responsibility for compliance by officers or employees with the following requirements:

29.3 All work will be performed under the supervision of the State of Oklahoma.

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

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

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

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

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

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

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

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

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

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

29.14 For purposes of this contract, the term "contractor" includes any officer or employee of the contractor with access to or who uses FTI, and the term "subcontractor" includes any officer or employee of the subcontractor with access to or who uses FTI.

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

30 CRIMINAL/CIVIL SANCTIONS

30.1 The provisions of Section 30 are inapplicable to the Services or parties under this Contract, however, in the event the Contract is modified to require such provisions, the following shall apply unless otherwise amended at that time:

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

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

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

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

30.6 Granting a contractor access to FTI must be preceded by certifying that each officer or employee understands the agency's security policy and procedures for safeguarding FTI. A contractor and each officer or employee must maintain their authorization to access FTI through annual recertification of their understanding of the agency's security policy and procedures for safeguarding FTI. The initial certification and recertifications must be documented and placed in the agency's files for review. As part of the certification and at least annually afterwards, a contractor and each officer or employee must be advised of the provisions of IRC sections 7213, 7213A, and 7431 (see IRS Publication 1075, Exhibit 4, Sanctions for Unauthorized Disclosure, and IRS Publication 1075, Exhibit 5, Civil Damages for Unauthorized Disclosure). The training on the agency's security policy and procedures provided before the initial certification and annually thereafter must also cover the incident response policy and procedure for reporting unauthorized disclosures and data breaches. For the initial certification and the annual recertifications, the contractor and each officer or employee must sign, either with ink or electronic signature, a confidentiality statement certifying their understanding of the security requirements.

31 INSPECTION

This Section 31 is inapplicable to the Services or parties under this Contract, however, in the event the Contract is modified to require such provisions, the following shall apply unless otherwise amended at that time. The IRS and the Agency, with 24-hour notice, shall have the right to send its inspectors into the offices and plants of the contractor to inspect facilities and operations performing any work with FTI under this contract for compliance with requirements defined in IRS Publication 1075. The IRS' right of inspection shall include the use of manual and/or automated scanning tools to perform compliance and vulnerability assessments of information technology (IT) assets that access, store, process or transmit FTI. Based on the inspection, corrective actions may be required in cases where the contractor is found to be noncompliant with FTI safeguard requirements.

32 SSA REQUIREMENTS

32.1 The provisions of Section 32 are applicable only to those relevant Services under this Contract, and the following shall apply to SSA data under those applicable Services.

32.2 PERFORMANCE: If Contractor takes possession or control of in SSA provided information in the performance of this contract, the contractor agrees to, where applicable and to the extent within Contractor's control comply with and assume responsibility for compliance by his or her employees with the following requirements:

32.3 All work will be done under the supervision of the State of Oklahoma.

32.4 Any SSA provided information made available shall be used only for carrying out the provisions of this Agreement. Information contained in such material shall be treated as confidential and shall not be divulged or made known in any manner to any person except as may be necessary in the performance of this contract. Inspection by or disclosure to anyone other than an officer or employee of the Contractor is prohibited.

32.5 All SSA provided information shall be accounted for upon receipt and properly stored before, during, and after processing. In addition, all related output and products will be given the same level of protection as required for the source material.

32.6 No work involving SSA provided information furnished under this contract shall be subcontracted without prior written approval by the applicable State of Oklahoma agency and the SSA.

32.7 The Contractor shall maintain a list of employees authorized access. Such list shall be provided upon request to the applicable State of Oklahoma agency or the SSA.

32.8 Contractor or agents may not legally process, transmit, or store SSA-provided information in a cloud environment without explicit permission from SSA's Chief Information Officer. Proof of this authorization shall be provided to the Contractor by the applicable State of Oklahoma agency prior to accessing SSA provided information.

32.9 Contractor shall provide security awareness training to all employees, contractors, and agents who access SSA-provided information. The training should be annual, mandatory, and certified by the personnel who receive the training. Contractor is also required to certify that each employee, contractor, and agent who views SSA-provided information certify that they understand the potential criminal, civil, and administrative sanctions or penalties for unlawful assess and/or disclosure.

32.10 Contractor shall require employees, contractors, and agents to sign a non-disclosure agreement, attest to their receipt of Security Awareness Training, and acknowledge the rules of behavior concerning proper use and security in systems that process SSA-provided information. Contractor shall retain non-disclosure attestations for at least five (5) to seven (7) years for each employee who processes, views, or encounters SSA-provided information as part of their duties.

32.11 The applicable State of Oklahoma agency shall provide the Contractor a copy of the SSA exchange agreement and all related attachments before initial disclosure of SSA data. Contractor is required to follow the terms of the applicable State of Oklahoma agency's data exchange agreement with the SSA. Prior to signing this Agreement, and thereafter at SSA's request, the applicable State of Oklahoma agency shall obtain from the Contractor a current list of the employees of such Contractor with access to SSA data and provide such list to the SSA.

32.12 Where the Contractor processes, handles, or transmits information provided to the applicable State of Oklahoma agency by SSA or has authority to perform on the agency's behalf, the applicable State of Oklahoma agency shall clearly state the specific roles and functions of the Contractor within the Agreement.

32.13 SSA requires all parties subject to this Agreement to exercise due diligence to avoid hindering legal actions, warrants, subpoenas, court actions, court judgments, state or Federal investigations, and SSA special inquiries for matters pertaining to SSA-provided information.

32.14 SSA requires all parties subject to this Agreement to agree that any Client-owned or subcontracted facility involved in the receipt, processing, storage, or disposal of SSA-provided information operate as a "de facto" extension of the Client and is subject to onsite inspection and review by the Client or SSA with prior notice.

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

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

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

32.18

33 CRIMINAL/CIVIL SANCTIONS

The provisions of Section 33 are inapplicable to the Services or parties under this Contract, however, in the event the Contract is modified to require such provisions, the following shall apply unless otherwise amended at that time.

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

33.1 Civil Remedies

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

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

c. the costs of the action together with reasonable attorney fees as determined by the court.

d. An action to enforce any liability created under 5 U.S.C. § 552a may be brought in the district court of the United States in the district in which the complainant resides, or has his principal place of business, or in which the records are situated, or in the District of Columbia, without regard to the amount in controversy, within two years from the date on which the cause of action arises, except that where parties subject to this Agreement have materially and willfully misrepresented any information required under this section to be disclosed to an individual and the information so misrepresented is material to establishment of the liability of the agency to the individual under 5 U.S.C. § 552a, the action may be brought at any time within two years after discovery by the individual of the misrepresentation. Nothing in this section shall be construed to authorize any civil action because of any injury sustained as the result of a disclosure of a record prior to September 27, 1975.

33.2 Criminal Penalties

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

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

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

34 CHILD SUPPORT FPLS REQUIREMENTS

34.1 Contractor, when applicable and to the extent within Contractor's control, and the applicable State of Oklahoma agency must comply with the security requirements established by the Social Security Act, the Privacy Act of 1974, the Federal Information Security Management Act of 2002 (FISMA), 42 United States Code (USC) 654(26), 42 UCS 654a(d)(1)-(5), the U.S. Department of Health and Human Services (HHS), the U.S. Department of Health and Human Services Administration of Children and Families Office of Child Support Enforcement Security Agreement and the Automated Systems for Child Support Enforcement: A Guide for States Section H Security and Privacy.

Contractor and applicable State of Oklahoma agency also agree to use Federal Parent Locator Service (FPLS) information and Child Support (CS) program information solely for the authorized purposes in accordance with the terms in this agreement. The information exchanged between state Child Support agencies and all other state program information must be used for authorized purposes and protected against unauthorized access to reduce fraudulent activities and protect the privacy rights of individuals against unauthorized disclosure of confidential information.

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

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

35 FERPA REQUIREMENTS

35.1 The provisions of Section 35 are inapplicable to the Services or parties under this Contract, however, in the event the Contract is modified to require such provisions, the following shall apply unless otherwise amended at that time.

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

36 CJIS REQUIREMENTS

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

36.2 The Entity or Affiliate acquiring the data or system is hereby ultimately responsible for compliance with the CJIS Security Policy and will be subject to an audit by the State of Oklahoma CJIS Systems Officer ("CSO") and the FBI CJIS Division's Audit Staff. Scheduling of any audit with Supplier is subject to a minimum of 2 weeks advanced notice, and will not conflict with other third party Supplier CJIS assessments.

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

36.4 DIRECTIVE CONCERNING ACCESS TO CRIMINAL JUSTICE INFORMATION AND TO HARDWARE OR SOFTWARE WHICH INTERACTS WITH CJI AND CERTIFICATION- The FBI CJIS Division provides state-of-the-art identification and information services to the local, state, tribal, federal, and international criminal justice communities for criminal justice purposes, as well as the noncriminal justice communities for noncriminal justice purposes.

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

36.6 In order to have access to CJI or to the aforesaid hardware or software, the vendor must be familiar with the FBI CJIS Security Policy version 6.0
.

36.7 This FBI Security Policy is located and may be downloaded at:

a. https://le.fbi.gov/file-repository/cjis_security_policy_v6-0_20241227.pdf

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

37 NOTICES

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

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

With a copy, which shall not constitute notice, to:
OMES Deputy General Counsel
3115 North Lincoln Blvd
Oklahoma City, Oklahoma 73105

Attachment E1 to

STATE OF OKLAHOMA CONTRACT WITH Equifax Workforce Solutions LLC.
RESULTING FROM SOLICITATION NO. EV00000579
Pricing Sheet

Solicitation Name:	
RFP #EV00000579	

Bidders Information	
Name	Equifax Workforce Solutions LLC
Contact Information	Roger Bishoproger.bishop@equifax.com

Instructions:

Overview

Supplier shall be compensated by a single, flat rate for products/services provided under this solicitation. The rate shall be inclusive of all Supplier costs. Supplier shall submit a proposed price for all products/services proposed which shall constitute the entire compensation due to the successful contractor for the products/services described in this solicitation, regardless of the difficulty, materials or equipment required, and shall include all applicable taxes, fees, overhead, profits, travel, and all other direct and indirect costs incurred or to be incurred by the supplier. **Cost proposal must be submitted in excel format.** The list of provided items is not all inclusive, if additional cost related items can be added to convey additional project costs, expand list as needed. If information for a specific item is not applicable, then insert "n/a" in that area.

Bidder has the option to break out the cost further into subtasks if they so desire.

Costs shall include complete development and maintenance of the project until it is turned over to the client. Costs shall also include training for the users of the system. ***If needed, additional lines can be added for an accurate cost submission. If additional lines are added, provide an explanation for the cost in column A, under hours used for the cost with the*** Include all value-added options, using the same format below, as a supplemental attachment to Exhibit 1. Mandatory Requrements.

Price and Cost

Job Description	**Initial Year**	**Optional Renewal year 1**	**Optional Renewal year 2**	**Optional Renewal year 3**	**Optional Renewal year 4**	**OTHER Fees**
Annual Cost (Up to 2M SSN searches annually)	$ 100,000.00	$ 120,000.00	$ 140,000.00	$ 160,000.00	$ 180,000.00	N/A
Monthly Cost (Up to 2M SSN searches monthly)	$ 8,333.33	$ 10,000.00	$ 11,666.67	$ 13,333.33	$ 15,000.00	N/A
~~Rate per SSN Submission (beyond 2M SSN searches annually)~~	$ 0.10	$ 0.11	$ 0.12	$ 0.13	$ 0.14	N/A
Hours Used	**# of hours**	**# of hours**	**# of hours**	**# of hours**	**# of hours**	**# of hours**
Implementation	N/A	N/A	N/A	N/A	N/A	N/A
Customization or Functionality						
(Web and Database Access,						
Queries, Staffing Plan)	N/A	N/A	N/A	N/A	N/A	N/A
price break for quantity)	N/A	N/A	N/A	N/A	N/A	N/A
Testing	N/A	N/A	N/A	N/A	N/A	N/A
year and ongoing)	N/A	N/A	N/A	N/A	N/A	N/A
a)Documentation/ User	N/A	N/A	N/A	N/A	N/A	N/A
or Other (Provide Details)	N/A	N/A	N/A	N/A	N/A	N/A
Total Hours	0	0	0	0	0	0
Total	**TBD**	**TBD**	**TBD**	**TBD**	**TBD**	N/A

Total Cost
$ -

Attachment E-3

UNIVERSAL MEMBERSHIP AGREEMENT
for
Equifax Verification Services for Social Services

("Agency" or "**Customer**"):
Agency's Address:
Effective date of this Universal Membership Agreement ("Effective Date"): (If blank, the Effective Date of this Universal Membership Agreement shall be the date of the last signature below).

This **Universal Membership Agreement** (the "**Agreement**"), effective as of the Effective Date, is entered into by and between Equifax Workforce Solutions LLC, a Missouri limited liability company and provider of Equifax Verification Services located at 11432 Lackland Road, St. Louis, Missouri 63146 ("**EVS**" or "**Supplier**"), and Agency.

RECITALS:

A. EVS operates a variety of services that can be used to learn information about an individual ("**Consumer**"), and offers various other services, directly or through other partners or entities within its family of companies, such as incarceration intelligence services which provide tip-and-lead or pointer data through Person Search ("**Person Search**") and/or Person Watch ("**Person Watch**") (collectively, the "**Services**"); and

B. Agency wishes to use the Service related to the Consumer and recent incarceration tip-and-lead or pointer information that comes from jails and/or other types of correctional facilities across the county.

NOW, THEREFORE, the parties agree as follows:

1. SCOPE OF THE AGREEMENT. This Agreement consists of the general terms set forth in the body of this Agreement, Exhibit 1, Exhibit 2, Exhibit 3, and each Schedule A executed by the parties which may contain additional terms. This Agreement is entered into pursuant to, and is subject to, the Master Agreement between the Agency and Supplier, and is not intended to constitute the entire agreement between the parties. In the event of a conflict between this Agreement and the Master Agreement, the terms of the Master Agreement will control unless expressly stated otherwise. If there is a conflict between the general terms and conditions of this Agreement and any Exhibit or Schedule, the provisions of the Exhibit or Schedule will govern and control. This Agreement specifically supersedes and replaces any agreement between the parties that predates this Agreement and which relates to the Service as provided in each Schedule A, even if the prior agreement contains an "entire agreement" or "merger" clause, and any such agreements are terminated.

2. EVS OBLIGATIONS. The Service(s) will provide Agency with automated access to certain incarceration data ("**Data**") and the Service(s) or other EVS services that may provide Agency with access to certain other information ("**Information**") as described in each Schedule A attached hereto.

3. AGENCY OBLIGATIONS.

a. Agency shall comply with the terms set forth in this Agreement, and each Exhibit and Schedule attached hereto.

b. Agency shall pay for the Services as set forth in each applicable Schedule. Applicable sales, use, privilege, or excise taxes shall be included in each invoice, except as otherwise exempted in the applicable Schedule.

c. Agency represents it (i) is administering a government funded benefit or program, (ii) has been given the legal authority to view the Data by the Consumer or by operation of law, and (iii) is requesting the Data in compliance with all laws.

d. Agency may use the Data and Information provided through the Service only as described in this Agreement. Agency may reproduce or store the Data and Information obtained from the Service solely for its own use in accordance with this Agreement, and will hold all Data and Information obtained from the Service under this Agreement in strict confidence and will not reproduce, reveal, or make it accessible in whole or in part, in any manner whatsoever, to any others unless permitted in this Agreement, required by law, or Agency first obtains EVS's written consent.

e. Agency acknowledges it shall employ decision making processes appropriate to the nature of the transaction and in accordance with industry standards and will use the Data and Information as part of its processes.

f. "**Processing**" means accessing (including access to view), transmitting, using, or storing the Services, and any Data or Information provided or obtained through the Services (the "**EVS Information**"). Agency may Process EVS Information from the United States, Canada, and the United States territories of American Samoa, Guam, the Northern Mariana Islands, Puerto Rico, and the U. S. Virgin Islands (collectively, the "**Permitted Territory**"). Agency must (i) notify EVS thirty (30) days prior to Processing EVS Information from a location outside of the Permitted Territory, in accordance with the notice requirements described in this Agreement; and (ii) sign an International Access and Use Addendum with EVS prior to Processing EVS Information from a location out of the Permitted Territory. EVS reserves the right to deny any such request for reasons including, without limitation, regulatory requirements, security concerns, or existing contractual obligations. Notwithstanding the foregoing, Agency is prohibited from Processing EVS Information from an Embargoed Country. "**Embargoed Country**" means any country or geographic region subject to comprehensive economic sanctions or embargoes administered by OFAC or the European Union.

g. Except as otherwise permitted in Section 4.b. below, Agency may not allow a third party service provider (hereafter "**Service Provider**") to access, use, or store the Data or Information on its behalf without first obtaining EVS's written permission and without the Service Provider first entering into a separate agreement with EVS.

h. In order to ensure compliance with this Agreement, applicable law and EVS policies, EVS may conduct reviews of Agency activities, from time to time, during normal business hours, at all locations containing relevant records, with respect to Agency's requests for Data

or Information and/or its use of Data or Information. Agency shall provide documentation within a reasonable time to EVS as reasonably requested for purposes of such review. Agency shall cooperate fully with any and all investigations by EVS of allegations of abuse or misuse of the Services and allow EVS to access its premises, records, and personnel for purposes of such investigations if EVS deems such access is necessary to complete such investigation(s). Agency agrees that any failure to cooperate fully and promptly in the conduct of any audit constitutes grounds for immediate suspension of the Service and/or termination of the Agreement, and (iii) shall promptly correct any discrepancy revealed by such investigation(s). Agency shall include the name and email address of the appropriate point of contact to whom such request should be made in the space provided below. Agency may change its contact information upon written notice:

Audit Contact Name	Audit Contact E-mail Address

i. Additional representations and warranties as may be set forth in each Schedule A.

4. DATA SECURITY. This Section 4 applies to any means through which Agency orders or accesses the Service including, without limitation, system-to-system, personal computer or the Internet. For the purposes of this Section 4, the term "**Authorized User**" means an Agency employee that Agency has authorized to order or access the Service and who is trained on Agency's obligations under this Agreement with respect to the ordering and use of the Service, and the Data provided through same, including Agency's obligations with respect to the access and use of Data.

a. Agency will, with respect to handling any Data or Information provided through the Service:

1. ensure that only Authorized Users can order or have access to the Service;
2. ensure that Authorized Users do not order Data or Information for personal reasons or provide Data or Information to any third party except as permitted by this Agreement;
3. inform Authorized Users that unauthorized access to Data may subject them to civil and criminal liability punishable by fines and imprisonment;
4. ensure that all devices used by Agency to order or access the Service are placed in a secure location and are accessible only by Authorized Users, and that such devices are secured when not in use through such means as screen locks, shutting power controls off, or other security procedures and controls which are standard practice in the data protection industry ("Industry Standard Practices"), for example compliance with ISO 27001 standards;
5. take all necessary measures to prevent unauthorized ordering of or access to the Service by any person other than an Authorized User for permissible purposes, including, without limitation, (i) limiting the knowledge of the Agency security codes, user names, User IDs, and any passwords Agency may use, to those individuals with a need to know. In addition, the User IDs must be unique to each person, and the sharing of User IDs or passwords is prohibited;
6. change Agency passwords at least every ninety (90) days or sooner if Agency suspects an unauthorized person has learned the password; and perform at a minimum, quarterly entitlement reviews to recertify and validate Authorized User's access privileges and disable the account of any Agency user who is no longer responsible for accessing the Service;
7. adhere to all security features in the software and hardware Agency uses to order or access the Services, including the use of IP restriction;
8. implement secure authentication practices when providing User ID and passwords to Authorized Users, including but not limited to using individually assigned email addresses and not shared email accounts;
9. in no event access the Services via any unregistered wireless hand-held communication device, that have not gone through Agency's device enrollment, access, and authentication process. Such process shall be reviewed and approved by EVS prior to allowing access to Services via any hand-held communication device;
10. not use non-agency owned assets such as personal computer hard drives or portable and/or removable data storage equipment or media (including but not limited to laptops, zip drives, tapes, disks, CDs, and DVDs) to store the Data or Information. In addition, Data and Information must be encrypted when not in use and all printed Data and Information must be stored in a secure, locked container when not in use, and must be completely destroyed when no longer needed by cross-cut shredding machines (or other equally effective destruction method) such that the results are not readable or useable for any purpose. In either case, Industry Standard Practices for the type of Data and Information received from EVS must be employed;
11. if Agency sends, transfers or ships any Data or Information, encrypt the Data and Information using the following minimum standards, which standards may be modified from time to time by EVS: FIPS 140-2 compliant ciphers and algorithms;
12. not ship hardware or software between Agency's locations or to third parties without deleting all of EVS's Confidential Information, Agency number(s), security codes, User IDs, passwords, Agency user passwords, and any Consumer information, or Data;
13. monitor compliance with the obligations of this Section 4, and immediately notify EVS if Agency suspects or knows of any unauthorized access or attempt to access the Service, including, without limitation, a review of EVS invoices for the purpose of detecting any unauthorized activity;
14. if, subject to the terms of this Agreement, Agency uses a Service Provider to establish access to the Service, be responsible for the Service Provider's use of Agency's user names, security access codes, or passwords, and Agency will ensure the Service Provider safeguards Agency's security access code(s), User IDs, and passwords through the use of security requirements that are no less stringent than those applicable to Agency under this Section 4;

15. use Industry Standard Practices to assure data security when disposing of any Data and Information obtained from EVS. Such efforts must include the use of those procedures issued by the federal regulatory agency charged with oversight of Agency's activities (e.g. the Federal Trade Commission, the applicable banking or credit union regulator) applicable to the disposal of consumer report information or records;

16. use Industry Standard Practices to secure Data and Information when stored on servers, subject to the following requirements: (i) servers storing Data and Information must be separated from the Internet or other public networks by firewalls which are managed and configured to meet industry accepted best practices, (ii) Data and Information must be protected through multiple layers of network security, including but not limited to, industry-recognized firewalls, routers, and intrusion detection/prevention devices (IDS/IPS), (iii) access (both physical and network) to systems storing Data and Information must be secure, which must include authentication and passwords that are changed at least every ninety (90) days; and (iv) all servers must be kept current and patched on a timely basis with appropriate security-specific system patches, as they are available;

17. not allow Data or Information to be displayed via the Internet unless utilizing, at a minimum, a three-tier architecture configured in accordance with industry best practices;

18. use Industry Standard Practices to establish procedures and logging mechanisms for systems and networks that will allow tracking and analysis in the event there is a compromise, and maintain an audit trail history for at least three (3) months for review;

19. provide immediate notification to EVS of any change in address or office location and are subject to an onsite visit of the new location by EVS or its designated representative; and

20. in the event Agency has a Security Incident involving EVS Confidential Information, Agency will fully cooperate with EVS in a security assessment process and promptly remediate any finding. For purposes of this Section 4, "**Security Incident**" means any actual breach, theft or unauthorized access, use, misuse, theft, vandalism, modification or transfer of or to Services or Data.

b. A cloud service provider ("**CSP**") is a company that offers a component of cloud computing. CSPs generally offer Infrastructure as a Service (IaaS), Platform as a Service (PaaS), or Software as a Service (SaaS). Agency may use a CSP to process, transmit, or store Data and Information, subject to the requirements below.

1. Agency may use Amazon Web Services, Google Cloud Platform, Microsoft Azure, or Salesforce exclusively as their CSP, so long as Agency certifies its CSP has the following minimum requirements: (i) Data and Information at rest is encrypted at a minimum of AES-256; (ii) Data and Information shall be encrypted in transit both internally and externally at a minimum of TLS version 1.2 and/or AES-128; (iii) Agency shall manage all encryption keys within the Agency's CSP; (iv) an inventory shall be kept of all Data and Information within the cloud environment; (v) Data and Information shall be logically and/or physically separated in multi-tenant environments in accordance with industry standards; and (vi) access control standards that include: user provisioning, regular access reviews, password requirements, need to know permissions, and least privilege principles.

2. For all other CSPs, Agency certifies that Agency will, and will contractually obligate it's CSP to, follow EVS's minimum requirements: (i) Data and Information at rest is encrypted at a minimum of AES-256; (ii) Data and Information shall be encrypted in transit both internally and externally at a minimum of TLS version 1.2 and/or AES-128; (iii) Agency shall manage all encryption keys within the Agency's CSP; (iv) an inventory shall be kept of all Data and Information within the cloud environment; (v) Data and Information shall be logically and/or physically separated in multi-tenant environments in accordance with industry standards; (vi) access control standards that include: user provisioning, regular access reviews, password requirements, need to know permissions, and least privilege principles; (vii) utilization of secure data destruction techniques shall be used to destroy Data and Information in accordance with industry standards; (viii) assets that are no longer needed for legal purposes shall be destroyed in accordance with industry standard; (ix) incident handling and forensic support shall be provided in the event of an investigation or Security Incident; (x) cloud hosted systems shall be patched at the most current levels and have vulnerabilities addressed in accordance with industry standards; (xi) information systems and infrastructures shall follow industry security hardening standard such as DISA STIG or CIS guidance; (xii) CSP's application environment shall be certified by an independent third party (SOC 2 Type 2), if operating in a hybrid environment, a SOC 2 Type 2 or equivalent shall also be required for the Agency; (xiii) Third parties providing support services to the Agency or Agency's CSP shall not have access to Data and Information without prior consent of EVS; (xiv) CSP shall have network-based Intrusion Detection Systems (IDS) and/or Intrusion Prevention Systems (IPS) tools deployed in or around the cloud network infrastructure; (xv) centralized logging and monitoring of the CSP's infrastructure/environment; and (xvi) Agency shall utilize multi-factor authentication (MFA) to remotely access CSP's infrastructure/environment.

c. If EVS reasonably believes Agency has violated this Section 4, EVS may, in addition to any other remedy authorized by this Agreement, with reasonable advance written notice to Agency and at EVS's sole expense, conduct, or have a third party conduct on its behalf, an audit of Agency's facilities, security practices and procedures to the extent EVS reasonably deems necessary, including an on-site inspection, to evaluate Agency's compliance with the data security requirements of this Section 4.Such audits shall, at EVS' expense, (1) be at a mutually agreed upon time, during normal business hours, without undue disruption of Agency's business, and subject to Agency's reasonable security requirements and information security practices to conduct on-site audits of Agency's practices and procedures relating to Agency's request for, and use of, the Services, consumer reports, and Agency's security practices with respect thereto under this Agreement; and (2) conduct audits by mail, email or similar electronic means that may require Agency to provide documentation regarding permissible purposes for particular consumer reports ordered by Agency. On-site assessments shall not involve access to Agency's systems and networks and shall occur no more than once per year unless (i) EVS has cause to believe that additional audits are necessary; (ii) EVS is following up on a prior audit where an issue was discovered and remediation was required; or (iii) as required by law.

5. CONFIDENTIALITY. See Attachment B Section 8.

6. **TERM AND TERMINATION**. The term for the Service(s) is set forth in the applicable Schedule. A Schedule may expire or be terminated without affecting the other Schedules. This Agreement shall remain in effect as long as there is an outstanding Schedule with a term then in effect. For termination rights for either party refer to Attachment B Sections 14, 15, and 16. Unless otherwise provided for in the relevant schedule, EVS may change the Service Schedule and/or Description with thirty (30) days' notice to Agency. Agency's use of the Service after such thirty (30) day period shall constitute its agreement to such change(s), without prejudice to its right to terminate this Agreement as provided above.

7. **RIGHTS TO SERVICE.** The Service and the Data are proprietary to EVS; and all rights to the Service and Data are proprietary to and reserved by EVS.

8. **WARRANTY.** See Attachment B Section 4.4.

9. **FORCE MAJEURE.** See Attachment B Section 18.

10. **INDEMNIFICATION.** See Attachment B Section 12.

11. **LIMITATION OF LIABILITY** See Attachment B Section 13.

12. **WAIVER OF JURY TRIAL.** Reserved.

13. **MISCELLANEOUS.** This Agreement sets forth the entire agreement between the parties regarding the Service. Except as otherwise provided in this Agreement, this Agreement may be amended only by a subsequent writing signed by both parties. Assignment provided for under Attachment B Section 9. If any provision of this Agreement is held to be invalid or unenforceable under applicable law in any jurisdiction, the validity or enforceability of the remaining provisions thereof shall be unaffected as to such jurisdiction and such holding shall not affect the validity or enforceability of such provision in any other jurisdiction. To the extent that any provision of this Agreement is held to be invalid or unenforceable because it is overbroad, that provision shall not be void but rather shall be limited only to the extent required by applicable law and enforced as so limited.

14. **NOTICES.** Every notice required under this Agreement may be (i) sent by electronic delivery to the applicable email address below; (ii) mailed first class postage prepaid or by other courier or delivery service to the applicable address below; or (iii) sent through other electronic means, including but not limited to, through Agency's online or integrated access to the Service. Every notice shall be effective upon the following as applicable: (i) day of email sent; (ii) delivery by an overnight or other courier or delivery service, or three (3) days after pre-paid deposit with the postal service; or (iii) date of electronic notification through Agency's online or integrated access to the Service. Agency agrees that if it does not provide the notice information below, then EVS may use the address listed above to provide notice to Agency. Either party may change its notice contact information upon notice to the other party.

	Agency (To be filled in by Agency)	EVS
E-mail Address		evscontracts@equifax.com
Agency Name		Equifax Workforce Solutions LLC
Agency Street Address		11432 Lackland Road
Agency City, State, Zip Code		St. Louis, MO 63146
Attn: Agency Notice Contact	Attn:	Attn: President

15. **COUNTERPARTS/EXECUTION.** See Attachment B Section 20.4.

IN WITNESS WHEREOF, the parties have executed this Agreement on the date indicated below.

Agency		**Equifax Workforce Solutions LLC, provider of Equifax Verification Services**	
By (signature):	_____	By (signature):	_____
Name (print):	_____	Name (print):	_____
Title:	_____	Title:	_____
Date:	_____	Date:	_____

SCHEDULE A

TO THE UNIVERSAL MEMBERSHIP AGREEMENT

EQUIFAX VERIFICATION SERVICES

"Agency":	
"Effective Date" of this Schedule A:	**<Month> 1, <Year>**
Industry Type:	Government
"Agreement":	***Universal Membership Agreement***
Agreement effective date:	MMMM d, yyyy

Agency may request various Services from EVS (i) during the term of the Agreement, (ii) in accordance with the Agreement and this Schedule A (which is part of the Agreement), and (iii) only when intended to be used for the use case described below. Some Services have additional terms and conditions which are referenced in Schedule A-1. Agency will pay EVS for the Services pursuant to the terms of Schedule A-2. Unless otherwise defined in this Schedule A, all defined terms used herein shall have the meaning ascribed to them in the Agreement. This Schedule A, including all attachments hereto, specifically supersedes and replaces any Schedules, Statements of Work, and other product or pricing agreements between the parties that predate this Schedule A and which relate to the Service(s) selected below in this Schedule A, even if the prior agreements contains an "entire agreement" or "merger" clause, and any such Schedules, Statements of Work, and other product or pricing agreements are terminated.

This Schedule shall begin on the Effective Date and continue for a period of one (1) year ("Initial Term"), unless earlier terminated as set forth in the Agreement. Upon expiration of the Initial Term, this Schedule shall automatically renew for successive one (1) year terms (each a "Renewal Term"), unless otherwise terminated in accordance with the terms of the Agreement.

1. AGENCY INFORMATION. *(Please use the physical business location address; a P.O. Box is not acceptable.)*

Agency Name:		Phone:	
Address:		State:	
City:		Zip Code:	

DBA or Management Agency, if different:	
Website address:	

2. MAIN CONTACT INFORMATION.

Name:		Phone / Fax:	/
Title:		Email:	
Supervisor:		Supervisor Phone:	

IN WITNESS WHEREOF, the parties have executed this Schedule A on the date indicated below.

Agency:

By (signature): _____
Name (print): _____
Title: _____
Date: _____

Equifax Workforce Solutions LLC, provider of Equifax Verification Services

By (signature): _____
Name (print): _____
Title: _____
Date: _____

SCHEDULE A-1

SERVICE DESCRIPTIONS / ADDITIONAL TERMS AND CONDITIONS

1. SERVICE DESCRIPTIONS

A. Appriss Insights Services.

(1) Appriss Insights Person Search (using Appriss Insights ("AIP") Database). Provides historical information on arrests and incarcerations. Provides a historic one-time lookback of arrests and incarceration data.

(2) Appriss Insights Person Watch (using Appriss Insights ("AIP") Database). Provides continuous near real time alerts about arrests and incarcerations.

2. ADDITIONAL TERMS AND CONDITIONS

A. Audit. Reserved.

B. Compliance with Laws. Agency will comply with all applicable laws, statutes and regulations regarding the Services. Where applicable, Agency will comply with Title V of the Gramm-Leach-Bliley Act, 15 U.S.C. Sec. 6801 et seq. ("GLB") and the implementing regulations issued thereunder and any other applicable statutes or federal laws, Agency will not use or disclose any Information other than in accordance with Section 6802(c) or with one of the General Exceptions of Section 6802(e) of the GLB and applicable regulations and all other Privacy Laws.

C. Modification of Service Description. EVS may modify this Schedule A, on thirty (30) days' notice to Agency. Agency may terminate the Agreement and/or this Schedule A within thirty (30) days after such modification notice by providing written notice of termination to EVS. Absence of such termination shall constitute Agency's agreement to the modification**.** Any pricing changes must be reflected in a mutually ageed upon and executed amendment to the Agreement.

D. Delivery Channels. Unless otherwise denoted herein, the Services will provide automated or manual access to requested Data and/or Information, as available by Service and selected by Agency, (i) web portal; or (ii) via a batch-only delivery mode ("Batch"). Data and/or Information will be delivered via the same mode it was requested.

E. Use. Information provided from Appriss Insights Services is limited to a single use for the purpose in which it was obtained.

3. ADDITIONAL TERMS AND CONDITIONS APPLICABLE TO APPRISS INSIGHTS SERVICES

A. Use Case Election. Use case and Delivery options are detailed in Appendix I to the Appriss Insights Data Use Agreement ("DUA"), attached hereto as Exhibit 1 ("**DUA**") which is hereby incorporated by reference. Agency elects to use the following use case: for Person Watch and for Person Search.

B. Limited License and Use Restrictions. EVS is acting solely as sales agent and/or connector with regard to the Services and Data under this Schedule A. The limited license and special use restrictions related to the Information Services and Data provided under this Schedule A are those detailed and agreed to between Agency and Appriss Insights in the DUA. As detailed in the DUA, information provided via the Services in this Schedule A are not "consumer reports" as defined in the Fair Credit Reporting Act ("FCRA"). Accordingly, any reference to FCRA requirements and obligations set forth in the Agreement shall not apply to the Services in this Schedule A. Agency certifies that it will not use any information provided by the Services under this Schedule A in such a manner that causes the information to be characterized as a "consumer report" under the FCRA. In the event the DUA is terminated pursuant to its terms, this Schedule A shall simultaneously terminate. This Schedule A is only effective while Agency and Appriss Insights are bound by the attached DUA.

C. Billing Terms and Conditions. The parties mutually agree and understand that EVS shall bill and/or invoice for the Appriss Insights Data and Services rendered under this Schedule in accordance with the terms and conditions contractually in place in a separate agreement between EVS and Appriss Insights.

D. Input Requirements.

(1) Batch. Should Agency choose to elect batch input and delivery methods, any additional terms and conditions, and file input/output information shall be as set forth in Appendix I to the DUA. Each party will bear the cost of producing their batch files. Upon submission of a file, Agency is obligated to pay all charges and/or fees in accordance with the Agreement and this Exhibit. Agency is responsible for providing a file in the correct format and for ensuring that the file being submitted is not in error. For the batch delivery, Agency will request the service on a minimum of one thousand (1,000) Consumers per request unless a set batch size is outlined below in Appendix I to the DUA.

(2) Online. Agency shall request access to Data and Service by inputting the various input element(s) at the relevant website.

E. Delivery.

(1) Batch. Following a batch submission consistent with the input requirements above, a return file of Data via the secure batch website.

(2) Online. The Service will be delivered online, providing automated access to requested Data.

SCHEDULE A-2

PAYMENT TERMS AND SERVICE PRICING

1. PAYMENT TERMS AND CONDITIONS.

A. **Invoices**. Subject to Title 62 O.S. §34.72 all Fees (except the one-time Setup Fee) shall apply during any Renewal Term. EVS reserves the right to increase all Fees pursuant to the terms of the Agreement. Invoices are due net thirty (30) days, but not deemed late for interest purposes until net forty-five (45) days with one and a half (1.5%) percent interest per month applied over forty five (45) days. Agency will be invoiced electronically through EVS's Electronic Invoice Presentation & Payment (EIPP) program. Requests for paper billing are available upon Agency's request and are subject to additional monthly fees. Such fees are subject to modification by EVS at intervals of no less than one year, upon prior written notice. If payment is made by credit card, EVS will charge the credit card each month for Transactions completed in the prior month.

Undisputed invoices outstanding over forty five (45) days may result in loss of access to the Service. If Agency, in good faith, disputes any portion of an amount invoiced, Agency shall pay such amount as it in good faith believes to be correct and provide written notice stating the reasons why the remaining disputed amount is incorrect, along with supporting documentation. All disputes must be submitted to EVS in writing within ninety (90) days from the date of the invoice for those Services. Agency waives the right to dispute any portion of the invoice that is not disputed within such ninety (90) day period.

Subject to Title 62 O.S. §34.72 in the event that it is determined or agreed that Agency must or will pay the disputed amount, then Agency shall pay interest from and including the original payment due date until, but excluding, the date the disputed amount is received by EVS at the interest rate set forth above. In the event the Parties are unable to resolve such dispute, either party may pursue any remedy available at law or in equity to enforce its rights hereunder. For the avoidance of doubt, invoices issued which reflect a price change or pertain to fees for service description modifications that have been accepted according to the terms of this Schedule, shall be deemed correct invoices for purposes of this section.

B. **Agency Purchase Orders.** If the use of a Purchase Order ("PO") or similar ordering document is required by Agency see Attachment B Section 4.

C. **Taxes**. In supplement to Attachment B Section 5, except to the extent that Agency has provided an exemption certificate, direct pay permit or other such appropriate documentation, EVS shall add to each invoice any sales, use, excise, value-added, gross receipts, services, consumption and other similar transaction taxes however designated that are properly levied by any taxing authority upon the provision of the Services, excluding, however, any state or local privilege or franchise taxes, taxes based upon EVS's net income and any taxes or amounts in lieu thereof paid or payable by EVS as a result of the foregoing excluded items.

2. SERVICE PRICING.

A. Third Party Fees Applicable To All Services.

(1) Third Party Fee. EVS will pass along any fees incurred by third parties to Agency, including program fees implemented by the IRS. EVS will post these third party fees as a separate line item on the invoices.

(2) Technology Portal Delivery Fee. EVS will pass along any delivery fees incurred for the use of a technology portal connection, as specified by Agency, to Agency. EVS will post these technology portal delivery fees as a separate line item on the invoices.

B. Appriss Insights Services

Term:

Service Name		**Annual Subscription Payment**	**Number of Submissions Included with Annual Subscription Payment**	**Monthly Installment Charge***
Appriss Insights Services	Internal EFX Use			
Person Serach - Subscription Service (Annual)	0210119397	$100,000.00	2,000,000 Submissions	$8,333.33
Person Watch - Subscription Service (Annual)	0210105941			

Overage Charges (per Submission)		$0.10

* Monthly Installment Charge = Annual Subscription Payment divided into 12 equal installment payments

Optional Term 1:

Service Name		**Annual Subscription Payment**	**Number of Submissions Included with Annual Subscription Payment**	**Monthly Installment Charge***
Appriss Insights Services	Internal EFX Use			
Person Serach - Subscription Service (Annual)	0210119397	$120,000.00	2,000,000 Submissions	$10,000.00
Person Watch - Subscription Service (Annual)	0210105941			
Overage Charges (per Submission)	0210119397 0210105941	$0.11		

* Monthly Installment Charge = Annual Subscription Payment divided into 12 equal installment payments

Optional Term 2:

Service Name		**Annual Subscription Payment**	**Number of Submissions Included with Annual Subscription Payment**	**Monthly Installment Charge***
Appriss Insights Services	Internal EFX Use			
Person Serach - Subscription Service (Annual)	0210119397	$140,000.00	2,000,000 Submissions	$11,666.67
Person Watch - Subscription Service (Annual)	0210105941			
Overage Charges (per Submission)	0210119397 0210105941	$0.12		

* Monthly Installment Charge = Annual Subscription Payment divided into 12 equal installment payments

Optional Term 3:

Service Name		**Annual Subscription Payment**	**Number of Submissions Included with Annual Subscription Payment**	**Monthly Installment Charge***
Appriss Insights Services	Internal EFX Use			
Person Serach - Subscription Service (Annual)	0210119397	$160,000.00	2,000,000 Submissions	$13,333.33
Person Watch - Subscription Service (Annual)	0210105941			
Overage Charges (per Submission)	0210119397 0210105941	$0.13		

* Monthly Installment Charge = Annual Subscription Payment divided into 12 equal installment payments

Optional Term 4:

Service Name		**Annual Subscription Payment**	**Number of Submissions Included with Annual Subscription Payment**	**Monthly Installment Charge***
Appriss Insights Services	Internal EFX Use			
Person Serach - Subscription Service (Annual)	0210119397	$180,000.00	2,000,000 Submissions	$15,000.00
Person Watch - Subscription Service (Annual)	0210105941			
Overage Charges (per Submission)	0210119397 0210105941	$0.14		

* Monthly Installment Charge = Annual Subscription Payment divided into 12 equal installment payments

C. Pricing Terms

(1) **Submission**. Each individual database search which is conducted regardless of whether or not Information is returned constitutes a separate "Submission". The above pricing reflects the fee for each Submission and is based on one use/decision per Submission.

(2) **Watch Submission**. The fee for Person Watch shall be charged per individual subject enrolled for watch such that each individual subject enrolled is a one-time monthly billable event, so long as such Service is contunious for that individual. Watch fees are charged in addition to Search fees on the individual subject.

(3) **Overages**. If Agency exceeds the Number of Submissions Included with Annual Subscription Payment during any Term (Initial Term or Renewal Term), applicable Overage Charges will be charged in addition to the Monthly Installment Charge for the remainder of the then-current Term. The Number of Submissions Included with the Annual Subscription Payment are available for use with either Service, the allocation and usage of which is at Agency's discretion.

(4) **Annual Subscription**. Notwithstanding anything herein or the Agreement to the contrary, in the event Agency terminates this Schedule A prior to the end of the then-current term, Agency shall pay the remaining Monthly Installment Charge then in effect and as due under the then-current year obligation, including any Overage Fees that have been incurred, but not paid. Should the Agency cancel prior to the end of the month, that month (and any overages incurred in that month) shall be considered part of the remaining Monthly Installment Charge.

3. <u>ADDITIONAL SERVICE FEES.</u>

Internal EFX Use		
Annual Setup Fee	0210100037	$125.00
Monthly Account Servicing Fee	0210100693	Waived
Security Monitoring Services Fee	0210100067	Waived

EXHIBIT 1

APPRISS INSIGHTS DATA USE AGREEMENT

THIS DATA USE AGREEMENT (the "**DUA Agreement**"), is entered into and is effective as of , ("**Effective Date**"), by and between **Appriss Insights, LLC,** a Delaware limited liability company, with its principal place of business located at 9901 Linn Station Road, Suite 200, Louisville, Kentucky 40223 ("**Insights**") and the ("**Agency**"), a **state/government agency**, with its principal place of operation located at **("Licensee**"). Insights and Licensee may collectively be referred to herein as the "**Parties**" and may individually be referred to herein as a "**Party**".

WHEREAS, Insights maintains a database pertaining to incarcerated individuals; and

WHEREAS, Licensee desires to utilize data from Insights' database pertaining to incarcerated individuals for its own internal purposes; and

WHEREAS, Licensee entered into that certain Universal Membership Agreement between Licensee and Equifax Workforce Solutions LLC (formerly known as TALX Corporation), a provider of Equifax Verification Services, a Missouri company with its principal place of business at 11432 Lackland Road, St. Louis, Missouri 63146, and its affiliates ("EVS"), last signed by the parties on or about July 1, 2024, and as amended, (the "**UMA Agreement**").

NOW, THEREFORE, the Parties, agreeing to be mutually bound by the terms and conditions of this DUA Agreement, and for other good and valuable consideration, the receipt and sufficiency of which is hereby acknowledged, do hereby agree as follows:

1. **SCOPE OF THE AGREEMENT.** Insights agrees to provide a restricted license so as to permit Licensee to utilize the data as detailed in Appendix I, attached hereto and incorporated by reference (the "Insights Data").Insights hereby grants Licensee a nonexclusive, nontransferable limited license, excluding the right to sub-license, to utilize the Insights Data for its own internal purposes only or as agent on behalf of a government agency in support of the UMA Agreement and subject to the terms and conditions, herein.

2. **TERM.** Subject to Section 7.2 of this DUA Agreement, the initial term of this DUA Agreement will begin on the Effective Date and shall remain in effect for the same term as identified in the applicable portion of the DUA Agreement, including all renewal periods entered into by the parties under the UMA Agreement (the "Term").

3. **[INTENTIONALLY OMITTED]**

4. **RESTRICTED LICENSE**

4.1 License

4.1.1 Insights hereby grants to Licensee, during the Term of this DUA Agreement, a nonexclusive, nontransferable limited license, without the right to sublicense, to access and use the Insights Data solely for Licensee's own internal purposes or as a duly authorized agent of a government agency, subject to the restrictions herein, and for no other purposes.

4.1.2 Licensee represents and warrants that its use of the Insights Data shall be for only lawful and legitimate business purposes relating to its business and as otherwise governed by the DUA Agreement. Licensee shall not use any information contained in the Insights Data for any purpose not expressly authorized by this DUA Agreement. Licensee agrees that if Insights determines that Licensee is violating any provision of this DUA Agreement, or any of the laws, regulations, or rules governing use of the Insights Data or otherwise described herein, Insights may take immediate action, up to and including terminating the delivery of the Insights Data. Licensee shall not access the Insights Data from Internet Protocol addresses located outside of the United States and its territories without Insights' prior written approval. Licensee shall comply with all laws, regulations and rules which may, in Insights' opinion, govern the use of the Insights Data and information provided therein.

4.1.3 The Insights Data contained in Schedule A may be used solely for "tip and lead" purposes to guide Licensee's independent investigation. The Insights Data is not consumer reports and must not be included in any consumer reports, as defined in the Fair Credit Reporting Act, 15 U.S.C. § 1681 et seq. ("FCRA") for any reason. Licensee certifies that the Insights Data will not be used to determine eligibility for a permissible purpose under the FCRA or in any manner that would cause the data to be characterized as a consumer report under the FCRA. Indeed, Licensee represents and warrants that is shall only use the Insights Data as an internal tool to identify jurisdictions from which Licensee (or its agents) will directly retrieve court records or arrest records. Licensee also represents and warrants that it shall not notify any of its customers of the existence of the Insights Data in regards to eligibility determinations for a permissible purpose under the FCRA; any notifications made by or on behalf of Licensee to individuals in this context shall be based solely off of records that Licensee (or its agents) have directly retrieved from government agencies or other third-party sources concerning such individuals.

4.2 **Use of Information**. Licensee hereby warrants that it will not, either directly or indirectly, itself or through any agents or third party: (a) request, compile, store, maintain or use the Insights Data (including any data elements contained therein) to build its own database; (b) copy or otherwise reproduce the Insights Data (including any data elements contained therein); and (c) provide, sell, resell, convey, disclose, or transfer the Insights Data (or any data element(s) contained therein) to any third party. The foregoing shall not be read as prohibiting Licensee from disclosing the Insights Data to a government agency when Licensee is acting as agent on behalf of such agency for the purpose of providing the Insights Data and subject to the terms of this DUA Agreement.

4.3 **Security**. Licensee shall use commercially reasonable security measures to safeguard against unauthorized access to and use of the Insights Data through Licensee by any individual, computer program, or other unauthorized user. Further, Licensee shall implement a commercially reasonable monitoring plan under which Licensee shall guard against but otherwise immediately detect any unauthorized access and/or use of the Insights Data through Licensee. Licensee shall immediately notify Insights of any unauthorized access and/or use of the Insights Data. In addition, Licensee shall notify any other person(s) required to be notified by Licensee under any relevant statute, regulation or order.

4.4 **Notice of Errors**. In the event Licensee becomes aware of any errors contained in the Insights Data, Licensee may notify Insights in writing

of such error and provide copies of any supporting documentation.

5. INTELLECTUAL PROPERTY; APPRISS OBLIGATIONS

5.1 No License. Insights does not transfer, and Licensee does not obtain, any patent rights, copyright interest or other right, claim or interest in the computer programs, systems, forms, formats, schedules, manuals or other proprietary items utilized or provided by Insights.

5.2 Restrictions on Use of Proprietary Designations. Neither Party will use, or permit their respective employees, agents, Customers, and subcontractors to use, the trademarks, service marks, logos, names, or any other proprietary designations of the other Party, or the other Party's affiliates, whether registered or unregistered, without such other Party's prior written consent.

5.3 Ownership of Data. Licensee acknowledges that Insights has expended substantial time, effort, and funds to create and deliver the Insights Data (including the information therein). The Insights Data, the information contained therein, the data elements contained in Insights databases, and Insights' databases themselves, are copyrighted and will continue to be the exclusive property of Insights. Nothing contained in this DUA Agreement shall be deemed to convey to Licensee, or to any other third party, any right, title or interest, including any patent, copyright, or other proprietary right, in or to the data in Insights' database(s) or (except to the extent of the limited license granted in Section 4.1 of this DUA Agreement) to the Insights Data and the information therein.

5.4 Copyright Notices. Licensee shall not remove or obscure any copyright notice or other notices contained in or affixed on any portion of the Insights Data.

5.5 Confidential Treatment. Licensee hereby acknowledges that the Insights Data it receives from Insights under this DUA Agreement may include personal information about individual consumers and, as such, requires confidential treatment. In addition, Licensee acknowledges that it may receive other proprietary and confidential information from Insights including but not limited to technical, developmental, operating, computer system, software, performance, cost, know-how and process information. Licensee warrants to Insights that (a) except as otherwise expressly permitted by this DUA Agreement, Licensee will maintain the information obtained through Insights in strict confidence and will not disclose such information other than to its duly authorized employees who have a business-related need for the information; and (b) Licensee will use the information only for purposes of this DUA Agreement. Upon termination of this DUA Agreement, Licensee shall cease all use of the Insights Data and any Insights confidential information.

5.6 Acknowledgment. Licensee acknowledges that Insights obtains the information contained in the Insights database from third party sources, and such third-party information may be included in the Insights Data. Insights expressly disclaims all liability for any alleged harms caused to the Licensee in the event that (a) any particular information contained within the Insights Data ceases to be available from the Insights database due to the actions of third-party sources; and/or (b) delivery or use of information obtained from third party sources is restricted for any reason. However, Insights shall inform Licensee through EVS of any material changes in the availability of third-party data as soon as practicable.

6. DISCLAIMER OF WARRANTIES, INDEMNIFICATION, AND LIMITATION OF LIABILITY

6.1 Disclaimer of Warranties. Insights will use reasonable efforts to deliver accurate data; provided, however, that the Licensee accepts all information "AS IS." Because the Insights Data involves delivering information provided to Insights by third-party sources, Insights cannot and will not, for the fee charged for the Insights Data, be an insurer or guarantor of the accuracy or reliability of the Insights Data or information contained in its database. INSIGHTS DOES NOT GUARANTEE OR WARRANT THE ACCURACY, TIMELINESS, COMPLETENESS, CURRENTNESS, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE OF THE INSIGHTS DATA, INFORMATION IN THE INSIGHTS DATA, OR THE MEDIA ON OR THROUGH WHICH THE INSIGHTS DATA ARE PROVIDED AND SHALL NOT BE LIABLE TO LICENSEE OR ANY THIRD PARTIES FOR ANY LOSS OR INJURY ARISING OUT OF OR CAUSED IN WHOLE OR IN PART BY INSIGHTS' ACTS OR OMISSIONS, WHETHER NEGLIGENT OR OTHERWISE, IN CREATING, COLLECTING, COMMUNICATING OR DELIVERING THE INSIGHTS DATA OR INFORMATION THEREIN.

6.2 Indemnification.

6.2.1 Insights shall defend, indemnify and hold harmless Licensee, its affiliates, and its successors and their respective directors, officers, employees, and agents, from and against any and all claims, liabilities, or losses, including costs of litigation and reasonable attorneys' fees, to the extent the Insights Data infringes upon or misappropriates a patent, copyright, trademark, trade secret, or other intellectual property right of any third party. Any such indemnification afforded to Licensee shall be limited only to the circumstances described in this Section 6.2.1, and the scope of indemnification shall not be extended for any reason.

6.3 Limitation of Liability.

Licensee acknowledges that Insights maintains a database, updated on a periodic basis, from which Licensee obtains Insights Data, and that while Insights takes reasonable steps to ensure that the database is accurate and up-to-date, Insights does not undertake a separate investigation for each individual query or request for Insights Data made by Licensee. Licensee also acknowledges that the cost to Licensee for its use of the Insights Data has been calculated by Insights to account for Insights' expectation that the risk of any loss or injury that may be incurred by use of the Insights Data in a manner not authorized by this DUA Agreement will be borne exclusively by Licensee, and not Insights. Licensee therefore agrees that it is solely responsible for determining whether the Insights Data provided satisfies Insights' obligations under this DUA Agreement. If Licensee reasonably determines that the Insights Data provided does not satisfy Insights' obligations under this DUA Agreement, Licensee shall so notify Insights in writing within thirty (30) days after receipt of the Insights

Data in question. Licensee's failure to notify \ Insights within the specified period of time, shall mean that Licensee accepts the Insights Data as is, and Insights and EVS will be discharged of any liability for non-performance of the Insights Data. If Licensee so notifies Insights within thirty (30) days after receipt of the Insights Data in question, then, unless Insights disputes Licensee's claim, Insights will, at its option, either (i) deliver to Licensee a satisfactorily conforming version of the Insights Data in question, or (ii) a credit will be issued for the amount Licensee paid for the nonconforming Insights Data in question. Notwithstanding the foregoing, Licensee agrees that Insights' aggregate liability for any and all losses or injuries arising out of any act or omission of Insights in connection with any action to be performed or any information to be furnished under this DUA Agreement, regardless of the cause of the loss or injury, and regardless of the nature of the legal or equitable right claimed to have been violated, shall never exceed the total fees paid by Licensee for the Insights Data within the preceding 12- month period before the alleged act or omission. IN NO EVENT SHALL APPRISS BE LIABLE TO LICENSEE OR ANY THIRD PARTY FOR ANY INDIRECT, INCIDENTAL, CONSEQUENTIAL OR SPECIAL DAMAGES (INCLUDING BUT NOT LIMITED TO DAMAGES TO BUSINESS REPUTATION, LOST BUSINESS OR LOST PROFITS), WHETHER FORESEEABLE OR NOT AND HOWEVER CAUSED, EVEN IF APPRISS RECEIVES NOTICE OF THE POSSIBILITY OF SUCH DAMAGES.

7. AMENDMENTS AND TERMINATION

7.1 **Amendments**. This DUA Agreement may be amended only by a written instrument signed by both Parties.

7.2 **Termination**. Notwithstanding any other term in this DUA Agreement, (a) if Licensee has failed to comply with any of its obligations hereunder, and has not cured such failure within thirty (30) days of its receipt of written notice from Insights detailing the failure, Insights may unilaterally terminate this DUA Agreement immediately, or take any lesser action Insights believes is appropriate in consultation with its sales agent, EVS, including but not limited to blocking Licensee's access to the Insights Data, provided, however, for any obligation under Section 4 of this DUA Agreement, the cure period shall be shortened to ten (10) days; and (b) Licensee may terminate this DUA Agreement for Insights' uncured breach of its obligations hereunder where Insights fails to cure such breach within a thirty (30) day cure period. Furthermore, in the event that any applicable federal law, or government regulation, rule, or order, or industry- wide self- regulation, whether currently in effect or enacted during the term of this DUA Agreement, prohibits, limits, or restricts the delivery or use of the Insights Data, or any material portion thereof, then the affected Party shall provide the other Party with as much advance written notice as practicable under the circumstances. The Parties and Insights' sales agent, EVS, shall meet within ten (10) days following receipt of such written notice to determine whether the Parties are able to mutually agree on a solution to carry out the terms of this DUA Agreement; provided, if the Parties, at their own discretion, are unable to reach a mutually agreed solution within ten (10) days of the Parties' initial meeting, then either Party may terminate this DUA Agreement upon at least ten (10) days prior written notice to the other Party; provided, however, if the effective date of such legislation, regulation, rule, or order does not allow sufficient time to initiate or complete the review process and there is not a commercially reasonable manner by which to extend the termination date to coincide with such review process, then the termination shall be effective as of the effective date of the applicable legislation, regulation, rule, or order to prevent all Parties from being noncompliant with applicable law.

7.3 **Effect of Termination**. Upon expiration or termination of this DUA Agreement, the license granted herein will automatically terminate, Licensee will cease accessing the Insights Data (and the information therein) and shall, within thirty (30) days after the effective date of termination, purge its computer system of and remove its means of access to further Insights Data and derivatives thereof except to the extent that retention of such data is strictly required by applicable law, regulation, or record retention requirements, in which case Licensee may retain such data solely for the purpose of complying with those obligations and shall not otherwise access or use the data. Any removal of further access to Insights Data shall be performed in accordance with applicable federal laws. Upon the request of Insights, Licensee will certify in writing that the actions required of it by the foregoing sentence have been taken. Without limitation, Sections 3, 4, 5, 6, 7.3, and 8 shall survive the expiration or termination of this DUA Agreement.

8. MISCELLANEOUS

8.1 **Status**. Insights will perform its obligations hereunder as an independent contractor. Nothing contained in this DUA Agreement shall be deemed to create any association, partnership, joint venture, or relationship of principal and agent or master and servant between the Parties. The Parties acknowledge that any and all rights not expressly granted pursuant to this DUA Agreement are reserved to the respective Party and that neither Party will have any right, power or authority to obligate the other to any contract, term or condition.

8.2 **[INTENTIONALLY OMITTED]**

8.3 **Governing Law**, Please refer to Attachment A-1, Section 14.1, Choice of Law and Venue.

8.4 **Severability**. This DUA Agreement shall be deemed to be severable and, if any provision of this DUA Agreement shall be finally determined to be void, illegal or unenforceable, then it is the Parties' desire and intention that such provision be deemed automatically adjusted to the minimum extent necessary to conform to applicable requirements of validity, legality and enforceability and, as so adjusted, be deemed a provision of this DUA Agreement as if it were originally included herein.

8.5 **Successors and Assigns**. This DUA Agreement will be binding upon and inure to the benefit of the Parties hereto and to their respective heirs, representatives, successors, and permitted assignees. This DUA Agreement may not be assigned, transferred, shared or divided in whole, or in part, by Licensee without Insights' prior written consent. The dissolution, merger, consolidation, reorganization, sale or other transfer of assets, properties, or controlling interest of more than twenty percent (20%) in, directly or indirectly, or acquisition of substantially all assets of, Licensee, constitutes an assignment of this DUA Agreement for purposes of this Section 8.5.

8.6 **Audit Rights**. At Insights' sole cost and expense, during normal business hours and upon at least fifteen (15) business days advance

written notice, Insights will have the right, in a time and manner reasonably agreed to by the Parties, to audit Licensee's books and records reasonably related to this DUA Agreement to assure compliance with the terms of this DUA Agreement. Licensee will provide commercially reasonable cooperation and will be responsible for assuring cooperation by its employees, in connection with such audits.

8.7 **Waiver**. Either Party may at any time waive compliance by the other with any covenant or condition contained in this DUA Agreement, but only by written instrument signed by the Party waiving such compliance. No waiver of any provision of this DUA Agreement shall be deemed to be, or shall constitute, a waiver of any other provision hereof, nor shall such waiver constitute a waiver in any other instance.

8.8 **[INTENTIONALLY OMITTED]**

8.9 **Publicity**. Except as specifically permitted by the Parties in writing or otherwise required by applicable law, under no circumstances will either Party disclose to any third party, directly or indirectly, the terms and conditions of this DUA Agreement.

8.10 **Notice**. All notices required or permitted to be provided to a Party under this DUA Agreement must be in writing and sent to the address for the Party set forth in the "Notices" section of this DUA Agreement, unless such address has been changed by prior written notice to the other Party to the DUA Agreement.

8.11 **Subject Headings**. The subject headings or captions of the articles and sections of this DUA Agreement are included solely for purposes of convenience and reference and will not be deemed to explain, modify, limit, amplify or aid in the meaning, construction or interpretation of any of the provisions of this DUA Agreement.

8.12

8.13 **Audits (Continued)**. Any clause of this DUA Agreement permitting Insights to audit Licensee's compliance with this DUA Agreement is hereby amended as follows: (A) Discrepancies found in an audit may result in a charge by Insights to the ordering activity. Any resulting invoice must comply with the proper invoicing requirements specified in the underlying UMA Agreement or Schedule. (B) This charge, if disputed by the ordering activity, will be resolved through the Disputes clause at 522.212–4(d); no payment obligation shall arise on the part of the ordering activity until the conclusion of the dispute process. (C) Any audit requested by Insights will be performed at Insights' expense, without reimbursement by the Licensee.

9. **NOTICES**

Notices provided under this DUA Agreement shall be provided by overnight courier to:

If to Insights:

Attn: Legal Department, Appriss Insights, LLC, 9901 Linn Station Road, Suite 200, Louisville, KY 40223

If to Licensee:

Attn: Louisiana Department of Health, Bureau of Legal Services – Bin #20, P. O. Box 3836, Baton Rouge, LA 70821-3836

IN WITNESS HEREOF, the Parties hereto set their hands in agreement to the terms and conditions of this **Appriss Insights Data Use Agreement**.

For Appriss Insights, LLC.:	For LICENSEE:
By (signature):	By (signature):
Name & Title (print):	Name & Title (print):
Date Signed:	Date Signed:

Appendix I

Appriss Insights Data

Except as otherwise noted herein, all defined terms have the meanings specified in the UMA or DUA Agreement.

1. The Insights Data contained in Schedule A may be used solely for "tip and lead" purposes to guide Licensee's independent investigation. They are not consumer reports and must not be included in any consumer reports, as defined in the Fair Credit Reporting Act, 15 U.S.C. § 1681 *et seq.* ("FCRA") for any reason. Licensee certifies that the Insights Data will not be used to determine eligibility for a permissible purpose under the FCRA or in any manner that would cause the data to be characterized as a consumer report under the FCRA.
2. **Information Service 1: Person Watch (using AIP Database).**
   - A. Description: Provides continuous near real time alerts about arrests and incarcerations.
   - B. Single Use: The results of any Person Watch hit may only be used by one Licensee one time and may not be reused in any way. All fees are based on a single-customer-single-use basis.
   - C. Pricing: Pricing is detailed in the UMA Agreement and/or relevant Schedule between Licensee and EVS.
   - D. Delivery and Implementation:
     - i. **Batch**: Person Watch requests may also be submitted via batch. Inputs are as follows:
       - A. First Name
       - B. Last Name
       - C. At least one of the following
         - (i) Date of Birth (preferred)
         - (ii) Social Security Number
         - (iii) Driver's License Number
     - ii. **Portal**: Person Search requests may also be submitted via portal. Inputs are as follows (NOTE: Additional inputs may improve **confidence** matching.):
       - A. First Name
       - B. Last Name
       - C. At least one of the following:
         - (i) Date of Birth (preferred)
         - (ii) Social Security Number
         - (iii) Driver's License Number
   - E. Upon receipt of a Person Watch request and a subsequent arrest or incarceration event, Insights will return the following response data, as available, based on the matching data in the AIP database. Specifically, Insights will provide, as available and permitted:
     - (1) First Name, Last Name, Year of Birth
     - (2) Confidence level indicating the strength of the matching logic based on input data
     - (3) Arrest Date
     - (4) Release Date
     - (5) Release Indicator (to indicate whether individual is in jail or is being released)
     - (6) Jail/prison facility, address and phone number, including county
     - (7) Charge information

3. **Information Service 2: Person Search (using AIP Database).**
   - a. Description: Provides a historic one-time lookback of arrests and incarceration data.
   - b. Single Use: The results of any Person Search hit may only be used by one Licensee one time and may not be reused in any way. All fees are based on a single-customer-single-use basis.
   - c. Pricing: Pricing is detailed in the UMA Agreement and/or relevant Schedule between Licensee and EVS.
   - d. Delivery and Implementation:
     - i. **Batch**: Person Search requests may also be submitted via batch. Inputs are as follows:
       - A. First Name
       - B. Last Name
       - C. At least one of the following
         - 1. Date of Birth (preferred)
         - 2. Social Security Number
         - 3. Driver's License Number
     - ii. **Portal**: Person Search requests may also be submitted via portal. Inputs are as follows (NOTE: Additional inputs may improve confidence matching.):
       - A. First Name
       - B. Last Name
       - C. At least one of the following:
         - 1. Date of Birth (preferred)
         - 2. Social Security Number
         - 3. Driver's License Number
   - e. Upon receipt of a Person Search request, Insights will return the following response data, as available, based on the matching data in the AIP database. Specifically, Insights will provide, as available and permitted:
     - i. First Name, Last Name, Year of Birth
     - ii. Confidence level indicating the strength of the matching logic based on input data
     - iii. Arrest or Booking Date
     - iv. Release Date

v. Release Indicator (to indicate whether individual is in jail or is being released)
vi. Jail/prison facility, address and phone number, including county
vii. Charge information (if available)

Exhibit A
Agency Information

(To be completed by Agency prior to Services being provided)

Physical address of where verifications will be performed (if different than above).	
Onsite contact for onsite inspection.	
Onsite contact email and phone number.	

Additional User Information

IMPORTANT: All individuals who will use the service must be registered below. During the login process, the user will be asked for their registered fax number. All fields are mandatory.

	Name	**E-mail Address**
User1:		
User2:		
User3:		
User4:		
User5:		

Please provide the names, fax numbers and e-mail addresses of up to five (5) additional users. Note: The "Main Contact" above will have the ability to add users via the webManager function. WebManagers have the ability to add, manage and approve users within the organization. If Agency has additional users, once Agreement is accepted, Agency will receive more information on how to register users.

Billing Information

Billing Contact:		**Billing Address:**	
Billing Contact Title:		**City:**	
Billing Phone #:		**State:**	
Billing Fax #:		**Zip Code:**	
Billing E-mail:			

Is Agency Tax Exempt? ☐ Yes ☐ No

If Yes, Please submit tax exemption certificate.

Agency Type:

☐	Federal/State/County/City/Local/Government	☐	Social Security Administration
☐	Non- Profit Organization	☐	Housing Authority
☐	For-Profit Organization	☐	Third Party Vendor for Government Agency
☐	Apartment Complex/Property Management	☐	Other: Please specify

Each program requires documented proof. Specific Program(s) that will use this service:

☐	Food Stamps	☐	TANF	☐	MEDICAID
☐	Child Support Enforcement	☐	Daycare Assistance	☐	Low-Income Energy Assistance
☐	Pre-Employment	☐	Work-related Assistance	☐	Collections

☐	Low-Income Housing	☐	Mortgage Loans		
☐	Other: (Please indicate other program(s) that will use this service:				

If Agency is an **Apartment Complex** or **Property Management Agency**, please answer the following questions:

How many units does Agency have? _____ How many of those are subsidized units? _____

Note: Subsidized units are those in which the owner receives funds from Federal, State, County or Local Government.

Is Agency affiliated with City/State Housing Authority? ☐ **Yes** ☐ **No**

If yes, please include the name: _____

Qualifications: In order to process Agency's application, Agency's agency/organization is required to provide proof (supporting documentation) of Agency's need for employment and income verifications. Please provide the following:

Federal/State/County/City/Local/Government Copy of program's application Income guidelines to determine eligibility	Social Security Administration Copy of program's application Income guidelines to determine eligibility
Non-Profit / For-Profit Organizations Copy of program's application Income guidelines to determine eligibility Affiliation (contract) with a Federal/State/County/City/Local/Government Funding source	Third Party Vendor for Government Agency Copy of program's application Income guidelines to determine eligibility Affiliation (contract) with a Federal/State/County/City/Local/Government Funding source.
Housing Authority Copy of tenant's application Income guidelines for low-income housing Complete HUD Schedule or Rural Development Rent Schedule or L.U.R.A. (Land Use Restriction Agreement)	Apartment Complex/Property Management Copy of tenant's application Income guidelines for low-income housing Complete HUD Schedule or Rural Development Rent Schedule or L.U.R.A. (Land Use Restriction Agreement)

Failure to provide supporting documentation, which must include the name of Agency's agency/organization/Agency name, **may delay processing of Agency's agreement or disqualify Agency's application.**

OKLAHOMA
Office of Management
& Enterprise Services

System Acceptable Use Standard

Introduction

In support of its mission, the State of Oklahoma provides access to information technology resources for employees and contractors. Protecting and preserving these resources is a cooperative effort and requires all users to act responsibly and guard against abuse.

Purpose

This document provides guidance on responsibilities for employees and contractors when using state information technology resources.

Standard

Users are expected to report suspected illegal activity or abuse, especially if related to any damage to or problems with their files. Reports are made by emailing servicedesk@omes.ok.gov. Any defects discovered in the system accounting or system security are to be reported so that steps can be taken to investigate and solve the problem. The cooperation of all users is needed to ensure prompt action. System administrators are required to report suspected unlawful or improper activities to Oklahoma Cyber Command. Users have an affirmative duty to cooperate with Oklahoma Cyber Command in investigations of system abuse.

It is a violation of this standard to use the state's information technology resources for transmitting political campaigning, commercial or personal advertisements, solicitations, promotions, or programs, to libel, harass, threaten, or without authorization, invade the privacy or impersonate the identity of other individuals.

Additionally, it is a violation to use state information technology resources for the purpose of introducing a malicious program into the network, any server or any computer connected to the network. The use of any unauthorized or destructive program may result in legal civil action for damages or other punitive action by any injured party, including the state, as well as criminal action.

This standard prohibits both the circumvention of mechanisms which protect private or restricted information, systems or networks, as well as use of state resources for unauthorized access to private or restricted systems or networks and/or damage to software or hardware components of those systems or networks.

Modifying or removing computer equipment, software, or peripherals without proper authorization is a violation of this standard.

Interfering with the intended use of information resources or without authorization, destroying, altering, dismantling, disfiguring, preventing rightful access to or otherwise interfering with the integrity of electronic information and/or information systems are not all, but further examples of systems abuse.

Compliance

This standard shall take effect upon publication and is made pursuant to Title 62 O.S. §§ 34.11.1 and 34.12 and Title 62 O.S. § 35.8. OMES IS may amend and publish the amended standards policies and standards at any time. Compliance is expected with all published policies and standards, and any published amendments thereof. Employees found in violation of this standard may be subject to disciplinary action, up to and including termination.

Rationale

To coordinate and require central approval of state agency information technology purchases and projects to enable the chief information officer to assess the needs and capabilities of state agencies as well as streamline and consolidate systems to ensure that the state delivers essential public services to its citizens in the most efficient manner at the lowest possible cost to

taxpayers.

Revision history

This standard is subject to periodic review to ensure relevancy.

Effective date: 04/07/2022	**Review cycle:** Annual
Last revised: 10/18/2022	**Last reviewed date:** 09/08/2024
Approved by: Joe McIntosh, Chief Information Officer	

Personal Device Standard

Introduction

OMES Information Services is committed to protecting the State of Oklahoma's employees, partners and its citizens from illegal or damaging actions by individuals, either knowingly or unknowingly. To this end, employees must obtain management approval to use personal devices in connection with state business. Effective security is a team effort involving the participation and support of every employee accessing state information and/or information systems. It is the responsibility of every employee to know the guidelines, and to conduct activities accordingly. Each employee who desires to use personal devices in connection with state business must follow the requirements outlined in this document.

Purpose

This standard outlines the acceptable use of personal devices for state employees. This standard is in place to protect the state, its employees and citizens. Inappropriate use exposes employees and the state to risks including malware attacks, compromise of networks systems and services and legal issues.

Definitions

Personal device – Any personal computing device connecting directly to the state network services including email and calendar services. This definition includes, without limitation, computers, smart phones and tablets.

State record – For the purpose of this standard, information on a personal device created by, received by, under the authority of, or coming into the custody, control or possession of a state employee in connection with the transaction of public business, the expenditure of public funds or the administering of public property and as otherwise may be defined by the Oklahoma Open Records Act.

Standard

The following are general use and ownership requirements for personal devices.

- State records stored on electronic and computing devices, whether owned or leased by the state, the employee or a third party, remain the sole property of the state.
- State records should not be downloaded or stored on personal devices.
- Reserved.
- Reserved.
- Employees are responsible for exercising good judgement regarding the reasonableness of personal use. If there is any uncertainty, employees should consult with their supervisor or manager.
- Employees shall abide by the state's or the individual agency's record retention policy for all state records.

The following are general security requirements for personal devices.

- Reserved.
- All devices must have anti-virus and anti-malware software installed, kept up-to-date and currently enabled. OMES offers CrowdStrike Falcon for Home Use to all state employees. Employees can contact the OMES Service Desk to obtain installation instructions.
- Employees are responsible for keeping personal devices current with all other security patches from the appropriate software update services. This includes applications such as Microsoft, Adobe, Firefox, Chrome, etc.
- Full disk encryption should be enabled for increased protection of the device.
- System level and user level passwords must comply with all state password requirements. Sharing of passwords or any other authentication information is strictly prohibited.
    - Use complex passwords that are at least ten characters with upper- and lower-case letters, numbers and special characters.
    - Avoid common dictionary words.
    - Change passwords periodically.
    - Do not use the same password for all accounts.
- All personal devices must be secured with a password protected screensaver with the automatic activation feature set to 10 minutes or less. Employees should lock the screen or log off when the device is unattended.
- Employees must use extreme caution when opening email attachments on a personal device as those may contain malware. Please visit Using Caution with Email Attachments for additional guidance and information.
- Employees must not install software that allows the user to bypass standard built-in security features and controls, otherwise known as jail breaking.
- Employees who share the personal device with other individuals or family members must ensure individuals do not access state records or business email while using the device. Furthermore, employees must take necessary steps to secure physical state records while working in a space that is shared with other individuals or family members.
- Employees must not print state records from a personal device.
- Employees may only use state-approved and configured applications to access resources.
- Avoid connecting to public or untrusted/insecure Wi-Fi connections.
- Employee must not enable potentially dangerous mobile services while accessing state information services that can export or transmit nonpublic information to unauthorized devices without the user's knowledge. For example, serving as a mobile hotspot or enabling Bluetooth without using recommended safeguards that prevent unauthorized devices from connecting while connected to state information systems.

Compliance

This standard shall take effect upon publication and is made pursuant to Title 62 O.S. §§ 34.11.1 and 34.12 and Title 62 O.S. § 35.8. OMES IS may amend and publish the amended standards policies and standards at any time. Compliance is expected with all published policies and standards, and any published amendments thereof. Employees found in violation of this standard may be subject to disciplinary action, up to and including termination.

Rationale

To coordinate and require central approval of state agency information technology purchases and projects to enable the chief information officer to assess the needs and capabilities of state agencies as well as streamline and consolidate systems to ensure that the state delivers essential public services to its citizens in the most efficient manner at the lowest possible cost to taxpayers.

Revision history

This standard is subject to periodic review to ensure relevancy.

Effective date: 04/01/2020	**Review cycle:** Annual
Last revised: 01/31/2022	**Last reviewed:** 09/19/2024
Approved by: Joe McIntosh, Chief Information Officer	

Data Security Standard

Introduction

Data belonging to the State of Oklahoma must be managed properly to ensure data use is compliant with all applicable state and federal regulations, and that data on Oklahoma citizens is not misused or allowed to fall into the hands of malicious actors. Storage, encryption and secure transmission of data is of paramount importance and the integrity of state data must be preserved at all times.

Purpose

This document establishes requirements for protecting State of Oklahoma data and applies to the following:

- The proper storage, encryption, and transmission of state data.
  - *Data encryption.*
- The proper handling of removable storage, and media destruction procedures,
  - *Data storage.*
  - *Removable media.*
  - *Media disposal.*
- The principals of *least privilege/least functionality* to minimize state data exposure to only those use cases for which it is needed.

Definitions

- Certificate – An authoritative certificate containing a public key that can encrypt or decrypt electronic messages, files, documents or data transmissions and establish or exchange a session key for these same purposes. Key management sometimes refers to the process of storing, protecting and escrowing the private component of the key pair associated with the encryption certificate.
- Data in transit – Any type of information that is actively moving between systems, applications or locations.
- Data at rest – Any type of information that is not actively moving from a device to a network (e.g., data stored on a hard drive, laptop, archive or mobile device).
- Offshore – A location that is outside the physical borders of the U.S.
- FIPS – Federal Information Processing Standards; Publicly announced standards developed by the National Institute of Standards and Technology for use in computer systems of non-military government agencies and contractors.
- PII – Personal Identity Information; any information related to an identifiable person. Personal identity information includes Social Security numbers, tax identification numbers, bank account numbers, credit card numbers, personal health information (PHI) and drivers' license numbers.
- Removable media device – Portable device that can be connected to an information system (IS), computer, or network to provide data storage. These devices interface with the IS through processing chips and may load driver software, presenting a greater security risk to the IS than non-device media, such as optical discs or flash memory cards. Examples include but are not limited to USB flash drives, external hard drives and external solid-state disk (SSD) drives.
- Sensitive data – Any data that includes PII, information deemed confidential by the nature of the agency's business, or information regulated by federal, state and local

regulations. Current and former state employee personal contact information, such as home phone numbers and addresses and information related to electronic communication devices are considered sensitive information by state statute.
- Media – Physical devices or writing surfaces including, but not limited to, magnetic tapes, optical disks, magnetic disks, large-scale integration memory chips, printouts (but not including display media) onto which information is recorded, stored, or printed within an information system.

Standard

Data encryption.

All state data must be encrypted while in transit and at rest. The primary method for data encryption is through the use of asymmetric key encryption, which uses security certificates to encrypt and decrypt data as needed. All security certificates for the State of Oklahoma are managed by Oklahoma Cyber Command, including acquisition, provisioning, renewals, and disposal.

Data storage.

All state data must be stored either on a server in the State Data Center, or on an approved cloud platform which limits data storage and access to the borders of the United States of America. No state data is to be stored in a data center, or on a cloud platform that uses offshore facilities, nor should offshore support personnel have access to live state data.

Offshore tech support is permitted under the following conditions:

- Offshore support resources are not permitted to have access to the production environment or to production/live data which is sensitive or subject to the State of Oklahoma or federal regulations.
- Offshore support resources can have access to dummy data on lower environments (e.g. development or test).
- No path to the production environment or data can exist for offshore support personnel, even if escorted (digitally or physically) by OMES IS personnel

Removable media.

As a general rule, removable media should not be used on State of Oklahoma devices because such devices are extremely easy to lose and do not support the same robust encryption safeguards that other storage media provide. There are cases, however, in which removable media is a valid option. In those cases, removable media which makes use of hardware-level encryption must be used. These devices must meet or exceed FIPS 140-2 encryption standards. A list of acceptable devices can be found on the Permitted Technologies list.

Media disposal.

It is crucial that authorized data destruction techniques be used for secure wiping of media, in compliance with NIST 800-88, Rev. 1, Guidelines for Media Sanitization, to ensure comprehensive eradication and deter data recovery.

Additional controls:

- Only authorized personnel/vendors should be involved in media disposal activities.
- Non-disclosure statements are required of vendors providing off-site media disposal services.
- Media destruction should be certified by a media disposal vendor or OMES surplus.
- Detailed disposal records must be maintained, documenting the media type, the disposal method employed and the accountable party overseeing the disposal.

Least privilege/least functionality.
To ensure that state data is adequately protected, all hardware, software and user accounts must follow the principals of least privilege and least functionality. Put simply, this means that no system or user should have access rights to data or software for which they do not have an approved business need, and that systems and accounts should be built to do one thing only. As an example, if a process needs a service account to move files from location A to location B, and also to write new data into location C, two separate accounts should be created. One to move files from location A to location B, and one to write new files to location C. This approach minimizes the risk of any one account or system becoming compromised.

Compliance
This standard shall take effect upon publication and is made pursuant to Title 62 O.S. §§ 34.11.1 and 34.12 and Title 62 O.S. § 35.8. OMES IS may amend and publish the amended standards policies and standards at any time. Compliance is expected with all published policies and standards, and any published amendments thereof. Employees found in violation of this standard may be subject to disciplinary action, up to and including termination

Rationale
To coordinate and require central approval of state agency information technology purchases and projects to enable the chief information officer to assess the needs and capabilities of state agencies as well as streamline and consolidate systems to ensure that the state delivers essential public services to its citizens in the most efficient manner at the lowest possible cost to taxpayers.

References
- National Institute of Standards and Technology.
- NIST SP 800-88 Guidelines for Media Sanitization.
- NIST SP 800-171 Rev. 3, Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations | CSRC.
- NIST SP 800-171A Rev. 3, Assessing Security Requirements for Controlled Unclassified Information | CSRC.

Revision history
This standard is subject to periodic review to ensure relevancy.

Effective date: 06/17/2025	**Review cycle:** Annual
Last revised: 06/17/2025	**Last reviewed:** 06/17/2025
Approved by: Dan Cronin, Chief Information Officer	

Acceptable Use Standard

Introduction

The State of Oklahoma establishes the acceptable behaviors and practices for using the state's technology and data resources to ensure integrity and accessibility as well as ensuring sensitive state information is protected.

Purpose

This standard establishes acceptable use behavior concerning the use of state's technology, data and resources. This standard applies to all employees, contractors and third-party vendors with access to the State of Oklahoma's systems, networks and data and covers the following:

- *Email protection and acceptable use*.
- *Network acceptable use*.
- *Information systems segregation*.

Definitions

- State email tenant – The environment managed, maintained and protected by the Office of Management and Enterprise Services which provides access to email services, instant messaging, online collaboration and virtual meetings.
- Forwarding – Redirecting communications from the intended destination to another without the sender's knowledge. Auto-forwarding involves automatically directing all incoming messages to another destination.
- Sensitive information – Any information protected by federal, state or local regulations or statute where loss, misuse, unauthorized access or modification thereof could adversely affect national or state interests or the conduct of federal/state programs or the privacy to which individuals are entitled under 5 U.S.C. Section 552a (Privacy Act).

Standard

Email protection and acceptable use.

All state employees and officials must use the state email tenant for all state business including, but not limited to, activities in support of agency missions and job specific functions.

In order to protect sensitive and confidential state information, no request to forward state email to addresses outside of the state email tenant is allowed. Additionally, the following applies to state email.

Any email containing sensitive information sent to an external party must be sent by secure email. Employees and contractors who fail to do so may be required to complete additional training. Repeat offenders may be referred to the agency's HR department and could result in loss of access.

Oklahoma Cyber Command may block unsecure email when sensitive information is identified.

The spam filter for the state automatically blocks messages with a high probability of being spam. End users are responsible for managing their spam filters through the Mimecast Personal Portal.

Personal use of email is not permitted. Users shall have no expectation of privacy in any personal information sent, received or stored by a user using a state email account.

Users shall respect the purpose and charters of email distribution groups. It is the responsibility of any user of an email distribution group to determine the purpose before sending messages to the group or receiving messages from the group.

The state provides email services to support each agency's mission, and email is used as an official form of communication. All users are expected to demonstrate good taste and sensitivity to others in their communications. However, the state cannot protect individuals against the existence or receipt of material that may be offensive, and users are warned they may willingly or unwillingly come across, or be recipients of, material they find offensive. Individuals can report offensive material by emailing servicedesk@omes.ok.gov.

There is no privacy associated with the use of state email resources. Emails routed through the state email tenant are subject to the provisions of the Oklahoma Open Records Act. The state owns, and has right of access to, for any purpose, the contents of all computing information transmitted through or stored on its systems. The state may access and disclose any, or all, of the following:

- Data transmitted through or stored on its email and Internet access systems, regardless of the content of the data.
- Information related to the use of electronic communication.

Network acceptable use.

Access to networks owned or operated by the State of Oklahoma is provided to employees and contractors for use to support the mission of the state. Individuals who have access to state network resources are responsible for using those resources in an ethical and lawful manner.

Excessive or inappropriate usage of network resources may result in network access restriction, revocation of access privileges or further sanctions.

The State of Oklahoma Computer and Mobile Computing Device Usage policy for computer usage prohibits the use of its resources to access, create, transmit (send or receive), print or download material that is discriminatory, derogatory, defamatory, obscene, sexually explicit, offensive or harassing based on gender, race, religion, national origin, ancestry, age, disability, medical condition, sexual orientation or any other status protected by state and federal laws.

Authorized users of these network resources are only permitted to connect and utilize network devices that have been previously reviewed and approved by OMES Cyber Command. Given the potential for unapproved devices to cause network disruptions, service outages and reliability issues, users are prohibited from connecting such devices to the State of Oklahoma network. These prohibited devices include hubs, switches, repeaters, routers, network modems and wireless access points

Devices not approved for use on the State of Oklahoma network will have network access disabled and may be confiscated to ensure the stability and availability of the network.

Personal endpoint devices such as cell phones and laptops may only be connected to "oklahoma_open" Wi-Fi SSID. While these devices do not require prior review and approval from OMES Cyber Command, they are subject to the same rules regarding excessive or inappropriate usage.

Information systems segregation.
Information systems in the State of Oklahoma should have at a minimum, segregated development (Dev) and production (Prod) environments. Separation is essential to maintain security, integrity, operational stability and to prevent unauthorized access and accidental disruptions.

- Logical separation:
  - Implement network segmentation to ensure development and production environments are on different logical networks.
  - Use firewall rules and access control lists (ACLs) to enforce separation and prevent unauthorized traffic between development and production environments.
  - Use virtual private networks (VPNs) or secure tunnels to access production environments from development environments.
  - Development environments should not use production data wherever possible.
    - In rare cases where production data must be used, it must be de-identified to ensure sensitive information is not compromised and requires prior CIO approval.
- User access controls:
  - Use role-based access control (RBAC) to restrict access, based on job responsibilities.
  - Limit developers and operations team access to production environments. They should use automated deployment tools or pipelines to deploy code to production.
  - Implement just-in-time (JIT) access, where applicable, to limit access to operational environments for specific periods.
  - Ensure configuration management maintain separate configuration management repositories for development and production environments.
  - Ensure configuration settings and secrets (e.g., API keys, passwords) are securely stored and managed using the State of Oklahoma's secret management tools.
- Monitoring and logging:
  - Implement separate monitoring and logging infrastructures for development and production environments within the State of Oklahoma SIEM.
  - Monitor access logs and audit trails to detect and respond to unauthorized access attempts or anomalies.
- Training and awareness:
  - Conduct regular security training and awareness programs for development and operational teams.
  - Educate developers and operators about maintaining separate production and operations environments and following security best practices.
- Compliance and enforcement:
  - Compliance with this standard is mandatory for all teams involved in development and operations.
  - Regular audits and reviews should be conducted to ensure adherence to this standard.
  - Non-compliance may result in disciplinary actions as per the organization's policies.
- Responsibilities:
  - The IT security team is responsible for overseeing the implementation and enforcement of this standard.
  - Development and operational teams are responsible for adhering to these guidelines in their day-to-day activities.

Compliance
This standard shall take effect upon publication and is made pursuant to Title 62 O.S. §§ 34.11.1 and 34.12 and Title 62 O.S. § 35.8. OMES IS may amend and publish the amended standards policies and standards at any time. Compliance is expected with all published policies

and standards, and any published amendments thereof. Employees found in violation of this standard may be subject to disciplinary action, up to and including termination

Rationale
To coordinate and require central approval of state agency information technology purchases and projects to enable the chief information officer to assess the needs and capabilities of state agencies as well as streamline and consolidate systems to ensure that the state delivers essential public services to its citizens in the most efficient manner at the lowest possible cost to taxpayers.

References
- State of Oklahoma Computer and Mobile Computing Device Usage Policy.

Revision history
This standard is subject to periodic review to ensure relevancy.

Effective date: 07/02/2025	**Review cycle:** Annual
Last revised: 07/02/2025	**Last reviewed:** 07/02/2025
Approved by: Dan Cronin, Chief Information Officer	

Offer of Value - Added Products and/or Services

Incarceration Intelligence - Person Watch

Helping Agencies Take Proactive Steps

Equifax invites OMES to explore Person Watch, a value added service that is part of our Incarceration Intelligence solution but currently not being leveraged by OMES today. By incorporating Person Watch into OMES' incarceration intelligence service select along with Person Search, OMES can take advantage of a comprehensive technology. The tip-and-lead pointer data returned from Person Watch offers another mechanism to help OMES with their internal processes to detect potential fraud or overpayment issues. Through Person Watch, agencies receive alerts on individuals in their relevant population for booking events or other changes. This helps agencies receive timely notice when a claimant is experiencing a change in status and that additional research or independent verifications may be needed. This can help agencies with their internal processes to account for an individual's transition related to eligibility, applications, or disenrollments for various government programs.

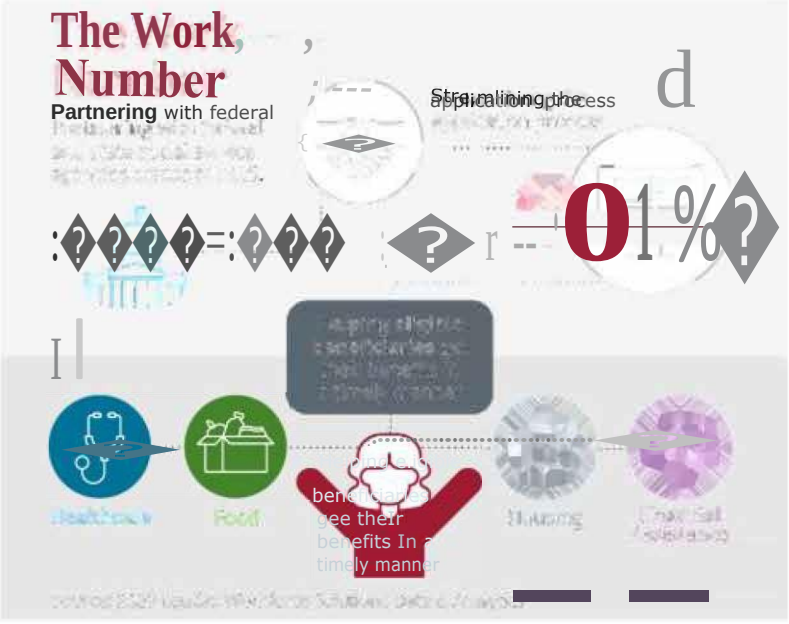
Understanding the Added Value Benefit - Search and Watch

- **Person Search -** a search during a specific point in time helping to identify if a claimant is currently incarcerated, experiencing a transition in the justice system, or has been in the past.
- **Person Watch -** an ongoing process for alerts of booking events or changes, helping agencies receive timely notice when a claimant is booked into a facility or released from custody (booking events within our network). This can help agencies with their internal processes related to benefit applications, enrollments, or disenrollments.
- **Notification Customization -** can be valuable to help oversee a large population with the flexibility to update, add, or delete files or modify alerts as the agency sees fit.

The Work Number®

An Employment and Income Verification Solution for Social Service Agencies

We invite OMES to explore our income and employment verification service, which leverages our proprietary The Work Number® (TWN) database which provides credentialed verifiers with permissible purpose access to the largest consolidated, commercial source of employment information. The data is current, as of the last time a contributing employer or payroll provider processes payroll, and verification results are available instantaneously. This automated data solution has helped numerous state and federal agencies make more efficient and effective eligibility decisions for program applicants while even bolstering program integrity and improving the applicant's customer experience. In contrast, manual verification efforts can drive up administrative and cost inefficiencies and even create room or unintentional manual processing errors. Using a more automated process however can help foster efficient and effective decisions, right-size benefits for eligible applicants, target



manual processing errors, and promote program

Source; 2023 Equifax Workrorce Solutions Data & Analyti15

integrity all while streamlining the benefit recipient experience and freeing up caseworker's time to address more complicated cases.

In 2023, The Work Number provided employment and income verifications for 25 million people seeking government benefits. Over two-thirds of state agencies use The Work Number to automate their eligibility determination processes.



Other methods of delivering employment and income data are based on either quarterly state-based wage data, modeled income, or Financial Asset Data - which can often be unreliable, stale, or incomplete and from sources that do not always return instantaneous results. TWN provides social service agencies with data insights into a claimants' current and previous income and employment status - often reducing the number of places a caseworker must go in order to retrieve that needed information and records.

Contact Complete

Efficiently Reach Beneficiaries for Eligibility Determinations

Social service agencies face a constant battle to keep beneficiary information current. This is crucial for effectively administering programs like Unemployment Insurance (UI), Medicaid, Supplemental Nutrition Assistance Program (SNAP), Low Income Home Energy Assistance Program (LIHEAP), and Temporary Assistance for Needy Families (TANF), but changes in address and contact details often slip through the cracks. This can lead to a cascade of problems, including:

- **Inefficient Determinations:** Difficulty verifying eligibility for benefits or not hearing back from a beneficiary who may have moved;
- **Strain on Resources**: Increased time and resources spent tracking down correct information;
- **Service Disruptions:** Missed renewals and recertifications, leading to gaps in essential services or erroneous procedural terminations.

Contact Complete™ offers a solution to these challenges. It provides insight into various points of contact information such as phone, email, and address while also offering other data points such as name changes or deceased indicators.

How Contact Complete works

Contact Complete helps validate applicant-reported information and automate the benefits process by providing access to current contact information for beneficiaries, if available on the database. Agencies can quickly validate applicant information by submitting search data (e.g. first name, last name, SSN, and DOB). If a match is found, Contact Complete returns a report with current and previous addresses, phone numbers, names, email addresses, and death information, as and if such information is available on the database.

With Contact Complete, agencies have access to data points to help identify residency, send communications like renewal forms and other critical correspondence, and to streamline the application and renewal process for new applicants. Available via the web and through system integration, Contact Complete supports both automated processing and quick lookups, making it adaptable to various agency needs.

Key Features

- **Address Validation:** Search for potential address changes and validate current addresses, crucial for residency verification and communication;
- **Variety of Data:** Provides current contact data such as addresses, phone numbers, emails, name details, and even a death indicator as and if such information is available on the database;
- **Flexible Access:** Available via the web and system-to-system integration for a variety of automated search processes;
- **Streamlined Eligibility Checks:** Helps agencies quickly validate applicant information and streamline the redetermination process.

ATTACHMENT F

Intentionally left blank

ATTACHMENT G

FEDERAL FUNDING TERMS

This State of Oklahoma Federal Funding Terms is a Contract Document in connection with a Contract awarded by and through the State of Oklahoma, Office of Management and Enterprise Services, with a vendor, supplier, or contractor ("Supplier"). Supplier acknowledges that acquisitions under this Contract may use federal assistance for purposes of funding the acquisition. When procuring property and services using Federal financial assistance, the State must follow the same policies it uses for procurements from its non-Federal funds along with all other requirements of the Title 2 U.S. Code of Federal Regulations Part 200, Uniform Administrative Requirements, Cost Principles, and Audit Requirements for Federal Awards (Uniform Guidance). In addition, the State and Supplier ("Parties") must agree to the standards identified in Federal Regulations 2 CFR Sections 200.321 through 200.323 and ensure purchase orders, contracts, or subcontracts include clauses required by 2 CFR Section 200.327.

The terms and conditions provided in this Attachment are general Federal award requirements. Additional terms, conditions, or exceptions may be required that are specific to the Federal financial assistance used in each procurement transaction. Any additional terms, conditions, or exceptions shall be incorporated into a purchase order, contract, or subcontract to ensure compliance with the Federal financial assistance attached to this Contract.

In addition to the terms contained in applicable Contract documents and the requirements mentioned above, the Parties agree to the following Federal Funding Terms.

1 AFFIRMATIVE STEPS FOR CONTRACTING.

1.1 Parties acknowledge that any non-Federal entity included in this Contract must take affirmative steps to assure that minority businesses, women's business enterprises, and labor surplus area firms are used when possible. In addition to and in conjunction with 74 O.S. Sections 85.45 through 85.45i., those affirmative steps must include:

a. Placing qualified small and minority businesses and women's business enterprises on solicitation lists;

b. Assuring that small and minority businesses, and women's business enterprises are solicited whenever they are potential sources;

c. Dividing total requirements, when economically feasible, into smaller tasks or quantities to permit maximum participation by small and minority businesses, and women's business enterprises;

d. Establishing delivery schedules, where the requirement permits, which encourage participation by small and minority businesses, and women's business enterprises;

e. Using the services and assistance, as appropriate, of such organizations as the Small Business Administration and the Minority Business Development Agency of the Department of Commerce; and

f. Requiring the prime contractor, if subcontracts are to be let, to take the affirmative steps listed in paragraphs (a.) through (e.) of this section.

2 INFORMATION SUBMITTED.

Supplier acknowledges that all information, reports, and other documents and data submitted to the State and its representatives in connection with this Contract were, at the time they were (or will be) furnished, and are, as of the date hereof (or will be as of the date they are furnished), true, correct, and complete in all material respects.

3 COMPETITIVE BIDDING.

All funds received by the Supplier herein are subject to the State Purchasing Act and the procurement standards found in 2 CFR Sections 200.321 through 200.323, and 2 CFR Section 200.327. The Supplier acknowledges and agrees that these funds were to the best of Supplier's knowledge competitively bid or covered by an exemption as described therein.

4 AUDITING AND MONITORING REQUIREMENTS.

Supplier acknowledges that the funds used in this transaction are subject to the requirements found in Sections 2 CFR Sections 200.500 through 2 CFR § 200.520; and therefore, the State is subject to audit by Federal and State entities.

4.1 The Supplier agrees to provide the State of Oklahoma, the U.S. Department of Treasury, the Comptroller General of the United States, or any of their authorized representatives access to any books, documents, papers, and records of the Supplier which are directly pertinent to this Contract for the purposes of making audits, examinations, excerpts, and transcriptions. The Supplier agrees to permit any of the foregoing parties to copy or reproduce, by any means, excerpts and transcriptions as reasonably needed, and agrees to cooperate with all such requests. All records related to this transaction must be kept for five years after the completion of this Contract.

4.2 If applicable, the Supplier agrees to provide the Treasury Department or authorized representatives access to construction or other work sites pertaining to the work being completed under the Contract.

4.3 No language in this Contract is intended to prohibit audits or internal reviews by the Treasury Department or the Comptroller General of the United States.

4.4 The Supplier further agrees to include a provision requiring such compliance in its lower tier covered transactions.

5 BUYING PREFERENCES.

5.1 Domestic Preferences, 2 CFR Section 200.322. Supplier should, to the greatest extent practicable under the scope of this Contract, provide a preference for the purchase, acquisition, or use of goods, products, or materials produced in the United States (including but not limited to iron, aluminum, steel, cement, and other manufactured products). The requirements of this section must be included in all subawards, including all contracts and purchase orders for work or products under this Contract. For purposes of this section:

a. "Produced in the United States" means, for iron and steel products, that all manufacturing processes, from the initial melting stage through the application of coatings, occurred in the United States;

b. "Manufactured products" means items and construction materials composed in whole or in part of non-ferrous metals such as aluminum; plastics and polymer-based products such as polyvinyl chloride pipe; aggregates such as concrete; glass, including optical fiber; and lumber; and

c. Federal financial assistance for infrastructure projects must implement the Buy America preferences set forth below.

5.2 Buy America Preference, 2 CFR Part 184. Applies to Federal awards where funds are appropriated or otherwise made available for infrastructure projects in the United States, regardless of whether infrastructure is the primary purpose of the Federal award. Must be included in all subawards, contracts, and purchase orders for the work performed, or products supplied under the Federal award. Infrastructure encompasses public infrastructure projects in the United States, which includes, at a minimum, the structures, facilities, and equipment for roads, highways, and bridges; public transportation; dams, ports, harbors, and other maritime facilities; intercity passenger and freight railroads; freight and intermodal facilities; airports; water systems, including drinking water and wastewater systems; electrical transmission facilities and systems; utilities; broadband infrastructure; and buildings and real property; and structures, facilities, and equipment that generate, transport, and distribute energy including electric vehicle (EV) charging.

6 STATUTES AND REGULATIONS PROHIBITING DISCRIMINATION.

6.1 Executive Order 11246, "Equal Employment Opportunity," as amended by EO 11375, "Amending Executive Order 11246 Relating to Equal Employment Opportunity," and as supplemented by regulations at 41 CFR part 60, "Office of Federal Contract Compliance Programs, Equal Employment Opportunity, Department of Labor. Applies to any construction work and subcontract work, or modification thereof, which is paid for in whole or in part with funds obtained from the Federal Government, unless otherwise exempted.

Construction Contracts 41 CFR Section 60-1.4(b). During the performance of this contract, the contractor agrees as follows:

a. The contractor will not discriminate against any employee or applicant for employment because of race, color, religion, sex, sexual orientation, gender identity, or national origin. The contractor will take affirmative action to ensure that applicants are employed, and that employees are treated during employment without regard to their race, color, religion, sex, sexual orientation, gender identity, or national origin. Such action shall include, but not be limited to the following:

   Employment, upgrading, demotion, or transfer; recruitment or recruitment advertising; layoff or termination; rates of pay or other forms of compensation; and selection for training, including apprenticeship.

b. The contractor agrees to post in conspicuous places, available to employees and applicants for employment, notices to be provided setting forth the provisions of this nondiscrimination clause. which includes that all qualified applicants will receive consideration for employment without regard to race, color, religion, sex, sexual orientation, gender identity, or national origin.

c. The contractor will not discharge or discriminate against any employee or applicant for employment because they inquired about, discussed, or disclosed the compensation of the employee or applicant or another employee or applicant. This does not apply to instances in which an employee who has access to the compensation as part of the employee's essential job function discloses the compensation to individuals who do not otherwise have access to such information, unless such disclosure is in response to a formal complaint or charge, in furtherance of an investigation, proceeding, hearing, or action, including an investigation conducted by the employer, or is consistent with the contractor's legal duty to furnish information.

d. The contractor will send to each labor union or representative of workers with which a collective bargaining agreement is in place or other contract or understanding, a notice to be provided advising the contractor's commitments under this section and shall post copies of the notice in conspicuous places available to employees and applicants for employment.

6.2 **Title VI of the Civil Rights Act of 1964** (42 U.S.C. §§ 2000d, *et seq.*) and Treasury's implementing regulations at 31 C.F.R. Part 22, which prohibits discrimination on the basis of race, color, or national origin under programs or activities receiving Federal financial assistance.

6.3 **Fair Housing Act, Title VIII of the Civil Rights Act of 1968** (42 U.S.C. §§ 3601, *et seq.*), which prohibits discrimination in housing on the basis of race, color, religion, national origin, sex, familial status, or disability.

6.4 **Section 504 of the Rehabilitation Act of 1973,** as amended (29 U.S.C. § 794), which prohibits discrimination on the basis of disability under any program or activity receiving federal financial assistance.

6.5 **Age Discrimination Act of 1975,** as amended (42 U.S.C. §§ 6101, *et seq.*), and Treasury's implementing regulations at 31 C.F.R. Part 23, which prohibit discrimination on the basis of age in programs or activities receiving federal financial assistance.

6.6 **Title II of the Americans with Disabilities Act of 1990**, as amended (42 U.S.C. §§ 12101, *et seq.*), which prohibits discrimination on the basis of disability under programs, activities, and services provided or made available by state and local governments or instrumentalities or agencies thereto.

6.7 **Protections for Whistleblowers.** In accordance with 41 U.S.C. § 4712, the Parties may not discharge, demote, or otherwise discriminate against an employee in reprisal for disclosing to any of the list of persons or entities provided below, information that the employee reasonably believes is evidence of gross mismanagement of a federal contract or grant, a gross waste of federal funds, an abuse of authority relating to a federal contract or grant, a substantial and specific danger to public health or safety, or a violation of law, rule, or regulation related to a federal contract (including the competition for or negotiation of a contract) or grant. The list of persons and entities referenced includes the following:

a. A member of Congress or a representative of a committee of Congress;

b. An Inspector General;

c. The Government Accountability Office;

d. A Treasury employee responsible for contract or grant oversight or management;

e. An authorized official of the Department of Justice or other law enforcement agency;

f. A court or grand jury; or

g. A management official or other employee of Recipient, contractor, or subcontractor who has the responsibility to investigate, discover, or address misconduct.

7 CONTRACT AND SUBCONTRACT LEVEL REQUIREMENTS.

In addition to State procurement regulations, the following Federal regulations apply.

7.1 **Contracts and Purchases in Excess of $2,000.** The following applies to contractors and subcontractors performing on Federal funded or assisted contracts in excess of $2,000 for the construction, alteration, or repair (including painting and decorating) of public buildings or public works, and requires that Supplier must comply with two sets of regulations:

a. **The Davis–Bacon Act (40 U.S.C. §§ 3141-3144, and 3146-3148)** as supplemented by Department of Labor regulations (29 CFR Part 5, "Labor Standards Provisions Applicable to Contracts Covering Federally Financed and Assisted Construction"). When applicable, contractors must be required to pay wages to laborers and mechanics at a rate not less than the prevailing wages specified in a wage determination made by the Secretary of Labor. In addition, contractors must be required to pay wages not less than once a week. The non–Federal entity must place a copy of the current prevailing wage determination issued by the Department of Labor in each solicitation. The decision to award a contract or subcontract must be conditioned upon the acceptance of the wage determination. The non–Federal entity must report all suspected or reported violations to the Federal awarding agency.

b. **Copeland "Anti–Kickback" Act (40 U.S.C. § 3145),** as supplemented by Department of Labor regulations (29 CFR Part 3, "Contractors and Subcontractors on Public Building or Public Work Financed in Whole or in Part by Loans or Grants from the United States"). The Act provides that each contractor or subrecipient must be prohibited from inducing, by any means, any person employed in the construction, completion, or repair of public work, to give up any part of the compensation to which he or she is otherwise entitled. The non–Federal entity must report all suspected or reported violations to the Federal awarding agency.

7.2 Contracts and Purchases in Excess of $10,000.

a. **Recovered Materials.** Any state agency or agency of a political subdivision of a state and its suppliers or contractors must comply with section 6002 of the Solid Waste Disposal Act, as amended by the Resource Conservation and Recovery Act. The requirements of Section 6002 include procuring only items designated in guidelines of the Environmental Protection Agency (EPA) at 40 CFR part 247 that contain the highest percentage of recovered materials practicable, consistent with maintaining a satisfactory level of competition, where the purchase price of the item exceeds $10,000 or the value of the quantity acquired during the preceding fiscal year exceeded $10,000; procuring solid waste management services in a manner that maximizes energy and resource recovery; and establishing an affirmative procurement program for procurement of recovered materials identified in the EPA guidelines.

7.3 Contracts and Subcontracts for $25,000 and Above

a. **Suspension and Debarment**. Restricts awards, subawards, contracts, and subcontracts with Suppliers that are debarred, suspended, or otherwise excluded, or declared ineligible for participation in federal assistance programs and activities. This Contract is a covered transaction for purposes of 2 CFR pt. 180 and 2 CFR pt. 3000. As such, the Supplier is required to verify that none of Supplier's principals (defined at 2 CFR § 180.995) or its affiliates (defined at 2 CFR § 180.905) are excluded (defined at 2 CFR § 180.940) or disqualified (defined at 2 CFR § 180.935). The Supplier must comply with 2 CFR part 180,

subpart C and 2 CFR part 3000, subpart C, and must include a requirement to comply with these regulations in any lower tier covered transaction it enters into. This certification is a material representation of fact relied upon by the State of Oklahoma. If it is later determined that the Supplier did not comply with 2 CFR part 180, subpart C and 2 CFR pt. 3000, subpart C, in addition to remedies available to the State, the federal government may pursue available remedies, including but not limited to suspension and/or debarment.

7.4 Contracts and Purchases $100,000 and Above

a. **The Contract Work Hours and Safety Standards Act,** 40 U.S.C. §§ 3701-3708. Applies to all contracts and subcontracts of more than $100,000 that involve the employment of mechanics or laborers. Under Section 3702 of the Act, contractors and subcontractors shall be required to compute the wages of every mechanic and laborer (including guards and watchmen) on the basis of a standard workweek of 40 hours. Work in excess of the standard workweek is permissible provided that the worker is compensated at a rate of not less than 1 1/2 times the basic rate of pay for all hours worked in excess of 40 hours in the workweek. The requirements of 40 U.S.C. § 3704 are applicable to construction work and provides that no laborer or mechanic shall be required to work in surroundings or under working conditions which are unsanitary, hazardous, or dangerous. *These requirements do not apply to the purchases of supplies or materials or articles ordinarily available on the open market, or contracts for transportation or transmission of intelligence.*

b. **Byrd Anti-Lobbying Amendment, 31 U.S.C. § 1352, as amended.** Supplier certifies that it will not and has not used Federal appropriated funds to pay any person or organization for influencing or attempting to influence an officer or employee of any agency, a Member of Congress, officer or employee of Congress, or an employee of a Member of Congress in connection with obtaining any Federal contract, grant, or any other award covered by 31 U.S.C. § 1352. This Supplier shall also disclose any lobbying with non-Federal funds that takes place in connection with obtaining any Federal award and require any entities receiving subawards or contracts to do the same. Such disclosures are forwarded from tier-to-tier up to the recipient who in turn will forward the certification(s) to the awarding agency.
**** Contractors must sign the attached certification.***

7.5 Contracts and Purchases $150,000 and Above

a. **Clean Air Act (42 U.S.C. §§ 7401– 7671q.) and the Federal Water Pollution Control Act (33 U.S.C. §§ 1251-1387), as amended.** Supplier agrees to comply with, and require all subcontractors to comply with, all applicable standards, orders, or regulations issued pursuant to these Acts. Supplier agrees to report each violation to the State entity that is party to this Contract and understands and agrees that the State entity will, in turn, report each violation as required to assure notification to the appropriate Environmental Protection Agency.

7.6 Contracts and Purchases $250,000 and Above

a. **Remedies.** Contracts for more than the simplified acquisition threshold, currently set at $250,000, must address administrative, contractual, or legal remedies in instances where contractors violate or breach contract terms, and provide for such sanctions and penalties as appropriate.

8 OTHER APPLICABLE LAWS

8.1 **Increasing Seat Belt Use in the United States**. Pursuant to Executive Order 13043, 62 FR 19217 (Apr. 18, 1997), Supplier is encouraged to adopt and enforce on-the-job seat belt policies and programs for employees when operating company-owned, rented or personally owned vehicles.

8.2 **Reducing Text Messaging While Driving.** Pursuant to Executive Order 13513, 74 FR 51225 (Oct. 6, 2009), Supplier is encouraged to adopt and enforce policies that ban text messaging while driving and establish workplace safety policies to decrease accidents caused by distracted drivers.

8.3 **Publications.** Any publications produced with funds from a Federal award must display the following language: "This project [is being] [was] supported, in whole or in part, by federal award number [enter project FAIN] awarded to [name of Recipient] by the U.S. Department of the Treasury."

8.4 **Rights to Inventions Made Under a Contract or Agreement.** If the Federal award meets the definition of "funding agreement" under 37 CFR § 401.2 (a) and the recipient or subrecipient wishes to enter into a contract with a small business firm or nonprofit organization regarding the substitution of parties, assignment or performance of experimental, developmental, or research work under that "funding agreement," the recipient or subrecipient must comply with the requirements of 37 CFR Part 401, "Rights to Inventions Made by Nonprofit Organizations and Small Business Firms Under Government Grants, Contracts and Cooperative Agreements," and any implementing regulations issued by the awarding agency.

> The term ***funding agreement*** means any contract, grant, or cooperative agreement entered into between any Federal agency, other than the Tennessee Valley Authority, and any contractor for the performance of experimental, developmental, or research work funded in whole or in part by the Federal government. This term also includes any assignment, substitution of parties, or subcontract of any type entered into for the performance of experimental, developmental, or research work under a funding agreement as defined in the first sentence of this paragraph.

8.5 Prohibition of Certain Telecommunications and Video Surveillance Services or Equipment.

a. Parties agree that no Federal funds may be obligated or expended in any contract or subcontract that includes obtaining any equipment, system, or service that uses covered telecommunications equipment or services as a substantial or essential component of any system, or as critical technology of any system.

> As described in Public Law 115–232, section 889, *Covered telecommunications equipment* is telecommunications equipment produced by Huawei Technologies Company or ZTE Corporation (or any subsidiary or affiliate of such entities).

b. This prohibition does not prevent parties to this Contract or subcontractors from using covered telecommunications equipment and services for their own purposes, provided the covered telecommunications equipment or services are not procured with Federal funds.

c. In implementing the prohibition under Public Law 115–232, section 889, subsection (f), paragraph (1), heads of executive agencies administering loan, grant, or subsidy programs shall prioritize available funding and technical support to assist affected businesses, institutions and organizations as is reasonably necessary for those affected entities to transition from covered communications equipment and services, to procure replacement equipment and services, and to ensure that communications service to users and customers is sustained.

8.6 Termination for Cause and Convenience – Provisions under Contract Attachment B apply.

This form is required for purchases of $100,000 and above

CERTIFICATION REGARDING LOBBYING
Required by 31 CFR Part 21

The undersigned certifies, to the best of their knowledge and belief, that:

I. No federal appropriated funds have been paid or will be paid, by or on behalf of the undersigned, to any person for influencing or attempting to influence an officer or employee of an agency, a Member of Congress, an officer or employee of Congress, or an employee of a Member of Congress in connection with the awarding of any federal contract, the making of any federal grant, the making of any federal loan, the entering into of any cooperative agreement, and the extension, continuation, renewal, amendment, or modification of any federal contract, grant, loan, or cooperative agreement.

II. If any funds other than federal appropriated funds have been paid or will be paid to any person for influencing or attempting to influence an officer or employee of any agency, a Member of Congress, an officer or employee of Congress, or an employee of a Member of Congress in connection with this Federal contract, grant, loan, or cooperative agreement, the undersigned shall complete and submit Standard Form-LLL, "Disclosure Form to Report Lobbying," in accordance with its instructions.

III. The undersigned shall require that the language of this certification be included in the award documents for all subawards at all tiers (including subcontracts, subawards, and contracts under grants, loans, and cooperative agreements) and that all Suppliers shall certify and disclose accordingly.

This certification is a material representation of fact upon which reliance was placed when this transaction was made or entered into. Submission of this certification is a prerequisite for making or entering into this transaction imposed by section 1352, Title 31, of the U.S. Code. Any person who fails to file the required certification shall be subject to a civil penalty of not less than $10,000 and not more than $100,000 for each such failure.

Supplier certifies or affirms the truthfulness and accuracy of each statement of its certification and disclosure, if any. In addition, the Supplier understands and agrees that the remedies found in Title 31, Chapter 38 of the U.S. Code applies to this certification and disclosure.

David Turner (May 26, 2026 14:44:04 EDT)

Signature of Supplier's Authorized Official

David Turner — May 26, 2026

Name — Date

SVP & General Manager

Title