State of Oklahoma

Office of Management and Enterprise Services

STATE OF OKLAHOMA CONTRACT WITH UPGUARD INC

This State of Oklahoma Contract ("Contract") is entered into between the State of Oklahoma by and through the Office of Management and Enterprise Services ("State") and UpGuard, Inc. ("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 provision to purchase of a Third-Party Risk Assessment platform that can assist with management and provide information into the security posture and risks associated with the state's vendor community, as more particularly described in certain Contract Documents. Supplier submitted a proposal containing exceptions to the Solicitation and Supplier submitted additional terms. 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 #EV00000484, Attachment A;
    2.2. State 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. Information Security Policies and Guidelines, Attachment D-1;
    2.7. Vendor Terms, Attachment E-1;
    2.8. Pricing, Attachment E-2; and
    2.9. First Year Order, Attachment E-3.

3. The parties additionally agree:

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

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

3.3. The price of services under this contract shall not exceed $168,000.00 as listed in Attachment E-2.

3.4. Services for the first year of this contract shall be provided at the rate and manner described in Attachment E-3. To the extent any provision or term of this document conflicts with the terms found elsewhere in this Contract, those the terms found in the Contract shall prevail.

4. Payment obligations rest solely with the Office of Management and Enterprise Services

Please send invoices and billing inquiries to:

OMES
Attn: Accounts Payable
3115 North Lincoln Boulevard
Oklahoma City, Oklahoma 73105

Email: accountspayable@omes.ok.gov

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

6. 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.

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

(Signatures on following page)

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
OFFICE OF MANAGEMENT AND ENTERPRISE SERVICES:

By: Dan Cronin
Dan Cronin (Feb 14, 2025 11:39 CST)

Name: Dan Cronin

Title: Chief Information Officer

Date: Feb 14, 2025

UPGUARD INC

By: Casey Altieri
Casey Altieri (Feb 13, 2025 17:59 EST)

Name: Casey Altieri

Title: SVP of Sales Americas

Date: Feb 13, 2025

Counsel Signature: Amanda E Alvarez
Amanda E Alvarez (Feb 13, 2025 17:00 CST)

ATTACHMENT A

Solicitation No. EV00000484

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

PURPOSE

The Office of Management and Enterprise Services (OMES), Central Purchasing Division, is seeking responses from potential Suppliers to provide a contract for the purchase of Third-Party Risk Assessment platform that can assist with management and provide information into the security posture and risks associated with the state's vendor community. The solution should provide for an end-to-end solution to assist with automation of the risk assessment evaluation process. A Contract resulting from this Solicitation may be designated for use as a Statewide Contract.[1]

The Contract is awarded on behalf of the Office of Management Enterprise Services for third party risk assessment software. All state agencies and state affiliates may avail themselves of this contract.

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:
      3.1.1. Cost
      3.1.2. Technical Response

4. **Scope and Description:**
   4.1. The Bid Response must reflect for each requirement on Exhibit 1 whether the requirement is met by an out-of-the-box solution or whether the requirement necessitates customization to the Bidder's proposed solution.

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

ATTACHMENT A

4.2. The Bid Response shall show the ability of the Bidder to meet or exceed the mandatory specifications in Exhibit 1.

4.3. Executive Summary and Company Information shall be included using Exhibit 03: Company Information.

4.4. All Technical responses shall be proposed using Exhibit 01: Response Matrix.

4.5. The response to pricing shall be proposed using Exhibit 02: Pricing.

4.6. Value-added products and/or services within the scope of the Acquisition may be included in Exhibit 02: Pricing.

4.7. Business References shall be included using Exhibit 04: Business References.

4.8. Third-party vendor information shall be included using Exhibit 05: Third Party Supplier Information.

ATTACHMENT A1

STATE OF OKLAHOMA LOCKDOWN GENERAL TERMS

This State of Oklahoma Lockdown General Terms ("Lockdown General Terms") is a Contract in connection with a Contract awarded by the Office of Management and Enterprise Services on behalf of the State of Oklahoma. The terms contained in this document are not negotiable.

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 Customer's liability or reduce the rights of Customer 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 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 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 replace the Acquisition at Supplier's expense or, if unable to replace, shall issue a refund to Customer. Refund under this section shall not be an exclusive remedy.

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.

ATTACHMENT A1

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 of Supplier

11.1 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.

11.2 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.

11.3 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.

12 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.

13 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.

14 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

15 Miscellaneous

15.1 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.

15.2 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.

15.3 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.

15.4 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.

15.5 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.

15.6 Section Headings

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

15.7 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.

15.8 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.

15.9 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.

15.10 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 GENERAL TERMS

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

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

1 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. terms contained in these General Terms.

C. any Contract-specific State terms contained in a Contract document including, without limitation, information technology terms and terms specific to a statewide Contract or a State agency Contract;

D. any contract-specific Supplier terms contained in a Contract document, including, without limitation, SAAS Terms of Service; and

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

1.2 If there is a conflict between the terms contained in these General Terms 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 except as agreed upon in writing. In no event will any linked document alter or override such referenced terms except as specifically agreed in an Amendment.

ATTACHMENT B

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.

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 mutually executed Contract documents and any applicable encumbering document as may be amended in writing from time to time, which evidences the final agreement between the parties with respect to the subject matter of the Contract.

2.6 **Customer** means the entity receiving goods or services contemplated by the Contract.

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 **Documentation** means the then-current standard documentation for the SAAS that Supplier makes generally available to its customers.

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 examining and testing an Acquisition (including, when appropriate, raw materials, components, and intermediate assemblies) to determine whether the Acquisition meets Contract requirements.

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

2.14 **Product** means any manufactured physical item or tangible deliverable provided by Supplier to Customer under this Contract. For the avoidance of doubt, Product shall not include any software, digital services, or intangible goods.

2.15 **Services** means the professional activities performed by Supplier for Customer under the Contract that (i) are described in an applicable Statement of Work and (ii) which result in Work Product (as defined below).

2.16 **Software as a Service ("SAAS")** means subscription-based, cloud-hosted, on-demand software offered on a one-to-many basis, and includes any and all applications, documentation, information, reports, output, assessments or related products arising from or related to the SAAS and provided by Supplier under the Contract. For the avoidance of doubt, SAAS does not include Products, Services, or any other good or service resulting in Work Product.

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

2.18 **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.

2.19 **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.

2.20 **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.

2.21 **Supplier Confidential Information** means certain confidential and proprietary information of Supplier that is clearly marked as confidential or that should be reasonably understood given the context to be confidential, as applicable, but does not include information excluded from confidentiality in provisions of the Contract or the Oklahoma Open Records Act.

2.22 **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 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. For the avoidance of doubt, any provision of SAAS (including any and all related documentation, reports, materials and information) under the Contract is expressly excluded from the definition of Work Product.

ATTACHMENT B

3 Additional Pricing

3.1 To the extent applicable, 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.

3.2 Supplier shall have no right of setoff.

3.3 Because funds are typically dedicated to a particular fiscal year, an invoice will be paid only when timely submitted, which shall in no instance be later than six (6) months after the end of the fiscal year in which the goods are provided or Services performed.

4 Ordering, Inspection, and Acceptance

4.1 Any Product or Service or SAAS 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 Services will be performed in accordance with industry best practices and are subject to acceptance by the Customer. Notwithstanding any other provision in the Contract, except in the case of SAAS, deemed acceptance of a Service or associated Service deliverable shall not apply automatically upon receipt of a Service deliverable or upon provision of a Service.

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

Any Product to be delivered pursuant to the Contract shall be subject to final

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

Pursuant to OAC 260:115-9-1, payment for a Product or Service does not constitute final acceptance of such Product or Service. If subsequent inspection affirms that the Product or Service does not meet or exceed the specifications of the order, that the Product or Service has a latent defect, the Supplier shall be notified as soon as is reasonably practicable. The Supplier shall retrieve and replace the Product or Service 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.

4.3 Supplier shall deliver Products and Services on or before the required date specified in a Contract document. Failure to deliver timely may result in liquidated damages as set forth in the applicable Contract document. Deviations, substitutions, or changes in a Product or Service, including changes of personnel directly providing Services, shall not be made unless expressly authorized in writing by the Customer. Any substitution of personnel directly providing Services shall be a person of comparable or greater skills, education and experience for performing the Services as the person being replaced. Additionally, Supplier shall provide staff sufficiently experienced and able to perform with respect to any Transitional Services provided by Supplier in connection with termination or expiration of the Contract.

4.4 Product warranty and return policies and terms provided under any Contract document will not be more restrictive or more costly than warranty and return policies and terms for other similarly situated customers for a like Product.

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 once annually upon written request of Customer shall 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'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;

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

D. Errors and Omissions Insurance (Including Cyber Liability) with primary limits of no less than $5,000,000.

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 ("Supplier Taxes") 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 Supplier Taxes or the provision of unemployment insurance and/or Workers' Compensation or any benefit available to a State or Customer employee.

5.3 Supplier agrees to indemnify Customer, the State, and its employees, agents, representatives, contractors, and assignees for any and all liability, actions, claims, demands, or suits, and all related costs and expenses (including without limitation reasonable attorneys' fees and costs required to establish the right to indemnification) relating to tax liability for Supplier Taxes, unemployment insurance and/or Workers' Compensation in connection with its performance under the Contract.

ATTACHMENT B

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, which may include but is not limited to the following:

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

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

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

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

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

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

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

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

I. Requirements of the Health Insurance Portability and Accountability Act of 1996; Health Information Technology for Economic and Clinical Health Act; Payment Card Industry Security Standards; Criminal Justice Information System Security Policy and Security Addendum; and Family Educational Rights and Privacy Act; and

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

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

6.3 The Supplier is responsible to review and inform its employees, agents, and subcontractors who provide a Product or perform a Service under the Contract of the Supplier's obligations under the Contract and Supplier certifies that its employees and each such subcontractor shall comply with minimum requirements and applicable provisions of the Contract. At the request of the State, Supplier shall promptly provide adequate evidence that such persons are its employees, agents or approved subcontractors and have been informed of their obligations under the Contract.

6.4 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.

6.5 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.

6.6 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.

6.7 Supplier represents that, to the best of its knowledge, any litigation or claim or any threat thereof involving Supplier has been disclosed in writing to the State and Supplier is not aware of any other litigation, claim or threat thereof.

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

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 applicable records necessary to confirm execution and performance of the Contract except, unless otherwise agreed, costs of Supplier that comprise pricing under the Contract.

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. 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.

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.

8 Confidentiality

8.1 The Supplier shall maintain strict security of all State and citizen data and records entrusted to it or to which the Supplier gains access, in accordance with and subject to applicable federal and State laws, rules, regulations, and policies "Confidential Information" and shall use any such data and records only as necessary for Supplier to perform its obligations or as otherwise permitted under the Contract. The Supplier further agrees to evidence such confidentiality obligation in a separate writing if required under such applicable federal or State laws, rules and regulations. The Supplier warrants and represents that, except as otherwise permitted under the Contract, Confidential Information shall not be sold, assigned, conveyed, provided, released, disseminated or otherwise disclosed by Supplier, its employees, officers, directors, subsidiaries, affiliates, agents, representatives, assigns, subcontractors, independent contractors, successor or any other persons or entities without Customer's prior express written permission. Supplier shall instruct all such persons and entities that the Confidential Information shall not be disclosed or used without the Customer's prior express written approval except as necessary for Supplier to perform its obligations under the Contract. The Supplier further represents that it has a tested and commercially appropriate system in effect designed to protect all Confidential Information.

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

8.3 Supplier shall report to the Customer without undue delay upon becoming aware of any and all unauthorized use, appropriation, sale, assignment, conveyance, provision, release, access, acquisition, disclosure or other dissemination of any Confidential Information. The Supplier shall also promptly furnish to Customer full details of the unauthorized use, appropriation, sale, assignment, conveyance, provision, release, access, acquisition, disclosure or other dissemination, or attempt thereof, and use its best efforts to assist the Customer in investigating or preventing the reoccurrence of such event in the future. The Supplier shall cooperate with the Customer in connection with any litigation and investigation deemed necessary by the Customer to protect any Confidential Information and shall bear all costs associated with the investigation, response and recovery in connection with any breach of Confidential Information arising out of Suppliers breach of its obligations in this Section 8, including, to the extent the breach of Supplier's obligations constitute of breach of personal data, to credit monitoring services

with a term of at least three (3) years, all notice-related costs and toll free telephone call center services.

8.4 Supplier further agrees to promptly take all reasonable steps to prevent a reoccurrence of any unauthorized use, appropriation, sale, assignment, conveyance, provision, release, access, acquisition, disclosure or other dissemination of Confidential Information.

8.5 Supplier acknowledges that any improper use, appropriation, sale, assignment, conveyance, provision, release, access, acquisition, disclosure or other dissemination of Confidential Information to others may cause immediate and irreparable harm to the Customer and certain beneficiaries and may violate state or federal laws and regulations. If the Supplier or its affiliates, parent company, subsidiaries, employees, officers, directors, assignees, agents, representatives, independent contractors, and subcontractors improperly use, appropriate, sell, assign, convey, provide, release, access, acquire, disclose or otherwise disseminate such Confidential Information to any person or entity in violation of the Contract, the Customer will immediately be entitled to injunctive relief and/or any other rights or remedies available under this Contract, at equity or pursuant to applicable statutory, regulatory, and common law without a cure period.

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

9 Assignment and Permitted Subcontractors

9.1 Supplier's obligations under the Contract may not be assigned or transferred to any other person or entity without the prior written consent of the State which may be withheld at the State's sole discretion. Should Supplier assign its rights to payment, in whole or in part, under the Contract, Supplier shall provide the State and all affected Customers with written notice of the assignment. Such written notice shall be delivered timely and contain details sufficient for affected Customers to perform payment obligations without any delay caused by the assignment.

9.2 Notwithstanding the foregoing, the Contract may be assigned by Supplier without consent to any corporation or other entity in connection with a merger,

consolidation, sale of all equity interests of the Supplier, or a sale of all or substantially all of the assets of the Supplier to which the Contract relates. In any such case, said corporation or other entity shall by operation of law or expressly in writing assume all obligations of the Supplier as fully as if it had been originally made a party to the Contract. Supplier shall give the State and all affected Customers notice of said assignment. 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 for the provision of Products or Services, the Supplier shall obtain written approval of the State of such subcontractor and each employee, as applicable to a particular Acquisition, of such subcontractor proposed for use by the Supplier. Such approval is within the sole discretion of the State. Any proposed subcontractor shall be identified by entity name, and by employee name, if required by the particular Acquisition, in the applicable proposal and shall include the nature of the Services to be performed. As part of the approval request, the Supplier shall provide a copy of a written agreement executed by the Supplier and subcontractor setting forth that such subcontractor is bound by and agrees, as applicable, to perform the same covenants and be subject to the same conditions and make identical certifications to the same facts and criteria, as the Supplier under the terms of all applicable Contract documents. Supplier agrees that maintaining such agreement with any subcontractor and obtaining prior written approval by the State of any subcontractor and associated employees shall be a continuing obligation. The State further reserves the right to revoke approval of a subcontractor or an employee thereof in instances of poor performance, misconduct or for other similar reasons.

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 the provision of Services by unapproved or disapproved employees of the Supplier or a subcontractor.

9.5 Upon written consent of Supplier, the rights and obligations of the State or a Customer under the terms of this Contract may be assigned or transferred, at no additional cost, to other Customer entities.

10 Background Checks and Criminal History Investigations

ATTACHMENT B

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 Supplier agree to provide the State with a description of the background check process to include any vendor's used to gather information. Supplier will further attest that each employee and subcontractor providing Services has passed the background check. 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. Should any employee or subcontractor of the Supplier who will be providing Services under the Contract not be acceptable as a result of the background check or criminal history investigation, the Customer may require replacement of the employee or subcontractor in question and, if no suitable replacement is made within a reasonable time, terminate the purchase order or other payment mechanism associated with the project or Services.

11 Patents and Copyrights

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

Should any third party bring a claim that any portion of a Product or Service or SAAS provided by Supplier under the Contract infringes that party's patent, intellectual property, copyright or other intellectual property right, and Customer's use of such Product, Service or SAAS is enjoined as a result of such claim, then Supplier shall procure for each affected Customer the right to legally continue to use the impacted Product, Service or SAAS, or modify for use, the portion of the Product, Service, or SAAS at issue or replace such potentially infringing Product or SAAS, or re-perform or redeliver in the case of a Service, with at least a functional non-infringing equivalent. Supplier's duty under this section shall extend to include any other Product or Service rendered materially unusable as intended due to replacement or modification of the Product or Service at issue. If the Supplier determines that none of these alternatives are reasonably available, the State shall return such portion of the Product or Service 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 Service deliverable

rendered materially unusable as intended due to removal of the portion of Product or Service 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.

12 Indemnification

12.1 Acts or Omissions

A. Supplier shall defend and indemnify the Indemnified Parties, as applicable, for any and all liability, claims, damages, losses, costs, expenses, demands, suits and actions of third parties (including without limitation reasonable attorneys' fees and costs required to establish the right to indemnification) arising out of, or resulting from any third-party action or claim for bodily injury, death, or property damage brought against any of the Indemnified parties to the extent arising from any grossly negligent act or omission or willful misconduct of the Supplier or its agents, employees, or subcontractors in the provision of Products or Services under the Contract.

B. To the extent Supplier is found liable for loss, damage, or destruction of any property of Customer when providing Products or Services due to any grossly negligent act or omission or willful misconduct on the part of the Supplier, its employees, agents, representatives, or subcontractors, the Supplier and Customer shall use best efforts to mutually negotiate an equitable settlement amount to repair or replace the property unless such loss, damage or destruction is of such a magnitude that repair or replacement is not a reasonable option. Such agreed upon amount shall be invoiced to, and is payable by, Supplier sixty (60) calendar days after the date of Supplier's receipt of an invoice for the negotiated settlement amount.

12.2 Infringement

Supplier shall defend and indemnify the Indemnified Parties, as applicable, for all liability, claims, damages, losses, costs, expenses, demands, suits and actions of third parties (including without limitation reasonable attorneys' fees and costs required to establish the right to indemnification) arising from an alleged infringement of any patent, intellectual property, copyright or other intellectual property right in connection with a Product or Service, or SAAS provided under the Contract. Notwithstanding the foregoing, Supplier's duty under this section shall not apply to the extent a claimed infringement results from: (a) a Customer's or user's content; (b) modifications by Customer or

third party to a Product, Service or SAAS delivered under the Contract or combinations of the Product, Service or SAAS with any non-Supplier-provided services or products unless Supplier required such modification or combination in applicable Documentation; (c) use of a Product, Service or SAAS by Customer in violation of the Contract unless done so at the written direction of Supplier, or (d) a non-Supplier product that has not been provided to the State by, through or on behalf of Supplier as opposed to its combination with products Supplier provides to or develops for the State or a Customer as a system. The foregoing states the entire obligation of Supplier and Customer's sole remedy with respect tot he obligations under this Section.

12.3 Notice and Cooperation

Suppliers indemnification obligations in Section 12. Are contingent on: (i) Customer's prompt written notice of any third-party claim; (ii) Customer affected by the claim will reasonably cooperate with Supplier and defense of the claim; and (iii) Supplier having sole authority to defend and settle such claim, provided that in no event shall Supplier settle such claim in any way that materially prejudices the Customer, without Customer's written consent...

12.4 Limitation of Liability

A. With respect to any claim or cause of action arising under or related to the Contract, neither party shall be liable to the other party for lost profits, lost sales or business expenditures, investments, or commitments in connection with any business, loss of any goodwill, or for any other indirect, incidental, punitive, special or consequential damages, even if advised of the possibility of such damages.

B. Notwithstanding anything to the contrary in the Contract, no provision shall limit damages, expenses, costs, actions, claims, and liabilities arising from or related to bodily injury or death caused by Supplier or its employees, agents or subcontractors; Supplier's Indemnity obligations, either party's confidentiality obligations; either party's breach of the other party's intellectual property rights, the bad faith, gross negligence, intentional misconduct or other acts for which applicable law does not allow exemption from liability of either party or its employees, agents or subcontractors.

C. The limitation of liability and disclaimers set forth in the Contract will apply regardless of whether Customer has accepted a Product or Service.

ATTACHMENT B

13 Termination for Cause

13.1 Supplier may terminate the Contract if (i) it has provided the State with written notice of material breach and (ii) the State fails to cure such material breach within thirty (30) days of receipt of written notice. If there is more than one Customer, material breach by a Customer does not give rise to a claim of material breach as grounds for termination by Supplier of the Contract as a whole. The State may terminate the Contract in whole or in part if (i) it has provided Supplier with written notice of material breach, and (ii) Supplier fails to cure such material breach within thirty (30) days of receipt of written notice. Any partial termination of the Contract under this section shall not be construed as a waiver of, and shall not affect, the rights and obligations of any party regarding portions of the Contract that are not terminated.

13.2 The State may terminate the Contract in whole or in part immediately without a thirty (30) day written notice to Supplier if (i) Supplier's material breach is reasonably determined to be an impediment to the function of the State and detrimental to the State or to cause a condition precluding the thirty (30) day notice or (iii) when the State determines that an administrative error in connection with award of the Contract occurred prior to commencing Contract performance.

13.3 Upon receipt of notice of a termination, Supplier shall immediately comply with the notice terms and take all reasonably necessary steps to minimize the incurrence of costs allocable to the work affected by the notice. If a purchase order or other payment mechanism has been issued and a Product or Service has been accepted as satisfactory, or access to SAAS has been provisioned prior to the effective date of termination, the termination does not relieve an obligation to pay for the Product or Service or SAAS but there shall not be any liability for further payments ordinarily due under the Contract or for any damages or other amounts caused by or associated with such termination. Such termination is not an exclusive remedy but is in addition to any other rights and remedies provided for by law. Any amount paid to Supplier in the form of prepaid fees for Products or Services 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.

13.4 The Supplier's repeated failure to provide an acceptable Product or Service; Supplier's unilateral revision of linked or supplemental terms that have a materially adverse impact on a Customer's rights or obligations under the Contract (except as required by a governmental authority); actual failure of

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

14 Termination for Convenience

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

14.2 Upon receipt of notice of such termination, Supplier shall immediately comply with the notice terms and take all necessary steps to minimize the incurrence of costs allocable to the work affected by the notice. If a purchase order or other payment mechanism has been issued and a Product or Service has been accepted as satisfactory prior to the effective date of termination, the termination does not relieve an obligation to pay for the Product or Service but there shall not be any liability for further payments ordinarily due under the Contract or for any damages or other amounts caused by or associated with such termination. Such termination shall not be an exclusive remedy but shall be in addition to any other rights and remedies provided for by law. Except for any amounts paid to Supplier for the provision of SAAS, 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.

15 Suspension of Supplier

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

15.2 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 for Products or Services in the form of prepaid fees attributable to a period of Suspension or suspended activity shall be refunded.

15.3 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.

16 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.

17 Force Majeure

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

17.2 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.

17.3 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 other than as a result of third-party service provider defaults or failures or general and widespread internet or telecommunications failures that are not limited to Supplier's systems or (b) the delay or failure of Supplier or subcontractor personnel to perform any obligation of Supplier hereunder unless such delay or failure to perform is itself by reason of a force majeure event and (ii) no force majeure event modifies or excuses Supplier's obligations related to confidentiality, indemnification, data security or breach notification obligations set forth herein.

18 Security of Property and Personnel

In connection with Supplier's performance under the Contract, Supplier may have access to Customer personnel, premises, data, records, equipment and other property. Supplier shall use commercially reasonable best efforts to preserve the safety and security of such personnel, premises, data, records, equipment, and other property of Customer. Supplier shall be responsible for damage to such property to the extent such damage is caused by its employees or subcontractors and shall be responsible for loss of Customer property in its possession.

19 Miscellaneous

19.1 Transition Services

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

19.2 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.

19.3 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 specified in the Contract and all other rights and interests are expressly reserved.

D. The Customer and Supplier shall reasonably cooperate with each other and any Supplier to which the provision of a Product and/or Service under the Contract may be transitioned after termination or expiration of the Contract.

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

19.4 Entire Agreement

The Contract documents taken together as a whole constitute the entire agreement between the parties. The Contract documents include these General Terms, any Amendments to these General Terms, and Exhibits or Addendums referencing this Contract. 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.

ATTACHMENT C

RESERVED

This Attachment has been 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 Products and Services and contracts on behalf of the State, allows other State agencies to use the Products and Services while retaining ownership and the right to reassign the Products and Services, at no additional cost, upon written notification to Supplier. OMES-IS is the data custodian for State agency data; however, such data is owned by the respective State agency.

1 DEFINITIONS

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

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

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

1.4 **Intellectual Property Rights** means the worldwide legal rights or interests evidenced by or embodied in any idea, design, concept, personality right, method, process, technique, apparatus, invention, discovery or improvement including any patents, trade secrets and know-how; any work of authorship including any copyrights, Moral Rights or neighboring rights; any trademark, service mark, trade dress, trade name or other indicia of source or origin; domain name registrations; and any other proprietary or similar rights. Intellectual Property Rights of a party also includes all worldwide legal rights or interests that the party may have acquired by assignment or license with the right to grant sublicenses.

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

1.6 **Personal Data** means Customer Data that contains 1) any combination of an individual's name, social security numbers, driver's license, state/federal identification number,

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

1.7 **Product** means any manufactured physical item or tangible deliverable provided by Supplier to Customer under this Contract. For the avoidance of doubt, Product shall not include any software, digital services, or intangible goods.

1.8 **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.

1.9 **Services** means the professional activities performed by Supplier for Customer under the Contract that (i) are described in an applicable Statement of Work and (ii) which result in Work Product (as defined below).

1.10 **Software means** customized computer software developed or modified exclusively for a State agency.

1.11 **Software-as-a-Service** means subscription-based, cloud-hosted, on-demand software offered on a one-to-many basis, and includes any and all applications, documentation, information, reports, output, assessments or related products arising from or related to the SAAS and provided by Supplier under the Contract. For the avoidance of doubt, SAAS does not include Products, Services, or any other good or service resulting in Work Product.

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

1.13 **Supplier Intellectual Property** means all tangible or intangible items or things, including the Intellectual Property Rights therein, created or developed by Supplier and identified in writing as such (a) prior to providing any services or Work Product to Customer and prior to receiving any documents, materials, information or funding from or on behalf of a Customer relating to the services or Work Product, or (b) after the effective date of the Contract if such tangible or intangible items or things were independently developed by Supplier outside Supplier's provision of services or Work Product for Customer under the Contract and were not created, prepared, developed, invented or conceived by any Customer personnel who then became personnel to Supplier or any of its affiliates or subcontractors, where, although creation or reduction-to-practice is completed while the person is affiliated with Supplier or its personnel, any portion of same was created, invented or conceived by such person while affiliated with Customer.

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

1.15 **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 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. For the avoidance of doubt, any provision of SAAS (including any and all related documentation, reports, materials and information) under the Contract is expressly excluded from the definition of Work Product.

2 TERMINATION OF MAINTENANCE AND SUPPORT SERVICES

Customer may terminate maintenance or support services purchased in connection with Products or 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 Products and Services 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. 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 or Services 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 Customer Data shall be stored or accessed internationally for any 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, 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. For the avoidance of doubt, the forgoing shall not apply to Supplier's provision of SAAS under the Contract and international support staff may access Supplier's platform in order to provide appropriate administrative and customer support or as otherwise necessary to perform its obligations under the Contract with respect to the provision of SAAS.

6 COMPLIANCE WITH TECHNOLOGY POLICIES

6.1 The Supplier agrees to adhere to the State of Oklahoma "Information Security Policy, Procedures, and Guidelines" attached as Attachment D-1, when providing Products or Services under the Contract, and further agrees to adhere to the State of

Oklahoma's Information Security Policy, Procedures and Guidelines when provisioning SAAS under the Contract to the extent consistent with Supplier's security policies.

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 when providing Products or Services under the Contract, and further agrees to adhere to the State of Oklahoma's Information Security Policy, Procedures and Guidelines when provisioning SAAS under the Contract to the extent consistent with Supplier's security policies.

6.2 Supplier shall comply with applicable Federal Information Processing Standards when providing Products or Services, including, without limitation, FIPS 200, FIPS 140-2 or successor standards and all applicable recommendations from the National Institute of Standards and Technology.

7 EMERGING TECHNOLOGIES

The State reserves the right to execute an Addendum to the Contract with Supplier 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, and to the extent that such technology is applicable to the provision of Products, Services or SAAS under the Contract.

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 for Products or Services at his or her sole option if the State Chief Information Officer determine such extension to be in the best interest of the State.

9 SOURCE CODE ESCROW

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

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

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

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

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

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

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

9.7 Supplier's ceasing of maintenance and support of the Software; or

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

10 COMMERCIAL OFF THE SHELF SOFTWARE OR SUPPLIER TERMS

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

11 OWNERSHIP RIGHTS

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

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

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

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

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

12 INTELLECTUAL PROPERTY OWNERSHIP TO WORK PRODUCT

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

12.1 As to the Intellectual Property Rights to Work Product between Supplier and Customer, Customer shall be the exclusive owner and not Supplier. Supplier specifically agrees that the Work Product shall be considered "works made for hire" and that the Work Product shall, upon creation, be owned exclusively by Customer. To the extent that the Work Product, under applicable law, may not be considered works made for hire, Supplier agrees that all right, title and interest in and to all ownership rights and all Intellectual Property Rights in the Work Product is effectively transferred, granted, conveyed, assigned, and relinquished exclusively to Customer, without the necessity of any further consideration, and Customer shall be entitled to obtain and hold in its own name all Intellectual Property Rights in and to the Work Product. Supplier acknowledges that Supplier and Customer do not intend Supplier to be a joint author of the Work Product within the meaning of the Copyright Act of 1976. Customer shall have access, during normal business hours (Monday through Friday, 8:00 a.m. to 5:00 p.m.) and upon reasonable prior notice to Supplier, to all Supplier materials, premises and computer files containing the Work Product. Supplier and Customer, as appropriate, will cooperate with one another and execute such other documents as may be reasonably appropriate to achieve the objectives herein. No license or other right is granted under the Contract to any Third-Party Intellectual Property, except as may be incorporated in the Work Product by Supplier.

12.2 Supplier, upon request and without further consideration, shall perform any acts that may be deemed reasonably necessary or desirable by Customer to evidence more fully the transfer of ownership and/or registration of all Intellectual Property Rights in all Work Product to Customer to the fullest extent possible including, but not limited to, the execution, acknowledgement and delivery of such further documents in a form determined by Customer. In the event Customer shall be unable to obtain Supplier's signature due to the dissolution of Supplier or Supplier's failure to respond to Customer's repeated requests for such signature on any document reasonably necessary for any purpose set forth in the foregoing sentence, Supplier hereby irrevocably designates and appoints Customer and its duly authorized officers and agents as Supplier's agent and Supplier's attorney-in-fact to act for and in Supplier's behalf and stead to execute and file any such document and to do all other lawfully permitted acts to further any such purpose with the same force and effect as if executed and delivered by Supplier, provided however that no such grant of right to Customer is applicable if Supplier fails to execute

any document due to a good faith dispute by Supplier with respect to such document. It is understood that such power is coupled with an interest and is therefore irrevocable. Customer shall have the full and sole power to prosecute such applications and to take all other action concerning the Work Product, and Supplier shall cooperate, at Customer's sole expense, in the preparation and prosecution of all such applications and in any legal actions and proceedings concerning the Work Product.

12.3 Supplier hereby irrevocably and forever waives, and agrees never to assert, any Moral Rights in or to the Work Product which Supplier may now have or which may accrue to Supplier's benefit under U.S. or foreign copyright or other laws and any and all other residual rights and benefits which arise under any other applicable law now in force or hereafter enacted. Supplier acknowledges the receipt of equitable compensation for its assignment and waiver of such Moral Rights.

12.4 All documents, information and materials forwarded to Supplier by Customer for use in and preparation of the Work Product shall be deemed the confidential information of Customer, subject to the license granted by Customer to Supplier hereunder. Supplier shall not otherwise use, disclose, or permit any third party to use or obtain the Work Product, or any portion thereof, in any manner without the prior written approval of Customer.

12.5 These provisions are intended to protect Customer's proprietary rights pertaining to the Work Product and the Intellectual Property Rights therein and any misuse of such rights would cause substantial and irreparable harm to Customer's business. Therefore, Supplier acknowledges and stipulates that a court of competent jurisdiction may immediately enjoin a material breach of the Supplier's obligations with respect to confidentiality provisions of the Contract and the Work Product and a Customer's Intellectual Property Rights, upon a request by Customer, without requiring proof of irreparable injury, as same is presumed.

12.6 Upon the request of Customer, but in any event upon termination or expiration of this Contract or a statement of work, Supplier shall surrender to Customer all documents and things pertaining to the Work Product, generated or developed by Supplier or furnished by Customer to Supplier, including all materials embodying the Work Product, any Customer confidential information and Intellectual Property Rights in such Work Product, regardless of whether complete or incomplete. This section is intended to apply to all Work Product as well as to all documents and things furnished to Supplier by Customer or by anyone else that pertains to the Work Product.

12.7 Customer hereby grants to Supplier a non-transferable, non-exclusive, royalty-free, fully paid license to use any Work Product solely as necessary to provide Services to Customer. Except as provided in this section, neither Supplier nor any subcontractor shall have the right to use the Work Product in connection with the provision of Services to its other customers without the prior written consent of Customer, which consent may be withheld in Customer's sole discretion.

12.8 To the extent that any Third Party Intellectual Property is embodied or reflected in the Work Product or is necessary to provide Services, Supplier shall obtain from the applicable third party for the Customer's benefit, an irrevocable, perpetual, non-exclusive, worldwide, royalty-free license, solely for Customer's internal business purposes; likewise, with respect to any Supplier Intellectual Property embodied or

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

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

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

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

13 HOSTING SERVICES

A Supplier shall be responsible for the obligations set forth in in this Contract, including those obligations related to breach reporting and associated costs when a Supplier that is 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 agreed upon in the Contract, service credits shall be provided by Supplier and may be used as an offset to payment due for Products and Services.

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 Products and Services and contracts on behalf of appropriated agencies of the State belong to OMES-IS. OMES-IS allows other State agencies to use the Products and Services while retaining ownership and the right to reassign the assets, at no additional cost, upon written notification to Supplier.

17 CUSTOMER DATA

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

17.2 Customer will be responsible for the accuracy and completeness of all Customer Data provided to Supplier by Customer. Customer shall retain exclusive ownership of rights, title, and interest in Customer Data. Non-Public Data and Personal Data shall be deemed to be Customer's confidential information. Supplier shall restrict access to Customer Data to their employees and subcontractors with a bona fide need to know in order to perform their obligations under the Contract (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. To the extent permitted by law and Supplier agrees to make reasonable efforts 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 upon becoming aware 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 gross negligence or willful misconduct. If Customer Data is lost or damaged for reasons other than as a result of Supplier's gross 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 Customer 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 data of similar kind.

18.2 All Customer Data shall be encrypted at rest and in transit with controlled access. Unless otherwise stipulated, the service provider is responsible for encryption of Customer Data. All Customer 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 Supplier's 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 as a result of Supplier's breach of their obligations in this Contract, 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. unless otherwise requested by Customer. SAAS shall be hosted using Google Cloud Platform servers located in the US. 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 Once annually, Supplier shall allow the Customer to audit conformance to the Contract terms. The Customer may perform this audit or contract with a third party at its discretion and at Customer's expense.

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

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

19 SECURITY ASSESSMENT

19.1 The State requires any entity or third-party Supplier Hosting Oklahoma Customer Data to submit to a State Certification and Accreditation Review process to assess initial security risk. Supplier submitted to the review and met the State's minimum security standards at time the Contract was executed. Failure to comply with the security terms of the Contract 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 and include in such notification any 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 promptly upon becoming aware of any Security Incident or Data Breach impacting Customer Data.

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 Supplier; and (iv) document all Security Incidents and their outcomes.

20.5 If Supplier has actual knowledge of a Data Breach, Supplier shall (1) promptly notify the appropriate Customer identified contact set forth herein within 48 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 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 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 or otherwise prevent its release, Supplier shall indemnify and hold harmless the Customer against all penalties assessed to Indemnified Parties by governmental authorities in connection with the Data Breach.

22 SUPPLIER REPRESENTATIONS AND WARRANTIES

Supplier represents and warrants the following:

22.1 The Product and Services provided in connection with the Contract do not infringe a third party's patent or copyright or other intellectual property rights.

22.2 Supplier will protect Customer 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 TERMINATION, EXPIRATION AND SUSPENSION OF SERVICE

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

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

Supplier shall implement an orderly return of Customer Data in a commercially reasonable format agreed upon by the parties and, as determined by the Customer:

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

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

c. a combination of the two immediately preceding options.

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

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

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

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

After such period and upon written request, Supplier shall, unless legally prohibited or otherwise stipulated, delete all Customer Data in its systems or

otherwise in its possession or under its control.

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

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

24 GENERAL INFORMATION SECURITY REQUIREMENTS

24.1 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.

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

24.3 Contractor or its subcontractors will disclose to Client any suspected breach of the security of the Client's 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.

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

25 HIPAA REQUIREMENTS

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

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

25.3 Business Associate Terms Definitions:

a. Unless otherwise defined in this BAA, all capitalized terms used in this BAA have the meanings ascribed in the HIPAA Regulations, provided; however, that "PHI" and "ePHI" shall mean Protected Health Information and Electronic Protected Health Information, respectively, as defined in 45 C.F.R. § 160.103, limited to the information Business Associate received from or created or received on behalf of the applicable State of Oklahoma agency as a Business Associate. "Administrative Safeguards" shall have the same meaning as the term "administrative safeguards in 45 C.F.R. § 164.304, with the exception that it shall apply to the management of the conduct of Business Associate's workforce, not the State of Oklahoma agency workforce, in relation to the protection of that information.

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

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

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

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

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

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

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

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

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

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

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

g. in accordance with 45 C.F.R. 164.502(e)(1) and 164.308(b), if applicable, require that any Sub-Contractors that create, receive, maintain or transmit PHI on behalf of the Business Associate agree to the same restrictions, conditions, and requirements that apply to the Business Associate with respect to such information; this shall be in the form of a written HIPAA Business Associate Contract and a fully executed copy will be provided to the Contract Monitor;

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

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

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

k. to the extent allowed by law, indemnify and hold Covered Entity harmless from all claims, liabilities costs, and damages arising out of or in any manner related to the unauthorized disclosure by Business Associate of any PHI resulting from the negligent acts or omissions of Business Associate or to the breach by Business Associate of any applicable obligation related to PHI;

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

requested shall be the responsibility of Covered Entity;

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

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

o. make its internal practices, books, and records related to the use and disclosure of PHI received from or created or received by Business Associate on behalf of Covered Entity available to the Secretary of the Department of HHS, authorized governmental officials, and Covered entity for the purpose of determining Business Associate's compliance with the Privacy Rule. Business Associate shall give Covered Entity advance written notice of requests from HHS or government officials and provide Covered Entity with a copy of all documents made available; and require that all of its Sub-Contractors, vendors, and agents to whom it provides PHI or who create, receive, use, disclose, maintain, or have access to Covered Entity's PHI shall agree in writing to requirements, restrictions, and conditions at least as stringent as those that apply to Business Associate under this Agreement, including but not limited to implementing reasonable and appropriate safeguards to protect PHI, and shall require that its Sub-Contractors, vendors, and agents agree to indemnify and hold harmless Covered Entity for their failure to comply with each of the provisions of this Agreement.

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

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

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

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

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

e. make uses and disclosures and requests for protected health information consistent with Covered Entity's minimum necessary policies and procedures;

f. de-identify any and all PHI obtained by Business Associate under this BAA, and use such de-identified data, all in accordance with the de-identification requirements of the Privacy Rule [45 C.F.R. § (d)(1)].

25.6 Obligations of Covered Entity

a. Covered Entity shall notify Business Associate of any changes in, or revocation of, the permission by an individual to use or disclose his or her PHI, to the extent that such changes may affect Business Associate's use or disclosure of PHI.

b. Covered Entity shall notify Business Associate of any restriction on the use or disclosure of PHI that Covered Entity has agreed to or is required to abide by under 45 C.F.R. 164.522, to the extent that such restriction may affect Business Associate's use or disclosure of protected health information.

c. Covered Entity shall not request Business Associate use or disclose PHI in any manner that would violate the Privacy Rule if done by Covered Entity.

d. Covered Entity agrees to timely notify Business Associate, in writing, of any arrangements between Covered Entity and the Individual that is the subject of PHI that may impact in any manner the use and/or disclosure of the PHI by Business Associate under this BAA.

e. Covered Entity shall provide the minimum necessary PHI to Business Associate.

25.7 Term and Termination:

a. Obligations of Business Associate upon Termination. Upon termination of this Agreement for any reason, Business Associate, with respect to PHI received from Covered Entity, or created, maintained, or received by Business Associate on behalf of Covered Entity, shall as applicable:

i. retain only that PHI that is necessary for Business Associate to continue its proper management and administration or to carry out its legal responsibilities;

ii. return to Covered Entity (or, if agreed to by Covered Entity, destroy) the remaining PHI that the Business Associate still maintains in any form;

iii. continue to use appropriate safeguards and comply with Subpart C of 45 C.F.R. Part 164 with respect to PHI to prevent use or disclosure of the PHI, other than as provided for in this Section, for as long as Business Associate retains the PHI;

iv. not use or disclose the PHI retained by Business Associate other than for the purposes for which such PHI was retained and subject to the same

conditions set out at above under "Permitted Uses and Disclosures By Business Associate" that applied prior to termination; and

v. return to Covered Entity (or, if agreed to by Covered Entity, destroy) the PHI retained by Business Associate when it is no longer needed by Business Associate for its proper management and administration or to carry out its legal responsibilities.

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

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

25.8 Miscellaneous Provisions:

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

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

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

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

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

f. If Business Associate maintains a designated record set in an electronic format on behalf of Covered Entity, then Business Associate agrees that within 30 calendar days of expiration or termination of the parties' agreement, Business Associate shall provide to Covered Entity a complete report of all disclosures of and access to the designated record set covering the three years immediately preceding the termination or expiration. The report shall include patient name, date and time of

disclosures/access, description of what was disclosed/accessed, purpose of disclosure/access, name of individual who received or accessed the information, and, if available, what action was taken within the designated record set.

g. Amendment: To the extent that any relevant provision of the HIPAA Regulations is materially amended in a manner that changes the obligations of Business Associates or Covered Entities, the Parties agree to negotiate in good faith appropriate amendment(s) to this Agreement to give effect to these revised obligations. The parties agree to amend this Agreement from time to time as is necessary for Covered Entity or to comply with the requirements of the Privacy Rule and related laws and regulations.

26 42 C.F.R. PART 2 RELATED PROVISIONS

26.1 Confidentiality of Information. Contractor's employees and agents shall have access to private data to the extent necessary to carry out the responsibilities, limited by the terms of this Contract. Contractor accepts the responsibilities for providing adequate administrative supervision and training to their employees and agents to ensurecompliance 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 Contract, whether during the period of the Contract or thereafter. Furthermore, Contractor:

26.2 Acknowledges that in receiving, transmitting, transporting, storing, processing, or otherwise dealing with any information received pursuant to this Contract that identifies or otherwise relates to the individuals under the care of or in the custody of a State of Oklahoma agency, then to the extent Contractor receives such information in order to fulfill its obligations under the Contract, 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 Contract or by law;

26.3 Acknowledges that pursuant to 43A O.S. §1-109, all mental health and drug or alcohol treatment information and all communications between physician or psychotherapist and patient are both privileged and confidential and that such information is available only to persons actively engaged in treatment of the client or consumer or in related administrative work. To the extent Contractor receives such information in order to fulfill its obligations under the Contract, 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;

26.4 Where applicable, 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;

26.5 Agrees to, when applicable and to the extent within Contractor's control, use appropriate administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of the electronic protected health information that it creates, receives, maintains, or transmits on behalf of the State of Oklahoma agency and to use appropriate safeguards to prevent the unauthorized use or

disclosure of the protected health information, and agrees that protected information will not be placed in the Child Protective Services (CPS) record of any individual involved with the Oklahoma Department of Human Services (DHS).

26.6 Agrees to report to the State of Oklahoma agency any use or disclosure or any security incident involving protected information provided for by this Contract. Such a report shall be made immediately when an employee becomes aware of such a disclosure, use, or security incident.

26.7 Where applicable, 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;

26.8 Where applicable, 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;

26.9 Where applicable, agrees to make available its internal practices, books, and records, including policies and procedures, relating to the use and disclosure of Protected Health Information received from theState 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;

26.10 Where applicable, 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.

27 FEDERAL TAX INFORMATION REQUIREMENTS IRS PUBLICATION 1075

27.1 PERFORMANCE: Solely to the extent 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:

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

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

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

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

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

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

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

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

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

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

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

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

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

28 CRIMINAL/CIVIL SANCTIONS

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

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

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

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

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

recertifications, the contractor and each officer or employee must sign, either with ink or electronic signature, a confidentiality statement certifying their understanding of the security requirements.

29 INSPECTION

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

30 SSA REQUIREMENTS

30.1 PERFORMANCE: Solely to the extent 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:

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

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

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

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

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

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

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

penalties for unlawful assess and/or disclosure.

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

30.10 The applicable State of Oklahoma agency shall provide the Contractor a copy of the SSA exchange agreement and all related attachments before initial disclosure of SSA data. Contractor is required to follow the terms of the applicable State of Oklahoma agency's data exchange agreement with the SSA. Prior to signing this Contract, 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.

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

30.12 SSA requires all parties subject to this Contract 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.

30.13 SSA requires all parties subject to this Contract 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.

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

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

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

31 CRIMINAL/CIVIL SANCTIONS

The Act specifically provides civil remedies, 5 U.S.C. Sec. 552a(g), including damages, and criminal penalties, 5 U.S.C. Sec. 552a(i), for violations of the Act. The civil action provisions are premised violations of the Act committed by parties subject to this Contract or regulations promulgated thereunder. An individual claiming such a violation by parties subject to this Contract 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 Contract 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 Contract to comply with the Act.

31.1 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 Contract 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 Contract 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.

31.2 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).

32 CHILD SUPPORT FPLS REQUIREMENTS

32.1 Solely to the extent applicable and to the extent within Contractor's control, Contractor 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.

32.2 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.

32.3 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).

33 FERPA REQUIREMENTS

33.1 Soley to the extent Contractor takes possession or control of Information covered by FERPA in performance of this Contract, 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.

34 CJIS REQUIREMENTS

34.1 INTRODUCTION - This section shall be applicable solely to the extent that Contractor takes possession or control of CJIS data in performance of this Contract. 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).

34.2 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.

34.3 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."

34.4 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.

34.5 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.

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

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

b. the general policies in §4;

c. the Policies in §5;

d. the appropriate forms in Appendices "D", "E", "F" & "H"; and

e. the Supplemental Guidance in Appendices "J".

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

a. https://www.fbi.gov/services/cjis/cjissecurity-policy-resource-centerhttps://www.fbi.gov/services/cjis/cjissecurity-policy-resource-center.

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

35 NOTICES

35.1 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

STATE OF OKLAHOMA INFORMATION SECURITY POLICY, PROCEDURES AND GUIDELINES (PPG)

THIS PAGE LEFT BLANK

INTRODUCTION

This document is a compilation of the Information Security standards for the State of Oklahoma and provides an easy reference to the published security standards for the state.

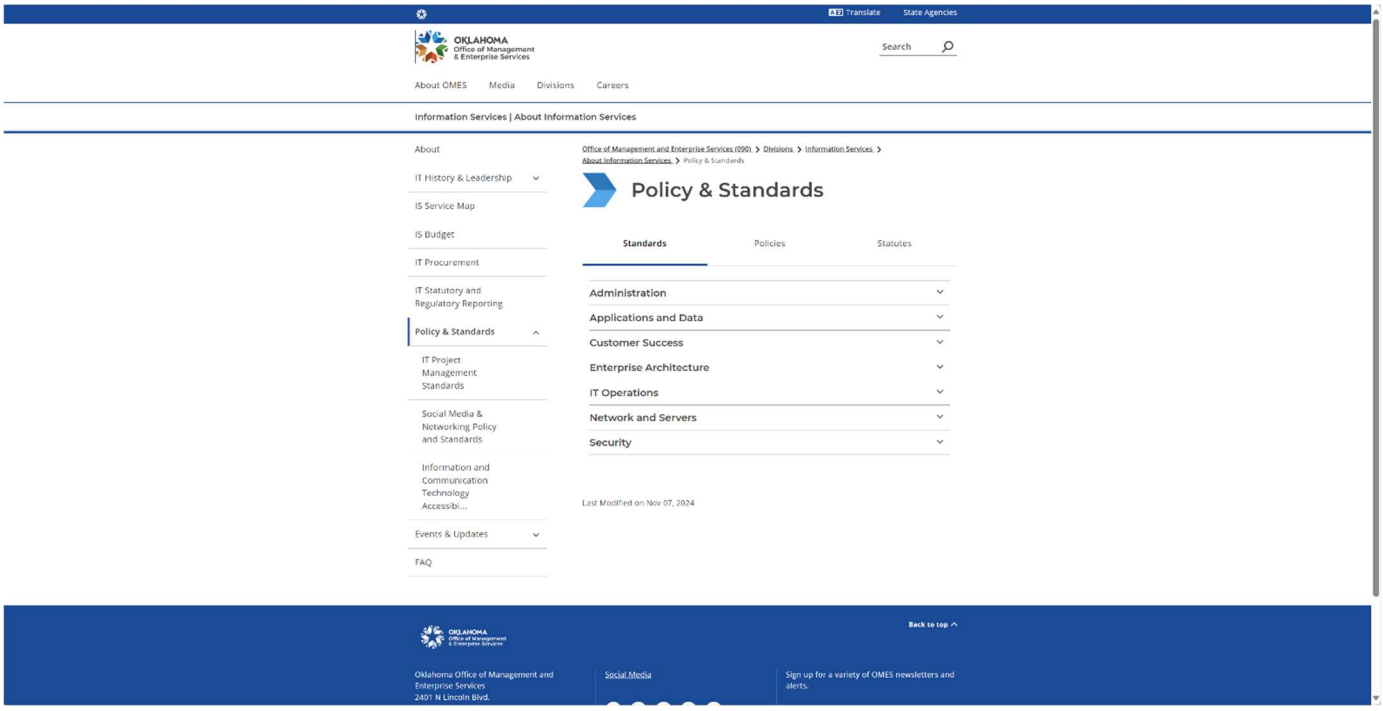
These standards describe the minimum acceptable security posture for state agency information systems, and for vendor partners providing either on-premises or cloud-based information systems to the state.

Certain legacy systems might not be capable of meeting these standards, or proposed solutions might require either a full or partial exception to one or more of the standards. In general, as long as proposed changes or exceptions do not result in an overall reduction of security policy, they will be granted in a timely manner to ensure that ongoing work is not unduly delayed. In these instances, requests should be made to Oklahoma Cyber Command for any exceptions as needed.

All information security standards are reviewed at least annually and updated as needed. The following link leads to all current standards for the State of Oklahoma approved by the OMES Chief Information Officer in accordance with Title 62 O.S. §§ 34.11.1 and 34.12 and Title 62 O.S. § 35.8.

Policy & Standards (oklahoma.gov).

ATTACHMENT D-1



OMES IS SECURITY STANDARDS

1. ACCESS CONTROL
   - Identity Management Standard.
   - Physical Access Control Standard.

2. AGENCY SECURITY
   - Non-unified agencies should follow the security standards listed on the OMES IS Policy & Standards website.

3. AWARENESS/TRAINING
   - Security Awareness Training Standard.

4. CENTRAL SECURITY PROGRAM
   - Security Services Standard

5. CONTROLS ON MALICIOUS SOFTWARE
   - Security Services Standard
   - Endpoint Protections and Connectivity Standard.

6. DISPOSAL OF MEDIA
   - Media Disposal Standard.

7. ELECTRIC COMMERCE SECURITY
   - Guidelines for the Evaluation of Electronic Data Interchange Products – NIST Special Publication 500-231.
   - Multifactor Authentication for E-Commerce - NIST SPECIAL PUBLICATION 1800-17.

8. EMAIL USAGE
   - Email Acceptable Use Standard.

9. EXCHANGES OF INFORMATION AND SOFTWARE
   - Exchanges of Information and Software Standard.
   - API Management Standard.
   - Batch File Transfer Standard.

ATTACHMENT D-1

Identity Management Standard

Introduction

User accounts are the only legitimate method by which OMES information systems may be accessed. OMES Information Services actively manages user accounts to prevent illegitimate use of state information systems. The use of authorization, identification and authentication controls ensure that only known users make use of state systems. Without these controls, the potential exists for information systems to be accessed illicitly, and the security of those information systems could be compromised.

Purpose

This document defines the types of user accounts managed by OMES IS.

Definitions

Affiliate – worker who is not a state employee but serves in a supporting role to a state agency's mission, typically at the county, local or municipality level.

Contractor – worker with economic independence who is in business for themselves but has been hired by the state to perform a particular function or produce a desired product.

Decentralized security representative (DSR) – individual, designated by the head of the agency, who is authorized to approve requests for their agency and state resources including creation of new user IDs, modification of user access and termination of user access.

Disabled account – inactive account requiring approval from an agency's DSR to enable.

Employee – worker who is economically dependent on the business of the employer.

Expired account – elapsed account for a contractor that has exceeded the configured expiration date.

Locked-out account – account that is blocked from user access and requires the OMES Service Desk to unlock (e.g. password expiration or a user incorrectly entering a password too many times).

Terminated account – User ID for an inactive affiliate, contractor or employee that has been disabled and had all permissions removed.

User ID – unique login ID assigned to each user of state systems.

Standard

- OMES IS ensures all users (affiliates, contractors and employees) are issued a user ID whose activity is uniquely identifiable on IT systems and is established through an authentication mechanism.
- Generic accounts are not permitted without CIO approval obtained through an exception request. Generic accounts have additional controls in place for accountability and a periodic review for their applicability.

- Access for new user ID access (onboarding) is requested via the OMES IS ticketing system and must be approved by the DSR.
- Access termination requests for departed employees (offboarding) must be submitted by the user's agency at the time of separation of employment and is requested via the OMES IS ticketing system.
- Contractor accounts expire quarterly, at which time the owning agency shall review and verify continued access requirements prior to requesting extension.
- User IDs not using the system for 60 days are verified against agency leave of absence reports prior to being disabled. Following a 30-day period of being disabled, the account is offboarded. Reactivation of the account requires an onboarding ticket to be submitted.
- Offboarded accounts are archived after a period of 30 days.
- To ensure proper access and continuity of business, individual user accounts shall not be used for shared resources, such as email or calendars. A dedicated resource for team or group activities must be requested.

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: 08/08/2023	**Review cycle:** Annual
Last revised: 10/07/2024	**Last reviewed:** 10/07/2024
Approved by: Joe McIntosh, Chief Information Officer	

OKLAHOMA
Office of Management
& Enterprise Services

Physical Access Control Standard

Introduction

The State of Oklahoma is committed to maintaining security of its facilities through strict control of building access. The state's environment requires controlled access to help ensure the safety of state employees and facilities from unlawful or unauthorized access. It is necessary to take appropriate measures to protect the confidentiality, integrity and availability of state data and resources.

Purpose

The document provides guidance on the layout of physical badges in order to be compatible with the statewide badging access control system and to define the underlining support model.

Standard

Physical access to non-public areas of state facilities is controlled by using state-issued badges that must be compatible with the statewide physical security control system. Badge format is uniform to ensure compatibility with the system, reduce the risk of counterfeit badges and facilitate accurate identification. Oklahoma Cyber Command manages and stores the format for all state-issued badges. Any variance to the approved format requires approval from the state Chief Operating Officer.

Due to the sensitivity of the information, the badge format and requirements are classified as confidential. Access to review the information may be granted as defined in the Confidential Standards Standard.

Additionally, all state facilities must adhere to the Physical Security Systems Standard. Only OMES IS authorized access control systems shall be used on state facilities as defined in the Physical Security Systems Standard. Oklahoma Cyber Command manages the state physical security 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.

References

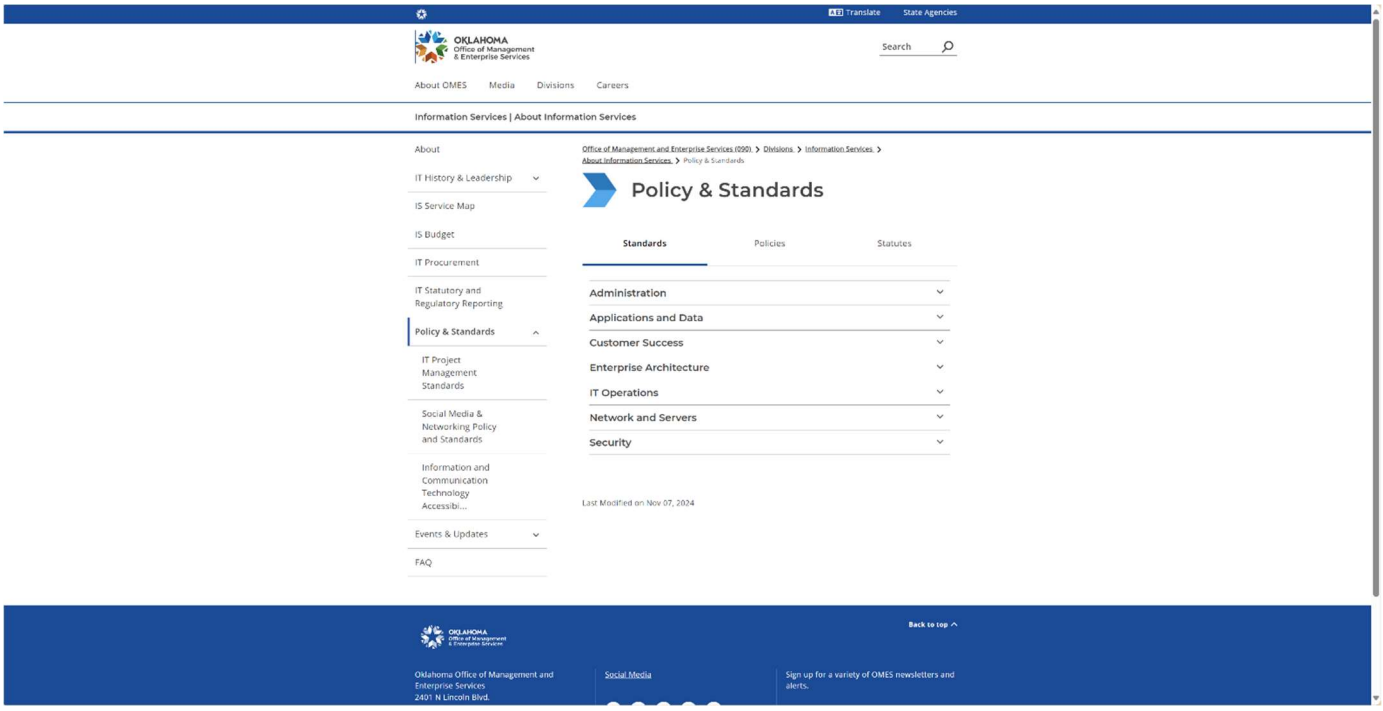
- Confidential Technology Standard.
- Physical Security Systems Standard – Confidential Standard.

Revision history

This standard is subject to periodic review to ensure relevancy.

Effective date: 03/02/2022	**Review cycle:** Annual
Last revised: 03/02/2022	**Last reviewed:** 08/23/2024
Approved by: Joe McIntosh, Chief Information Officer	

ATTACHMENT D-1



OKLAHOMA
Office of Management
& Enterprise Services

Security Awareness Training Standard

Introduction

OMES IS is responsible for developing, implementing and maintaining a security awareness and education training plan for all state agencies. The plan documents the process for employee and contractor training, education and awareness, as well as ensures all state employees and contractors understand their role in protecting the confidentiality, integrity and availability of state data.

Purpose

This document establishes the security awareness training standard for the State of Oklahoma. The purpose of awareness presentations is to focus attention on security and are intended to promote an environment recognizing IT security concerns and responding accordingly.

Awareness relies on reaching broad audiences, whereas training is more formal, with a goal of building knowledge and skills to facilitate job performance. Effective IT security awareness presentations must be designed. Awareness presentations must be on-going, creative and motivational, with the objective of focusing attention so the learning will be incorporated into conscious decision-making.

Definitions

User – All State of Oklahoma employees, contractors, board members or other persons authorized to connect to the state network.

Security education and awareness training – Also known as SEAT, is used to educate employees and contractors on how to protect state assets and information systems.

Phishing simulation – An internal control testing methodology which stimulates a real-life phishing attempt. Pushed enterprise-wide to gather metrics on click rates/trends to better inform the focus of training efforts.

Standard

All users are required to complete OMES provided SEAT training annually unless required to do so more frequently due to IS departmental requirements or elevated access.

All state agencies are responsible for ensuring all staff members complete security awareness training.

Additionally, the state has an established cadence for facilitating phishing simulations. By providing simulated phishing exercises, the state can obtain a direct measurement of employee understanding, as well as progress in user behavior. Continuous email phishing assessments can be effective by indicating patterns of phishing vulnerabilities within a department and identifying further awareness training needs.

Any users who fail simulated exercises are required to complete additional training. Repeated failures may be referred to the agency’s HR department and could result in loss of access.

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: 01/31/2021	**Review cycle:** Annually
Last revised: 05/16/2023	**Last reviewed:** 10/14/2024
Approved by: Joe McIntosh, Chief Information Officer	

ATTACHMENT D-1

OKLAHOMA
Office of Management
& Enterprise Services

Security Services Standard

Introduction

Oklahoma Cyber Command is responsible for protecting state users and their devices, networks, data and applications. Oklahoma Cyber Command's top priority is safeguarding the state's data and computer infrastructure against unauthorized data use, disclosure, modification, damage and loss. The OMES IS division supports Cyber Command's vision to provide leadership in the development, delivery and maintenance of cybersecurity, information security, risk management, enterprise fraud, physical security systems, compliance and privacy programs.

Purpose

This document defines the authority and services provided by Oklahoma Cyber Command.

Standard

Oklahoma Cyber Command is required to provide information security services to all state agencies, as defined in Title 62 O.S. §§ 34.11.1, including, but not limited to the following.

- Defensive services:
  - Endpoint management.
  - Virtual Desktop Infrastructure (VDI).
  - Endpoint Detection and Response (EDR).
  - Endpoint encryption.
  - Security assessment.
  - Secure Mail Gateway (SMG).
  - Secure Web Gateway (SWG).
  - Virtual Private Network (VPN).
  - Intrusion Prevention/Detection Systems (IPS/IDS).
  - Multi-Factor Authentication (MFA).
  - Privilege Access Management (PAM).
- Security education:
  - Security Education and Awareness Training (SEAT).
  - Simulated phishing campaigns.
- Offensive services:
  - Access control.
  - Threat intelligence collection, analysis, exploitation and production.
  - Forensics.
  - Investigations.
  - Threat assessments.
  - Threat monitoring and analysis.
  - Security Information and Event Management (SIEM).
  - Incident response.
  - Security assessment.
  - Facility Access Management Systems (FAMS).
  - Surveillance systems.
  - Physical Intrusion Detection Systems (IDS).
  - Facility project support.
  - Fraud prevention, detection, and investigation.
  - Third-party risk management.
  - Information sharing and analysis.

It is the responsibility of Oklahoma Cyber Command to interpret, design, implement and manage required regulatory controls. Staff performing similar functions within state agencies must collaborate and coordinate all activities with Oklahoma Cyber Command and defer interpretation of regulations and final decisions/solutions to Oklahoma Cyber Command. Through the Oklahoma Information Sharing and Analysis Center (OK-ISAC), Oklahoma Cyber Command maintains relationships and facilitates information sharing between regulatory bodies, including federal partners, industry oversight bodies and state/local law enforcement agencies to monitor cyber trends and help reduce the risk of cyber threats.

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

- Oklahoma OMES Cyber Command.
- OMES Unified but not Consolidated.

Revision history

This standard is subject to periodic review to ensure relevancy.

Effective date: 04/07/2022	**Review cycle:** Annual
Last revised: 08/25/2023	**Last reviewed:** 08/26/2024
Approved by: Joe McIntosh, Chief Information Officer	

ATTACHMENT D-1

OKLAHOMA
Office of Management
& Enterprise Services

Security Services Standard

Introduction

Oklahoma Cyber Command is responsible for protecting state users and their devices, networks, data and applications. Oklahoma Cyber Command's top priority is safeguarding the state's data and computer infrastructure against unauthorized data use, disclosure, modification, damage and loss. The OMES IS division supports Cyber Command's vision to provide leadership in the development, delivery and maintenance of cybersecurity, information security, risk management, enterprise fraud, physical security systems, compliance and privacy programs.

Purpose

This document defines the authority and services provided by Oklahoma Cyber Command.

Standard

Oklahoma Cyber Command is required to provide information security services to all state agencies, as defined in Title 62 O.S. §§ 34.11.1, including, but not limited to the following.

- Defensive services:
  - Endpoint management.
  - Virtual Desktop Infrastructure (VDI).
  - Endpoint Detection and Response (EDR).
  - Endpoint encryption.
  - Security assessment.
  - Secure Mail Gateway (SMG).
  - Secure Web Gateway (SWG).
  - Virtual Private Network (VPN).
  - Intrusion Prevention/Detection Systems (IPS/IDS).
  - Multi-Factor Authentication (MFA).
  - Privilege Access Management (PAM).
- Security education:
  - Security Education and Awareness Training (SEAT).
  - Simulated phishing campaigns.
- Offensive services:
  - Access control.
  - Threat intelligence collection, analysis, exploitation and production.
  - Forensics.
  - Investigations.
  - Threat assessments.
  - Threat monitoring and analysis.
  - Security Information and Event Management (SIEM).
  - Incident response.
  - Security assessment.
  - Facility Access Management Systems (FAMS).
  - Surveillance systems.
  - Physical Intrusion Detection Systems (IDS).
  - Facility project support.
  - Fraud prevention, detection, and investigation.
  - Third-party risk management.
  - Information sharing and analysis.

It is the responsibility of Oklahoma Cyber Command to interpret, design, implement and manage required regulatory controls. Staff performing similar functions within state agencies must collaborate and coordinate all activities with Oklahoma Cyber Command and defer interpretation of regulations and final decisions/solutions to Oklahoma Cyber Command. Through the Oklahoma Information Sharing and Analysis Center (OK-ISAC), Oklahoma Cyber Command maintains relationships and facilitates information sharing between regulatory bodies, including federal partners, industry oversight bodies and state/local law enforcement agencies to monitor cyber trends and help reduce the risk of cyber threats.

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

- Oklahoma OMES Cyber Command.
- OMES Unified but not Consolidated.

Revision history

This standard is subject to periodic review to ensure relevancy.

Effective date: 04/07/2022	**Review cycle:** Annual
Last revised: 08/25/2023	**Last reviewed:** 08/26/2024
Approved by: Joe McIntosh, Chief Information Officer	

OKLAHOMA
Office of Management
& Enterprise Services

Endpoint Protection and Connectivity Standard

Introduction

Oklahoma Cyber Command is responsible for protecting state users, their managed devices, and connectivity to data and applications. Oklahoma Cyber Command's top priority is safeguarding the state's data and computer infrastructure against unauthorized data use, disclosure, modification, damage and loss.

Purpose

This document defines the authority and services provided by Oklahoma Cyber Command.

Standard

Oklahoma Cyber Command is required to provide information security services to all state agencies, as defined in Title 62 O.S. §§ 34.11.1, including, but not limited to the following endpoint protection and connectivity services:

- Endpoint management and resilience.
- Endpoint Detection and Response (EDR).
- Endpoint encryption.
- Secure Web Gateway (SWG).
- Virtual Private Network (VPN).
- Multi-Factor Authentication (MFA).
- Privilege Access Management (PAM).
- Individual and shared account password management.
- Virtual Desktop Infrastructure (VDI).

It is the responsibility of Oklahoma Cyber Command to interpret, design, implement and manage required regulatory controls. Staff performing similar functions within state agencies must collaborate and coordinate all activities with Oklahoma Cyber Command and defer interpretation of regulations and final decisions/solutions to Oklahoma Cyber Command.

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

- Oklahoma OMES Cyber Command.

Revision history

This standard is subject to periodic review to ensure relevancy.

Effective date: 12/12/2023	**Review cycle:** Annual
Last revised: 12/12/2023	**Last reviewed:** 09/19/2024
Approved by: Joe McIntosh, Chief Information Officer	

OKLAHOMA
Office of Management
& Enterprise Services

Media Disposal Standard

Introduction
This document outlines the proper disposal of media to ensure confidential data, sensitive data and licensed software cannot be accessed by unintended persons.

Purpose
This standard establishes clear guidelines for the secure disposal of all forms of media containing sensitive information, with the aim of preventing unauthorized access and potential data breaches.

Definitions
- 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.
- Sensitive data – Confidential information that is stored, processed or managed by an organization that is confidential and only accessible to authorized users with proper permission, privilege or clearance to view.

Standard
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.

According to the Third-Party Cybersecurity Management Standard, the approved media disposal vendor must undergo routine managed assessments to identify any potential risk and ensure appropriate controls are in place to protect sensitive data.

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.

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

- Third-Party Cybersecurity Management Standard.
- NIST 800-88, Rev. 1, Guidelines for Media Sanitization.

Revision history

This standard is subject to periodic review to ensure relevancy.

Effective date: 07/26/2024	**Review cycle:** Annual
Last revised: 07/26/2024	**Last reviewed:** 07/26/2024
Approved by: Joe McIntosh, Chief Information Officer	

Guidelines for the Evaluation of Electronic Data Interchange Products

Published February 1, 1996

Author(s)
John J. Garguilo, Paul Markovitz
Citation Special Publication (NIST SP) - 500-231
Report Number 500-231
NIST Pub Series Special Publication (NIST SP) (https://www.nist.gov/nist-pub-series/special-publication-nist-sp)
Pub Type NIST Pubs
Information technology (https://www.nist.gov/topic-terms/information-technology) and Software testing (https://www.nist.gov/topic-terms/software-testing)

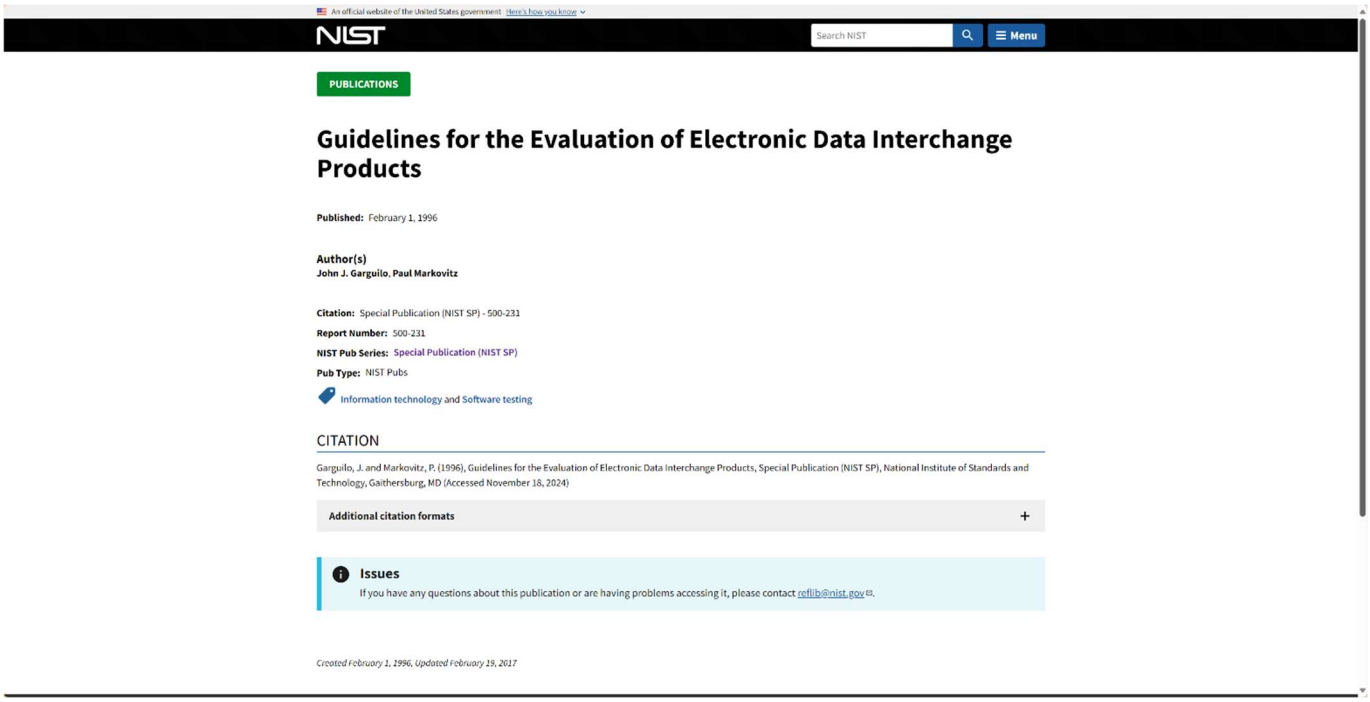
Citation

Additional citation formats

Issues

Created February 1, 1996, Updated February 19, 2017

ATTACHMENT D-1



ATTACHMENT D-1

PUBLICATIONS

NIST SP 1800-17

Multifactor Authentication for E-Commerce: Risk-Based, FIDO Universal Second Factor Implementations for Purchasers

Documentation Topics

Date Published: July 2019

Author(s)
William Newhouse (NIST), Brian Johnson (MITRE), Sarah Kinling (MITRE), Jason Kuruvilla (MITRE), Blaine Mulugeta (MITRE), Kenneth Sandlin (MITRE)

Abstract
As retailers in the United States have adopted chip-and-signature and chip-and-PIN (personal identification number) point-of-sale (POS) security measures, there have been increases in fraudulent online card-not-present electronic commerce (e-commerce) transactions. The risk of increased fraudulent... See full abstract

Keywords
electronic commerce (e-commerce) security; internet shopping security; multifactor authentication (MFA)

Control Families
None selected

DOCUMENTATION

Publication:
https://doi.org/10.6028/NIST.SP.1800-17
Download URL

Supplemental Material:
SP 1800-17 files
Project homepage

Related NIST Publications:
Project Description

Document History:
08/22/18: SP 1800-17 (Draft)
07/30/19: SP 1800-17 (Final)

TOPICS

Security and Privacy
access control, audit & accountability, authentication, risk assessment, security controls, system authorization

Technologies
hardware, mobile, software & firmware

Sectors
retail

HEADQUARTERS
100 Bureau Drive
Gaithersburg, MD 20899

PUBLICATIONS

NIST SP 1800-17

Multifactor Authentication for E-Commerce: Risk-Based, FIDO Universal Second Factor Implementations for Purchasers

Date Published: July 2019

Author(s)

William Newhouse (NIST), Brian Johnson (MITRE), Sarah Kinling (MITRE), Jason Kuruvilla (MITRE), Blaine Mulugeta (MITRE), Kenneth Sandlin (MITRE)

Abstract

As retailers in the United States have adopted chip-and-signature and chip-and-PIN (personal identification number) point-of-sale (POS) security measures, there have been increases in fraudulent online card-not-present electronic commerce (e-commerce) transactions. The risk of increased fraudulent online shopping became more widely known following the adoption of chip-and-PIN technology that increased security at the POS in Europe.

The NCCoE at NIST built a laboratory environment to explore methods to implement multifactor authentication (MFA) for online retail environments for the consumer and the e-commerce platform administrator. The NCCoE also implemented logging and reporting to display authentication-related system activity.

This NIST Cybersecurity Practice Guide demonstrates to online retailers that it is possible to implement open standards-based technologies to enable Universal Second Factor (U2F) authentication at the time of purchase when risk thresholds are exceeded.

The example implementations outlined in this guide encourage online retailers to adopt effective MFA implementations by using standard components and custom applications that are composed of open-source and commercially available components.

Keywords

electronic commerce (e-commerce) security; internet shopping security; multifactor authentication (MFA)

Control Families

None selected

DOCUMENTATION

Publication:
https://doi.org/10.6028/NIST.SP.1800-17
Download URL

Supplemental Material:
SP 1800-17 files
Project homepage

Related NIST Publications:
Project Description

Document History:
08/22/18: SP 1800-17 (Draft)
07/30/19: SP 1800-17 (Final)

TOPICS

Security and Privacy
access control, audit & accountability, authentication, risk assessment, security controls, system authorization

Technologies
hardware, mobile, software & firmware

Sectors
retail

OKLAHOMA
Office of Management
& Enterprise Services

Email Acceptable Use Standard

Introduction

Electronic mail is a highly efficient form of communication media, and when used appropriately, provides people with a means to facilitate business contact. However, this convenience also tempts users to experiment or take advantage of this media, resulting in email of unwelcome types (collectively known as Net Abuse). The improper use of email technology may jeopardize the integrity of state systems, security and service levels. Access to email is provided to employees and contractors to assist with conducting state business, and the use of email must not jeopardize the operation of systems or the reputation and/or integrity of the state.

Email is a critical mechanism for business communication at the State of Oklahoma. Use of state email systems and services are a privilege, not a right.

Purpose

This document outlines acceptable use of email for State of Oklahoma employees and contractors.

Standard

As with other state resources, email is made available to employees and contractors in support of each agency's mission. Use of state email services is intended to be in furtherance of such goals and mission.

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.

Users should be aware the state's officers and employees are subject to the provisions of the Oklahoma Open Records Act. There is no privacy associated with use of state email resources. 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.

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: 4/4/2022	**Review cycle:** Annual
Last revised: 10/18/2022	Last Reviewed Date: 09/19/2024
Approved by: Joe McIntosh, Chief Information Officer	

ATTACHMENT D-1

OKLAHOMA
Office of Management
& Enterprise Services

Exchanges of Information and Software Standard

Introduction

Information can be vulnerable to unauthorized access, misuse or corruption physical transport, for instance when sending media via the postal service or via courier. As such, media being transported must be protected from unauthorized access, misuse or corruption.

Purpose

Exchanges of information and software between organizations should be controlled and compliant with any relevant legislation.

Standard

Exchanges of information and software should be carried out on the basis of agreements. Procedures and standards to protect information and media in transit must be established. The business and security implications associated with electronic data interchange, electronic commerce and electronic mail and the requirements for controls should be considered.

Agreements, some of which must be formal, must be established for the electronic or manual exchange of information and software between organizations. The security content of such an agreement should reflect the sensitivity of the business information involved. Agreements on security conditions should include:

- Responsibilities for controlling and notifying transmission, dispatch and receipt.
- Procedures for notifying sender, transmission, dispatch and receipt.
- Minimum technical standards for packaging and transmission.
- Courier identification standards.
- Responsibilities and liabilities in the event of loss of information.
- Information and software ownership and responsibilities for information protection, software copyright compliance and similar considerations.
- Technical standards for recording and reading information and software.
- Any special controls that may be required to protect sensitive items, such as cryptographic.

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

- Information Security Policy, Procedures and Guidelines.

Revision history

This standard is subject to periodic review to ensure relevancy.

Effective date: 09/06/2024	**Review cycle:** Annual
Last revised: 09/06/2024	**Last reviewed:** 09/06/2024
Approved by: Joe McIntosh, Chief Information Officer	

ATTACHMENT D-1

API Management Standard

Introduction

MuleSoft is the standard for integrations, ESB, API management, API gateway, API catalog and message brokers at OMES.

Purpose

The purpose of this document is to provide a roadmap of standard policy and best practices when developing on the MuleSoft platform for the state. This standard defines and outlines the procedures MuleSoft developers should use when building integrations, APIs, deploying apps, publishing apps to Exchange, managing consumption and monitoring and alerting when developed by or for OMES.

Definitions

ESB – Enterprise Service Bus.
API – Application Programming Interface.
MuleSoft – Software for connecting SaaS and enterprise applications in the cloud and on-premises.
C4E – Center 4 Enablement.
VPC – Virtual Private Cloud.
CloudHub – Integration platform as a service.
HTTP – Hypertext Transfer Protocol
TLS – Transport Layer Security
MUnit – Testing software designed to test individual units of source code to see if they are fit for use or not.

Standard

General

- The State of Oklahoma provides the Anypoint platform to all agencies within the MuleSoft Anypoint organization called ok-omes.
- The Anypoint platform offers agencies separate tenants that are independently accessed through business groups and are secured trough the Teams feature.
- Mule applications run in CloudHub or on-premises with approval from C4E.
- New Mule applications shall be developed using the latest version.
- Existing Mule applications are expected to run on a version of Mule that is covered by extended support.

Architecture

- Each agency defines local environments in its own Anypoint business group.
    - This allows agencies to adapt to the logical Anypoint environment construct to their specific needs.
- MuleSoft applications need to follow the design patterns developed by the OMES architecture group to optimize experience, scalability and promote reuse.
- The architecture of the current VPC configuration is available for review and discussion during the development on-boarding and is available here.
- Any proposed platform solutions need to be presented and approved by the C4E.

ATTACHMENT D-1

Network

- Mule applications are deployed in one of two dedicated OMES AWS Virtual Private Clouds that are USA based.
- OMES provides one VPC for production applications and another for non-production applications.
- Each agency must designate the non-production VPC as its default VPC and explicitly map the production environment to the production VPC.
- Each VPC configures firewall rules to specifically allow inbound traffic to the CloudHub workers where the Mule applications run.
    - These firewall rules apply to the entire VPC and therefore affect all agencies' business groups.
- Each VPC is connected to the OMES network using IPSec.
    - As additional OMES networks require connectivity with CloudHub VPCs, the IPSec tunnel routing must be explicitly updated to including appropriate routes.
- Each agency's APIs are access to subdomains that reflect the agency's name.
    - E.g., oesc.oklahoma.gov

Security

- User access to the Anypoint platform control plane is governed by security roles and permissions mapping.
    - The latest documented guidelines are located here.
    - Inbound and outbound traffic to each VPC, which constitutes the runtime plane, is principally allowed in OMES Palo Alto firewalls that are owned by Network Operations.
- The CloudHub Dedicated Load Balancer must be configured with OMES-signed SSL certificates that are provisioned by the OMES Entrust Tenant.
- To make an API accessible, an OMES Anypoint administrator must configure a specific mapping rule in the CloudHub Dedicated Load Balancer.
- All publicly available APIs require HTTP over TLS 1.2.
- A Mule application should call another Mule API through the CloudHub Dedicated Load Balancer using HTTP over TLS 1.2.
- Mule APIs are, by default, reachable from the public internet.
- Exposing Mule APIs to external consumers over the internet is a controlled process that requires the documented approval of CyberCommand.
- APIs must be protected by a client ID enforcement policy or a suitable alternative. Using a dedicated set of credentials that is issued by the Anypoint platform and is maintained by Anypoint platform users is recommended.
- Alternative out-of-the-box or custom security policies may be configured with the approval of CyberCommand.
- Credentials are issued by the Anypoint platform to an Anypoint user.
    - Specifically, production credentials are encrypted in source-code configuration files in GitHub and are included in the deployed application archive in their encrypted form.
- Mule application credentials are encrypted in source-code configuration files in GitHub and are included in the deployed application archive in their encrypted form.
- Each agency has one or more production encryption keys that are used to encrypt secrets for all applications controlled by that agency.
- Azure Key Vault is approved as a preferred alternative to encrypting secret in source code.
- Each agency has a set of Azure Key Vaults that are environment specific.
- Mule applications use agency-specific service principles to differentially enable access to production and non-production key vaults.

- Users access the Anypoint Platform Control Plane based on their group membership in Azure Active Directory.
- Azure DevOps agents use the Anypoint platform API to deploy Mule applications with a connected app that acts on its own behalf.
- Deployment to production is only performed through the Azure DevOps release pipeline.
    - Deployment to test/user access test should be performed through the Azure DevOps release pipeline.

Development

- MuleSoft integrations should be designed according to API Led Connectivity.
- APIs are implemented as Mule applications using APIKit.
- Mule applications include automated tests within MUnit.
- A default template for an OMES Mule application is in Anypoint Exchange.
- Agency-specific templates should be published to their respective Anypoint Exchange business group.
- Published guidelines for logging and error handling may be found here.
- All Mule application source code is maintained in the agency's assigned GitHub.com tenant or a shared OMES-owned tenant.

Development Environment

- Anypoint Studio is used to develop Mule applications using OMES issued devices or virtual machines.
    - The minimum version of Anypoint Studio is 7.12.0.
    - Download it here.
- Anypoint Studio is specifically configured to support the development of OMES compliant Mule applications.

Monitoring

- Applications are expected to log to OMES Splunk, CloudHub and Anypoint Monitoring.
- CloudHub applications are expected to log to Splunk using the OMES Splunk System API and not all logs are expected to be directed to Splunk.
- Applications must avoid logging sensitive information to any of the log destinations.
- Logs should be traceable across Mule applications and, where possible, more broadly across the entire network.
    - i.e., API clients and backends.
- The CloudHub worker monitoring agent should be enabled for each CloudHub application.

CICD

- Applications are built using Apache Maven leveraging a MuleSoft specific plugin.
- Applications are built in Azure DevOps build pipelines and are deployed by Azure DevOps release pipelines.
- Deployment to production requires an approved change control record.
- Steps to build and prepare release in Azure DevOps are provided here and here.

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

- Mule Application Development.

Revision history

This standard is subject to periodic review to ensure relevancy.

Effective date: 1/31/2023	**Review cycle:** Annual
Last revised: 1/18/2023	**Last reviewed:** 8/14/2023
Approved by: Joe McIntosh, Chief Information Officer	

ATTACHMENT D-1

Batch File Transfer Standard

Introduction

This standard specifies batch file transfer standards for Oklahoma state agencies. The standard describes tools included in the state reference architecture. This document and all information contained within are applicable to all State of Oklahoma agencies and partners.

Modern applications usually interoperate with other applications using modern interfacing methods, such as application programming interfaces or APIs. However, when the state's legacy applications were developed, the usual way of sharing data between applications was the basic file transfer process. The state still has many applications that rely heavily on file transfers to share data.

The most common method for sending these files and receiving files from other applications is using the file transfer protocol, or FTP. FTP does not encrypt the data during transit whereas secure FTP (e.g. SFTP, SCP, etc.) does encrypt data during transit.

Whenever business requirements call for a new file transfer process, the development and implementation of the process often spans multiple OMES IS departments and is very laborious and time consuming.

The basic file transfer protocols are intentionally designed to not abend when the transfer does not work. This causes issues for processes that depend upon successful file transfers because downstream processes continue to run even when the transfer failed.

Today, the state and its agencies have a large number of file transfers but no coherent or consistent way of managing them. There is no established way to inventory all the file transfers that are in production, how much data is being moved, where the data is coming from, where it is going, what type of data is being moved, who owns the process, etc.

Purpose

The purpose of this document is to describe the state standard for batch file transfers. The goal of this standard is to control costs, reduce technical debt, reduce file transfer sprawl, enable creation of file transfers in a consistent, standardized manner, reduce time needed to create new file transfers, enhance the state's ability to support file transfers and collect metrics around file transfers. Developing on common tools and platforms creates shared context for understanding state data and facilitates knowledge transfer between agencies, departments and teams.

Definitions

FTP – File transfer protocol. A method of sending one or more files from one computer to another. The data is not encrypted during transit.

MFT – Managed file transfer. A software tool designed specifically to facilitate file transfers.

SCP – Secure copy. A method of sending one or more files from one computer to another. The data is encrypted during transit.

SFTP – Secure file transfer protocol. A method of sending one or more files from one computer to another. The data is encrypted during transit.

Standard
Agencies developing file transfers should utilize one of the tools from our reference architecture.

- File transfers must be secured.
- File transfers must have retry functionality.
- File transfers must have alert notification functionality in the event of failure.
- In the event of a failure, the file transfer system must have the ability for an operator to retry any failed jobs after corrections have been made.
- File transfers must have the ability to log anomalies, errors and failures to Splunk or current log/event monitoring system.
- File transfer processes must be documented in a central repository.
- File transfers must have the ability to promote configuration changes to multiple environments.

The two MFT tools supported by OMES are: MuleSoft and MOVEit.

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: 05/24/2022	**Review cycle:** Annual
Last revised: 05/24/2022	**Last reviewed:** 09/24/2024
Approved by: Joe McIntosh, Chief Information Officer	

10. THIRD PARTY RISK
- IT Contractor Requirement Standard.
- Third-Party Cybersecurity Management Standard.
- Offshore Data Storage Standard.

11. HOSTING AGENCY SECURITY
- Workstation Standard.
- Mobile Services Standard.
- Mobile Device Platform Standard.
- State Data Platform Standard.
- Data Storage Standard.
- Enterprise Reference Architecture Standard.

12. INCIDENT MANAGEMENT & SECURITY REPORTING PROCEDURE
- Incident Response Standard.

13. INFORMATION ACCESS
- Decentralized Security Representative (DSR) Standard.

14. INFORMATION AVAILABILITY
- Data Archiving Standard.
- Data Retention Standard.
- Data Storage Standard.

15. INFORMATION CONFIDENTIALITY
- Password Requirements Standard.
- Identity Management Standard.

16. INFORMATION CONTENT
- System and Information Integrity Standard.

17. INTRUSION DETECTION SYSTEMS (IDS)
- Network Protection Standard.

18. MANAGEMENT OF REMOVABLE COMPUTER MEDIA
- Media Disposal Standard.

19. PERSONAL COMPUTER USAGE
- Personal Device Standard.
- System Acceptable Use Standard.

ATTACHMENT D-1

IT Contractor Requirements Standard

Introduction
OMES IS is responsible for the IT onboarding process for State of Oklahoma employees and contractors. To support this effort, as well as promote consistency, the following standard has been established for the onboarding of contractors.

Purpose
This document outlines the standards for onboarding contract employees to ensure a consistent onboarding process.

Definitions
Least privilege – A security best practice to limit user privileges to only have access to what they need to perform their tasks and no more.

Standard
Any supplier accessing, processing, transmitting or storing state data must have their internal security controls appropriately evaluated and undergo a third-party risk assessment as defined in the Third-Party Cybersecurity Management Standard.

Agencies must ensure contractors comply with state policies, procedures and standards. Regardless of procurement method, prior to establishing a contractual relationship Oklahoma Cyber Command must evaluate contractors and/or organizations for potential security risks. Contracts or agreements, which may specify additional security requirements, must be completed and signed before a contractor is granted privileges for access to, or provisioning of, state information or resources.

Agencies negotiating, administering or managing contracts must ensure contractors comply with all applicable state policies, procedures, standards and with the terms specified in the applicable contract(s).

An OMES IS service division manager must be identified as an account sponsor. The service division manager is responsible for initiating the onboarding process.

Naming standards for contractors are in place to ease recognition of contract resources.

Contractors shall employ rule of least privileges. Additionally, contractor accounts shall be monitored by Customer Success – Provisioning to ensure utilization. Any account not using the system for 60 days will be disabled. After remaining in a disabled state for 30 days, the account will be offboarded for non-use. Semi-annual audits of contractor accounts will be provided to the contractor point of contact.

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

- Third-Party Cybersecurity Management Standard.
- Background Check Standard.
- Security Awareness Training Standard.

Revision history

This standard is subject to periodic review to ensure relevancy.

Effective date: 01/31/2022	**Review cycle:** Annual
Last revised: 10/17/2024	**Last reviewed:** 10/17/2024
Approved by: Aleta Seaman, Interim Chief Information Officer	

ATTACHMENT D-1

Third-Party Cybersecurity Management Standard

Introduction

OMES Information Services is committed to preventing incidents that may impact the confidentiality, integrity or availability of information assets through third-party cyber management (TPCM) for the State of Oklahoma. Third-party cyber management is a critical component of the OMES IS information security program, which helps ensure any risk to confidentiality, integrity and/or availability is identified, analyzed and maintained at acceptable levels.

State policy requires the performance of regular security reviews to identify risk and ensure appropriate controls are in place. TPCM security reviews allow the alignment of information security with business objectives and regulatory requirements. Identifying information security risk and control requirements from the onboarding of a vendor is essential and far less costly than retrofitting or addressing the impact of a security incident. Furthermore, these security reviews allow management to prioritize and focus on areas that pose the most significant impact on critical and sensitive information assets, providing the foundation for informed decision-making regarding cybersecurity.

OMES IS considers current and potential vulnerabilities, the current threat landscape and current/future security controls in place in the state's IT infrastructure. These inputs help determine the resulting level of risk posed to information, information systems, processes and individuals that support business functions and the citizens of Oklahoma. While TPCM and related security reviews takes many forms (e.g., security assessments, software reviews, risk analysis platform, configuration analysis, and/or vulnerability scanning and testing), they all have the same goal: to improve overall security posture by identifying and acting on current and potential risk. An entity can never truly eliminate risk but can take steps to mitigate it.

As per OMES IS policy, any vendor that is or will be hosting, storing, transmitting, processing and /or accessing State of Oklahoma data or having direct access to State of Oklahoma information systems on premises must be properly assessed and managed for risk and undergo a TPCM security review as part of its business partnership life cycle.

Purpose

This document establishes the requirement for TPCM security reviews for vendors that are or will be hosting, accessing, processing, transmitting or storing State of Oklahoma data in compliance with OMES IS security policies, standards and procedures.

Definitions

Vendor – Any supplier, contractor, service provider, consultant or any other individual and/or organization external to state government providing services on behalf of, for, or as an agent of state government.

Tier 3: Low criticality – Any system or data intended for public disclosure. The loss of confidentiality, integrity or availability of the system or data would have no adverse impact on safety, finances or reputation.

Tier 2: Medium criticality – Any system or data not generally available to the public. The loss of confidentiality, integrity or availability of the system or data could have a mildly adverse impact on safety, finances or reputation.

Tier 1: High criticality – Any system or data protected by law or regulation (e.g., FTI, CJI, PHI, PII and PCI). The loss of confidentiality, integrity or availability of the data or system could significantly and adversely impact safety, finances or reputation. This type of risk requires the state to self-report to the regulatory entity and/or notify the individual if data is inappropriately accessed.

Standard

The state agency shall categorize data as confidential by system owners, including protected health information and personally identifiable information, in accordance with applicable federal and state laws, directives, standards, guidance, policies and regulations.

OMES IS shall conduct third-party cybersecurity reviews. The review should address the likelihood and magnitude of harm should there be unauthorized access, use, disclosure, disruption, modification or destruction of the information system and the information it processes, stores or transmits. Additionally, these guidelines apply to risk assessments:

- OMES IS shall document the results of the annual security review.
- OMES IS shall review risk analysis results annually.
- OMES IS shall disseminate security review results to stakeholders.
- OMES IS shall update the third-party security review annually or whenever there are significant changes to the information system or environment of operation (including the identification of new threats and vulnerabilities) or other conditions that may impact the system's security state.

All vendors given access to State of Oklahoma information, information systems or information assets must complete a security review. The purpose of the review is for the State of Oklahoma to identify and manage the risk stemming from the business partnership.

A vendor is required to complete a TPCM security review if hosting, accessing, processing, storing or transmitting State of Oklahoma data. The review is not restricted to a specific service or solution but is for the vendor to be assessed from an internal security standpoint (organizational policies, standards, procedures, guidelines and controls). The security of hardware, software, IT solutions and/or IT services being acquired should have no bearing on the enterprise security controls of the vendor.

Industry-standard assessments and certifications may be used in lieu of the OMES IS review if they are substantially similar in structure and content. The following industry- standard assessments and certifications are approved:

- SIG Lite for Tier 2 and 3 vendors.
- SIG Core for Tier 1, 2 and 3 vendors.
- CSA CAIQ v3.1 for Tier 1, 2 and 3 cloud service providers.
- CSA CCM/CAIQ v4 for Tier 1, 2 and 3 cloud service providers.
- FedRAMP for Tier 1, 2 and 3 cloud service providers.
- StateRAMP for Tier 1, 2 and 3 vendors (preferred for cloud service providers).
- ISO 27001 for Tier 2 and 3 vendors.
- HITRUST for Tier 1, 2, and 3 vendors.
- AICPA SOC 2 Type II for Tier 1, 2, and 3 vendors (Must cover all 5 Trust Services Criteria).
- DoD CMMC 2.0 Level 2 or 3 for Tier 2 and 3 vendors.

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 Special Publications: NIST SP 800-53a –Risk Assessment, NIST SP 800-12, NIST SP 800-30, NIST SP 800-39, NIST SP 800-40, NISTSP 800-70, NIST SP 800-100 and NIST SP 800-115; NIST Federal Information Processing Standards 199.
- Attachment D State of Oklahoma IT Terms.
- State of Oklahoma Information Security Policy, Procedures, Guidelines.
- Cloud Security Alliance (CSA).
- Shared Assessments (SIG).
- FedRAMP Authorization Management Program.
- StateRAMP.
- International Organization of Standardization (ISO).
- DOD CMMC 2.0.

Revision history

This standard is subject to periodic review to ensure relevancy.

Effective date: 11/06/2020	**Review cycle:** Annual
Last revised: 04/18/2024	**Last reviewed:** 08/28/2024
Approved by: Joe McIntosh, Chief Information Officer	

OKLAHOMA
Office of Management
& Enterprise Services

Offshore Data Storage Standard

Introduction
Data is a valuable asset to business and government, and as such, it is imperative that state data be stored securely. Offshore data storage is a popular industry option, particularly for cloud storage. However, because other countries and regions use different guidelines, international laws and regulations, offshore storage options may be less secure and more vulnerable to security incidents than data stored within the United States. Offshore data storage also increases the risk that data stored offshore could be subject to the sovereign control of another country. To reduce the security and jurisdictional concerns inherent to offshore data storage, OMES requires state data to remain within the boundaries of the U.S.

Purpose
This document establishes the standard for state data to be stored within the boundaries of the U.S.

Definitions
Offshore – A location that is outside the physical borders of the U.S.

Standard
OMES requires all state data to be hosted, stored, processed, transmitted, accessed and disposed of by approved vendors within the boundaries of the U.S.

State agency systems and data shall not be accessible from outside the physical boundaries of the U.S. Any requests for exemption to this standard require coordination through the OMES chief information security officer.

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: 08/29/2022	**Review cycle:** Annual
Last revised: 08/29/2022	**Last reviewed:** 08/24/2024
Approved by: Joe McIntosh, Chief Information Officer	

ATTACHMENT D-1

Workstation Standard

Introduction

This standard is intended to support the business needs for all State of Oklahoma agencies by:

- Bringing a systematic approach to the lifecycle of computer equipment.
- Ensuring hardware and software requirements are met.
- Standardizing equipment to maximize maintenance and support efforts.
- Providing a cost-effective solution while still accommodating business needs.
- Validating all approved workstations to ensure security standards are met.
- Ensuring only approved workstation configurations and associated services are procured.

Purpose

OMES has an established list of standard hardware configurations to promote the standardization of equipment, improve the security of the state's computing environment and realize economies-of-scale cost savings in the procurement and maintenance of computing equipment.

Definitions

Workstation – A computer device that an end user uses to complete work, including any desktop, laptop, tablet or virtual desktop hardware.

Golden software image – A single, base configuration for operating systems, applications and security tools upon which other packaged software may be installed via the state's client management system.

Business class – Devices designed for higher performance and longer service that are securely sourced and allow on-site certified maintenance. They typically have longer warranties and are known to be compatible with the state's infrastructure with minimum complexity.

Standard

Workstations must be procured from one of the designated configurations approved by OMES IS and deployed via an approved service provider.

Deployment of a workstation is included in the procurement.

Hardware standards review cycle

OMES reviews the workstation standards on a regular basis, or as information becomes available from the vendor, to align with agency business needs, ensuring that vendors still support the equipment, verifying pricing and updating the model version if necessary.

Hardware refresh cycle

All devices, whether purchased or leased, must be refreshed on a three-year cycle.

ATTACHMENT D-1

Hardware specifications
Every device acquired on behalf of the State of Oklahoma must adhere to the following specifications:

- Manufacturer – Dell, Apple, Microsoft or Panasonic.
- Operating system – Windows 10 Enterprise 64-bit or newer, or the latest version of macOS.
- Ability to add MacBooks to Apple Business Manager.
- Processor – Intel i7 minimum.
- Memory – 16GB minimum. 32GB is preferred.
- Hard drive size – Solid state drive or M2 drive with minimum storage size of 500GB.
- Wi-Fi capability on each device.
- TPM enabled in the BIOS.
- Security product - Absolute Resilience Premium three-year license – must be factory-installed.
- Enterprise-class system model.
- Must be covered under the manufacturer's original warranty. For leased devices, the manufacturer's extended warranty must be active for the life of the lease.
- State agency purchase or lease of devices must be through Insight or Dell.

For information on mobile devices, refer to the Mobile Device Platform Standard.

Software specifications.
Every device acquired on behalf of the State of Oklahoma must be compatible with the state's golden software image. Agency-specific software requests should be submitted to the OMES Service Desk for packaging for distribution via the state's endpoint management solution.

The state's golden software image shall be installed on all devices acquired on behalf of the State of Oklahoma to ensure supportability, inclusion of all required security measures and compliance with enterprise licensing requirements.

Local accounts are prohibited without the written consent of the state CIO.

Users requiring remote desktop services shall utilize the state's virtual desktop environment utilizing the state's golden software image. Agency-specific software requests should be submitted to the OMES Service Desk for packaging for distribution via the state's endpoint management solution.

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

- Mobile Device Platform Standard.

Revision history

This standard is subject to periodic review to ensure relevancy.

Effective date: 04/29/2022	**Review cycle:** Annual
Last revised: 04/30/2024	**Last reviewed:** 07/11/2024
Approved by: Joe McIntosh, Chief Information Officer	

ATTACHMENT D-1

Mobile Services Standard

Introduction

In February 2012, Congress enacted The Middle-Class Tax Relief and Job Creation Act of 2012, containing landmark provisions to create a nationwide public safety broadband network that provides law enforcement, firefighters, emergency medical service, emergency managers and 911 with wireless broadband communication services on a nationwide network. The laws governing the framework for the deployment of this network are the new First Responder Network Authority known as FirstNet, an independent authority within the National Telecommunications and Information Administration.

Purpose

FirstNet holds the spectrum license for the network and is charged with taking all actions necessary to build, deploy and operate the network in consultation with federal, state, tribal and local public safety entities and other key stakeholders.

FirstNet allows more than 60,000 public safety agencies to take advantage of expanded coverage and capacity based on commercial standards. The additional benefits of this program include:

- Make first responders safer.
- Improve communication tool security and effectiveness.
- Enhance data and information sharing during daily, emergency or joint operations.
- Promote and sustain partnerships with responders and responder organizations across the nation at all levels.
- Help investigate cybercrime and cases involving digital evidence.
- Secure 911 emergency call systems from cyberattacks.

Extended primary users such as agencies or organizations that provide public safety services in support of the primary users may also use FirstNet.

Standard

FirstNet is the service standard for all state agencies eligible to participate. FirstNet is monitored and managed by public safety personnel for the State of Oklahoma.

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

- FirstNet website.

Revision history

This standard is subject to periodic review to ensure relevancy.

Effective date: 12/16/2021	**Review cycle:** Annual
Last revised: 10/20/2022	**Last reviewed date:** 07/11/2024
Approved by: Joe McIntosh, Chief Information Officer	

ATTACHMENT D-1

Mobile Device Platform Standard

Introduction
OMES Information Services takes all necessary measures to ensure the security and acceptable performance of the State of Oklahoma mobile device network. This standard defines the criteria for accessing state information assets from mobile devices. Any mobile device connecting to state information assets must comply with this standard, regardless of whether the device is personal or state-issued.

Purpose
This document establishes guidance for mobile technology management of state-issued and personal-owned mobile devices.

Definitions
Mobile device management – The software and service provided device management, security and monitoring in order for the smart device to be eligible to connect to the state network.

Mobile device – For the purpose of this standard, a portable computing device that: (i) has a small form factor such that it can easily be carried by a single individual; (ii) is designed to operate without a physical connection; (iii) possesses local, non-removable data storage; and (iv) is powered-on for extended periods of time with self-contained power source.

Microsoft Intune – Cloud-based, endpoint management solution. It manages user access to organizational resources and simplifies app and device management across many devices, including mobile devices, desktop computers and virtual endpoints.

Standard
The state standard for mobile device management is Microsoft Intune.

To mitigate security threats, OMES has established minimum hardware and software requirements for state-issued mobile devices. The mobile device standard for the State of Oklahoma is Apple iOS devices. Apple iOS devices are the only mobile devices authorized to authenticate to the state network and access resources. Any authorized device authenticating to the state network must be running an iOS version for which Apple still offers standardized technical support. In addition, all mobile device hardware must be within two major releases and must be purchased from a service provider listed on the statewide contract.

To mitigate many of the risks associated with using mobile devices, OMES IS utilizes a mobile device management solution to manage a device's authorized access to state network, systems and other enterprise resources. All state mobile devices used to access, transmit or store state data are required to have the state MDM product, Microsoft Intune, installed. In addition, users may not take steps to circumvent the security policies put in place by the MDM software.

Any exceptions to the above require annual state CIO approval.

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

1. Statewide Mobile Device Contract – SW1012.
2. OMES Personal Device Standard.

Revision history

This standard is subject to periodic review to ensure relevancy.

Effective date: 12/16/2021	Review cycle: Annual
Last revised: 10/04/2023	Last reviewed date: 07/11/2024
Approved by: Joe McIntosh, Chief Information Officer	

ATTACHMENT D-1

State Data Platform Standard

Introduction
Google Cloud Platform is the state data platform for the State of Oklahoma Modern Data Strategy.

Purpose
The purpose of this document is to describe and identify the state standards for GCP and to outline its intended use as the established SDP.

Definitions
Google Cloud Platform – Provides infrastructure as a service, service platform and serverless computing environments, in addition to other cloud service offerings.

BigQuery – A GCP Scalable managed enterprise data warehouse for analytics.

Hub and spoke model – A distribution method where a centralized hub exists. Data can be shared or exchanged upon registration and approval by the authorized agency data owner. Data must be stored in an agency spoke to be registered on the hub. A centralized data catalog provides the ability for an authorized consumer to view the schema. Agencies may use their spoke functionalities without registering or sharing data in the hub. In GCP, agency spokes are containerized and masked from other agencies or individual view.

Standard
The primary purpose of the SDP is to provide a secure platform to replicate critical data sets from source to an agency spoke that delivers meaningful insight, improve quality, accuracy and timeliness of the key performance indicator's approved analytics and visualization, and enable AI/ML in a multi-cloud environment. However, as approved GCP/SDP may be utilized for transactional datasets allowing for agencies to rapidly scale application and respond to market shifts delivering cloud-based services.

All access to GCP must be in accordance with the state security provisioning standards, active directory and Azure Active Directory. Per state access provisioning, all GCP access service accounts must be provided in accordance with an established provisioning standard with a ServiceNow request ticket.

All agencies must procure GCP services, either as a pay-as-you-go agreement or a negotiated enterprise agreement to control overage charges. Agency data is prohibited from being stored on GCP outside of the approved ok.gov domain. Exceptions must receive written approval from the State of Oklahoma chief information officer.

To achieve maximum benefits from the GCP environment, the following services are approved but not limited to:

- Compute.
    - App Engine.
    - Google Kubernetes Engine.
    - Cloud Functions.
    - Cloud Run.

- Storage and databases.
    - Cloud Storage.
    - Cloud SQL.
    - Cloud DataStore.
- Big data.
    - BigQuery.
    - Cloud DataFlow.
    - Cloud DataProc.
    - Cloud Composer.
    - Cloud Dataprep.
    - Cloud Pub/Sub.
    - Cloud Data Studio.
- Management tools.
    - Cloud Console.
    - Cloud Shell.
    - Operations Suite.
    - Cloud Deployment Manager.
- Identity and security.
    - Cloud Identity.
    - Cloud IAM.
    - Cloud Data Loss Prevention.
    - Cloud Security Command Center.
- Location of data and procedures: Critical production data and processes must be stored and replicated in at least two regional zones to ensure data sets and processes remain operational. Per federal, state and business classification and compliance standards, all agency data must be stored on U.S. soil and be hosted in the following approved regional priorities:
    - us-central.
    - us-east.
    - us-west.
    - us-**.

  Data may only be deployed to other GCP zones outside the U.S. upon written approval from the State of Oklahoma chief information officer.

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: 03/21/2022	**Review cycle:** Annual
Last revised: 06/14/2024	**Last reviewed:** 06/14/2024
Approved by: Joe McIntosh, Chief Information Officer	

OKLAHOMA
Office of Management
& Enterprise Services

Data Storage Standard

Introduction

To ensure quality service and appropriate governance, data should be stored on a narrow set of purpose-built platforms.

Purpose

The purpose of this standard is to provide broad guidance to data owners on where data should be stored.

Definitions

Transactional Data – Data, which is accessed by numerous users to perform fast, simple queries. Typically, data which is directly associated with a user-facing application.

Analytical Data – Multi-dimensional data which is used to drive analytics and insights.

Document Data – Data derived from scanning paper documents.

Archival Data – Data which has no active use but needs to be kept because it may be subject to audits, open records requests or similar scenarios.

Historical Data – Data, for which its original use case has been retired, but still needs to be periodically searched. These datasets are no longer changing and no longer queried by other applications.

State Data Platform (SDP) – The State Data Platform is a centralized platform with data storage, management and processing capabilities.

Standard

Data Characteristics	Data Storage Solution	Details
• Archive or Historical Data	Please see Data Archiving Standard	
• Application or otherwise transactional data	SQL or Oracle database	• Solution and hosting location defined by the Database Administration team
• Operational or Log data	ITOCC	
• Documents	Please see the standard for document storage	
• Analytical, event-based, or any other type of data	State Data platform	• Solution defined by the Data Platform team

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: 07/24/2023	**Review cycle:** Annual
Last revised: 07/20/2023	**Last reviewed:** 07/20/2023
Approved by: Joe McIntosh, Chief Information Officer	

ATTACHMENT D-1

Access Data FTK

Access Data FTK (Forensic Toolkit) is a digital forensics software used for analyzing and extracting data from various sources, such as computers, mobile devices, and network storage. It helps investigators collect and preserve evidence for legal and investigative purposes.

Omes->Cyber Command->Cyber Command Operations

Cyber | **Security Operations Command**

ACF2

ACF2 (Access Control Facility) is an access control and security management system for IBM mainframe computers. It helps protect mainframe resources and data from unauthorized access.

Omes->Cyber Command->Cyber Command Operations

Mainframe Sec

Active Directory Local Administrator Password Solution (AD LAPS)

Password manager

Omes->IT Operations->Identity Management

Security Provisioning

Adobe Acrobat DC

Adobe Acrobat Document Cloud tool to create, convert, edit and sign PDFs.

Omes->Application & Data Services->Web and Citizen Experience

Electronic Signature | **Graphic Design** | **Document Generation**

Adobe Analytics

Enables web, marketing, predictive analysis and reporting of data.

Omes->Application & Data Services->Web and Citizen Experience
Service Oklahoma->Application & Data Services->Web and Citizen Experience

CX | **Citizen Facing** | **Analytics**

Adobe Campaign

Set of solutions to personalize and deliver campaigns.

Omes->Application & Data Services->Web and Citizen Experience

CX | **Digital Marketing**

Adobe Creative Suite

Predecessor of Adobe Creative Cloud with less features and a different license model.

Omes->Application & Data Services->Web and Citizen Experience

Branding | **Graphic Design**

Adobe Experience Manager

Content management solution.

Omes->Administration Services->Communications/Outreach
Omes->Application & Data Services->Web and Citizen Experience
OMMA->Application & Data Services->Web and Citizen Experience

UI/UX | **Branding** | **Tech Writing**

Adobe Forms

Online form generator by Adobe.

Omes->Application & Data Services->Web and Citizen Experience

UI/UX

Adobe Sign

E-signature service.

Omes->Administration Services->Business Administration

Omes->Application & Data Services->Web and Citizen Experience
Electronic Signature

Angular

TypeScript-based, free and open-source single-page web application framework.

Omes->Application & Data Services->Data Services
Data Science **Advanced Analytics** **Exploration**

Anomali

ANOMALI

Anomali is a threat intelligence platform that helps organizations identify, analyze, and respond to security threats. It collects and analyzes threat data from various sources to provide actionable intelligence and automate threat response.

Omes->Cyber Command->OK-ISAC
Cyber **Logging and Alerting** **Log Forensics**

Aruba Airwave

A network operations system to manage wired and wireless infrastructure from Aruba.

Omes->IT Operations->Networks
Operations

ASP .NET Identity

Identity framework to handle authentication and authorization. Single Sign-On.

Omes->IT Operations->Identity Management
Security Provisioning

ASPRunner

Creates a set of ASP pages to access and modify databases, or any other ODBC datasource.

Omes->Application & Data Services->Custom/COTS Apps
Custom Development

Atlassian

Helps teams to collaborate and share knowledge efficiently.

Omes->Application & Data Services->Service Quality
Project Testing

AWS

Amazon Web Services

Omes->IT Operations->Cloud
Service Oklahoma->Application & Data Services->Custom/COTS Apps
Service Oklahoma->IT Operations->Cloud
Operations

Axe

Accessibility tool.

Omes->Application & Data Services->Service Quality
Accessibility

Azure

Microsoft`s flexible cloud platform that includes legacy support and provisioning.

Omes->Application & Data Services->Service Quality
Omes->Application & Data Services->Legacy Application Support
Omes->Application & Data Services->Application Modernization Services
Omes->IT Operations->Cloud
Agency Application Support **Application Modernization** **Operations**

Azure Active Directory

A built-in solution for managing identities in Azure.

Omes->IT Operations->Identity Management
Security Provisioning

Azure Virtual Desktop

Azure Virtual Desktop is a cloud-based virtual desktop infrastructure (VDI) service that allows users to access virtualized desktops and applications from any device. It provides secure and scalable desktop virtualization solutions.

Omes->IT Operations->Servers

Operations

B2C

Identity management service.

Omes->IT Operations->Identity Management

Security Provisioning **Operations**

Bitlocker

BitLocker is a full disk encryption feature in Windows that helps protect data on Windows devices. It encrypts the entire hard drive to prevent unauthorized access in case of theft or loss.

Omes->Cyber Command->Defense

Cyber

BitSight

BITSIGHT

BitSight is a cybersecurity ratings platform that assesses and monitors the security performance of organizations and their third-party vendors. It provides insights and ratings based on factors such as security practices, vulnerabilities, and data breaches.

Omes->Cyber Command->Compliance

Third Party Risk Mgt

BlazeMeter

Open source, automated enterprise testing platform.

Omes->Application & Data Services->Service Quality

Project Testing

BridgeMaster

ODOT->Roadway->Engineering

Project Management

C#

Object-oriented programming language.

Omes->Application & Data Services->Legacy Application Support

Application Modernization

Canva

Graphic design platform used to create visual content

Omes->Administration Services->Communications/Outreach
Omes->Administration Services->Human Resources

Content Design **Tech Writing** **Social Media Management**

CastleBranch

CastleBranch is a background screening and compliance management platform used primarily in the healthcare and education sectors to manage employee and student screening processes.

Omes->Administration Services->Human Resources
Omes->Cyber Command->Compliance

Cyber **Background Checks**

Celonis

celonis

Celonis Process Intelligence allows you to analyze, improve, and monitor your processes.

Omes->Administration Services->Business Administration

Process Management | **Process Mining and Analysis**

Checkmarx

Software security solution for modern enterprise software development.

Omes->Application & Data Services->Custom/COTS Apps

Custom Development

Cloud Composer

A Google environment for managing data. Manages data ingestion, data transformation, data analysis and utilization, job scheduling, tasks, etc.

Omes->Application & Data Services->Data Services

Data Ingest and Pipeline

Cloud Data Fusion

Omes->Application & Data Services->Data Services

Data Integration

Cloud Functions

Google Cloud Service: Open source functions as a service.

Omes->Application & Data Services->Data Services

Data Ingest and Pipeline

CMDB

Configuration management database.

Omes->Application & Data Services->Custom/COTS Apps

Application Management

Cohesity

Cohesity DataProtect is a software-defined solution for protecting data sources.

Omes->IT Operations->Disaster Recovery/Business Continuity

Operations

Commvault

Data center backup and recovery solution for physical, virtual and cloud environments, and for different operating systems.

Omes->IT Operations->Disaster Recovery/Business Continuity

Operations

CrowdStrike

CROWDSTRIKE

CrowdStrike is a cloud-native endpoint protection platform that uses artificial intelligence and behavioral analytics to detect and respond to advanced cyber threats. It provides real-time visibility and threat intelligence to protect endpoints from attacks.

Omes->Cyber Command->Defense

Cyber

Crystal Reports

Business intelligence application used to create custom reports from a variety of data sources.

Omes->Application & Data Services->Custom/COTS Apps

Custom Development

Customer Information Control System (CICS)

Application servers for transaction processing for z/OS IBM mainframe systems.

Omes->Application & Data Services->Data Services

Data Mgt and Monitoring | **Mainframe Data Management**

Data Domain

A backup solution used and replaced the SAN.

Omes->IT Operations->Disaster Recovery/Business Continuity
Operations

Data Fusion

Data integration service.

Omes->Application & Data Services->Data Services
Data Ingest and Pipeline **Data Engineering**

Data Quality Tool

Data validity configuration tool for the data pipeline.

Omes->Application & Data Services->Data Services
Governance **Master Data Dictionary Repository** **Metadata Repository**

DataStudio (IBM)

IBM Tool for database development and administration of IBM DB2 for Linux, Unix and Microsoft Windows environments.

Omes->Application & Data Services->Data Services
Data Mgt and Monitoring **Mainframe Data Management**

DB2 (IBM)

Data management products developed by IBM including the DB2 relational database.

Omes->Application & Data Services->Data Services
Data Mgt and Monitoring **Mainframe Data Management**

DBF Viewer

Utility to view legacy DBFs.

Omes->Application & Data Services->Data Services
Data Mgt and Monitoring

Delinea

Privileged access management platform.

Omes->Cyber Command->Cyber Command Operations
Cyber **Security Provisioning**

Delinea PAM

Delinea

Delinea PAM (Privileged Access Management) is a comprehensive solution that helps organizations secure and manage privileged accounts and access rights. It provides capabilities for privileged account discovery, credential management, and session monitoring.

Omes->Cyber Command->Defense
Privileged Access Management

DevOps

Used to help plan, work and build applications. Code Management and Deployment.

Omes->Application & Data Services->Web and Citizen Experience
Omes->Application & Data Services->Custom/COTS Apps
Omes->Application & Data Services->Service Quality
Custom Development **Project Testing** **Automated Testing** **Operations** **DevOps**

DMBOK2

Data Management Body of Knowledge.

Omes->Application & Data Services->Data Services
Governance **Master Data Catalog**

Dragon Naturally Speaking

Accessibility tool used to covert speech to text.

Omes->Application & Data Services->Service Quality
Accessibility

Dynatrace

Tool for application and infrastructure performance monitoring

Omes->Application & Data Services->Data Services
Omes->Application & Data Services->Custom/COTS Apps
Application Mgmt & Monitoring | **Data Mgt and Monitoring** | **Database Monitoring** | **SQL Platform**

Enterprise Data Governance Tool

A tool that aids the process of creating and maintaining a structured set of policies, procedures and protocols that control how data is stored, managed and used.

Omes->Application & Data Services->Data Services
Governance | **Master Data Dictionary Repository** | **Metadata Repository**

ESRI ArcGIS

ArcGIS is GIS mapping and analysis solution.

Omes->Application & Data Services->Custom/COTS Apps
GIS

Fiddler

Traffic inspector that inspects HTTP/HTTPS traffic to and from browsers and desktop apps.

Omes->Application & Data Services->Custom/COTS Apps
Custom Development

FileZilla Pro

Software for FTP/SFTP/FTPS.

Omes->Administration Services->Human Resources
Omes->Application & Data Services->Application Modernization Services
Application Modernization

Foglight

Database monitoring tool.

Omes->Application & Data Services->Data Services
Database Monitoring

GitHub

Development platform for code repository, code sharing and workflows.

Omes->Application & Data Services->Custom/COTS Apps
Omes->Application & Data Services->Service Quality
Service Oklahoma->Application & Data Services->Custom/COTS Apps
Service Oklahoma->Application & Data Services->Service Quality
Custom Development | **Automated Testing**

Google

Internet search engine

Omes->Administration Services->Enterprise Architecture
Research

Google BigQuery

Serverless, multicloud data warehouse.

Omes->Application & Data Services->Data Services
Data Engineering

Google Cloud CLI

Command line interface to create and manage Google cloud resources.

Omes->Application & Data Services->Data Services
Data Engineering

Google Cloud Platform (GCP)

Cloud data platform.

Omes->Application & Data Services->Data Services
Omes->IT Operations->Cloud
Service Oklahoma->Application & Data Services->Data Services
Service Oklahoma->IT Operations->Cloud
Operations | **Data Sharing** | **Data Mgt and Monitoring**

Google Colaboratory

Hosted Jupyter Notebook service.

Omes->Application & Data Services->Data Services
Data Science | **Advanced Analytics** | **Exploration**

Google Data Studio

Online tool for converting data into customizable informative reports and dashboards.

Omes->Application & Data Services->Data Services
Analytics | **Reporting** | **Self Service**

GovDelivery

Web based Email Subscription Management System - Communications tool used for content delivery via email.

Omes->Administration Services->Communications/Outreach
Omes->Administration Services->Human Resources
Omes->IT Operations->IT Operation Command Center
OMMA->Application & Data Services->Web and Citizen Experience
Content Delivery

Host-Integration Server (HIS)

Gateway application providing connectivity between Microsoft Windows networks and IBM mainframe and IBM i systems.

Omes->Application & Data Services->Custom/COTS Apps
ESB/Integration Platform

IBM Spectrum Protect

Data Protection Solution - Enterprise-scale data protection for physical file servers, virtual environments and a wide range of applications.

Omes->IT Operations->Disaster Recovery/Business Continuity
Operations

IdentoGO iTouch

Center that provides fingerprinting services

Omes->Cyber Command->Compliance
Background Checks

IMS

Mainframe database system.

Omes->Application & Data Services->Data Services
Data Mgt and Monitoring | **Mainframe Data Management**

Infoblox DNS

A hierarchical and decentralized naming system for computers, services, or other resources connected to the internet or a private network.

Omes->IT Operations->Servers
Operations

InRule

Business rules engine.

Omes->Application & Data Services->Custom/COTS Apps
Rules Engine/BPA

Intrusion Prevention

Network security and threat prevention system.

Omes->Cyber Command->Defense
Network Security

Intune

Microsoft cloud-based management tool for mobile devices.

Omes->Cyber Command->Defense
Cyber | **Defense Operations**

IP Address Management (IPAM)

Methodology implemented in computer software for planning and managing the assignment and use of IP addresses and closely related resources of a computer network.

Omes->IT Operations->Networks

Operations

JAVA

Object-oriented programming language.

Omes->Application & Data Services->Custom/COTS Apps
Omes->Application & Data Services->Application Modernization Services

Custom Development **Application Modernization**

JAWS

A computer screen reader program for Microsoft Windows that allows blind and visually impaired users to read the screen.

Omes->Application & Data Services->Service Quality

Accessibility

Jmeter

Testing tool for software for analyzing performance and measures from Apache.

Omes->Application & Data Services->Service Quality

Automated Testing

Juniper Mist Portal

End-to-end network observability.

Omes->IT Operations->Networks

Operations

Juniper Space

Network management solution.

Omes->IT Operations->Networks

Operations

Juniper Wired Assurance

A solution for proactive remediation of network operations.

Omes->IT Operations->Networks

Operations

Juvare

Leading provider of emergency preparedness and response software.

Omes->Application & Data Services->Custom/COTS Apps

Healthcare Supply Chain Management

Katalon

Automation testing software tool.

Omes->Application & Data Services->Service Quality
Service Oklahoma->Application & Data Services->Service Quality

Automated Testing

Kerberos

Kerberos is a network authentication protocol used to verify the identity of users and provide secure communication over a network. It is commonly used in Windows and Unix environments.

Omes->Cyber Command->Auth

Cyber

KnowBe4

KnowBe4 is a security awareness training and simulated phishing platform. It helps organizations educate their employees about cybersecurity threats, vulnerabilities, and best practices through interactive training modules and simulated phishing attacks.

Omes->Cyber Command->Compliance

Cyber **SEAT Training**

LAMP Stack

A set of tools for web application development (Linux, Apache, MySQL, PHP/Perl/Python)

Omes->Application & Data Services->Custom/COTS Apps
Custom Development

Looker

Google Data Analytics and Reporting.

Omes->Application & Data Services->Data Services
Analytics **Reporting** **Self Service**

Magento

An open-source eCommerce platform.

Omes->Application & Data Services->Web and Citizen Experience
Ecommerce

MAMPP

Omes->Application & Data Services->Custom/COTS Apps
Custom Development

Microsoft Access

Manages data. It combines the relational Microsoft Jet Database Engine with a graphical user interface and software-development tools.

Omes->Application & Data Services->Service Quality
Agency Application Support

Microsoft SQL 2019

Microsoft SQL database version 2019.

Omes->Application & Data Services->Data Services
Data Mgt and Monitoring **SQL Platform**

Microsoft SQL Management Studio

A software application used for configuring, managing and administering all components within Microsoft SQL Server.

Omes->Application & Data Services->Custom/COTS Apps
Custom Development **Data Science** **Advanced Analytics** **Exploration**

Microsoft SQL Suite

Suite of database software to manage/administer Microsoft SQL
database.

Omes->Application & Data Services->Data Services
Data Mgt and Monitoring

Microsoft Visual Studio

Application development platform.

Omes->Application & Data Services->Custom/COTS Apps
Omes->Application & Data Services->Application Modernization Services
Custom Development **Application Modernization**

Microsoft Visual Studio Code

Source-code editor made by Microsoft for Windows, Linux and macOS.

Omes->Application & Data Services->Custom/COTS Apps
Omes->Application & Data Services->Application Modernization Services
Custom Development **Application Modernization** **Data Science** **Advanced Analytics** **Exploration**

Mimecast

Cloud cybersecurity services for email, data and web.

Omes->Cyber Command->Cyber Command Operations
Cyber

MobaXterm

Omes->Application & Data Services->Data Services
Data Mgt and Monitoring

MoveIt

Managed file transfer software produced by Ipswitch, Inc.

Omes->Application & Data Services->Data Services
Service Oklahoma->Application & Data Services->Data Services
Managed File Transfer

MuleSoft

An integration platform for applications and data.

Omes->Application & Data Services->Data Services
Omes->Application & Data Services->Custom/COTS Apps
Omes->Application & Data Services->Service Quality
Service Oklahoma->Application & Data Services->Data Services
ESB/Integration Platform **Agency Application Support** **Data Ingest and Pipeline** **Data Integration**

MYSQL Workbench

A MySQL database management tool.

Omes->Application & Data Services->Data Services
Data Mgt and Monitoring

Narrator

Web accessibility software.

Omes->Application & Data Services->Service Quality
Accessibility

Nerdio

Azure deployment and management service.

Omes->IT Operations->Cloud
Operations

Notepad++

Free source code editor.

Omes->Application & Data Services->Custom/COTS Apps
Custom Development

NVDA

Screen reader for Microsoft Windows.

Omes->Application & Data Services->Service Quality
Accessibility

O365 Data Loss Prevention

To help protect this sensitive data, and to reduce the risk from oversharing, they need a way to help prevent their users from inappropriately sharing sensitive data with people who shouldn`t have it. This practice is called data loss prevention (DLP).

In Microsoft Purview, you implement data loss prevention by defining and applying DLP policies. With a DLP policy, you can identify, monitor, and automatically protect sensitive items across:

Microsoft 365 services such as Teams, Exchange, SharePoint, and OneDrive accounts
Office applications such as Word, Excel, and PowerPoint
Windows 10, Windows 11, and macOS (three latest released versions) endpoints
non-Microsoft cloud apps
on-premises file shares and on-premises SharePoint
Fabric and Power BI
DLP detects sensitive items by using deep content analysis, not by just a simple text scan. Content is analyzed:

For primary data matches to keywords
By the evaluation of regular expressions
By internal function validation
By secondary data matches that are in proximity to the primary data match
DLP also uses machine learning algorithms and other methods to detect content that matches your DLP policies

Omes->Application & Data Services->Service Quality
Omes->Cyber Command->Cyber Command Operations
Cyber **Misc. Testing/Support**

OAuth2

Open Authentication 2.0. A Protocol that allows a user to grant a third-party website or application access to the user`s protected resources.

Omes->Cyber Command->Auth
Cyber

OCI

Oracle Cloud Infrastructure

Omes->IT Operations->Cloud
Operations

OEM

OEM Tools

Omes->Application & Data Services->Data Services
Data Mgt and Monitoring **Database Monitoring**

OnBase

A single enterprise information platform designed to manage your content, processes and cases.

Omes->Application & Data Services->Custom/COTS Apps
Omes->Application & Data Services->Application Modernization Services
Enterprise Records & Content Management **Data Archiving**

OneTrust

onetrust

OneTrust is a comprehensive privacy management platform that helps organizations comply with data protection and privacy regulations. It provides tools for data inventory and mapping, consent management, privacy impact assessments, and more.

Omes->Cyber Command->Compliance
Third Party Risk Mgt

OPENID Connect2

A simple identity layer on top of the OAuth 2.0 protocol.

Omes->Cyber Command->Auth
Cyber

Oracle 19C

A multi-model database that provides full support for relational
data and non-relational data.

Omes->Application & Data Services->Data Services
Data Mgt and Monitoring **Oracle Platform**

Paint.net

Digital photo editing software.

Omes->Application & Data Services->Data Services
Data Science **Advanced Analytics** **Exploration**

Palo Alto Firewall

paloalto NETWORKS

Palo Alto Firewall is a network security appliance that provides advanced firewall protection, intrusion prevention, and threat intelligence. It helps organizations secure their network infrastructure and prevent unauthorized access.

Omes->Cyber Command->Defense
Network Security

Pega

Java-based business process management tool.

Omes->Application & Data Services->Custom/COTS Apps
Rules Engine/BPA

Peoplesoft

Oracle application system.

Omes->Administration Services->Business Administration
Omes->Administration Services->Human Resources
Omes->Cyber Command->Cyber Command Operations
Service Oklahoma->Administration Services->Business Administration
Security Provisioning

PeopleSoft Financials Platform

Suite of Peoplesoft modules to keep track of financials.

Omes->Administration Services->Enterprise Architecture
Omes->Application & Data Services->Financial Enterprise Apps
EA Approvals

PeopleSoft Inventory

A flexible, comprehensive inventory management system.

Omes->Application & Data Services->Financial Enterprise Apps
Inventory **Asset Management**

PHP

A general-purpose scripting language geared toward web development.

Omes->Application & Data Services->Custom/COTS Apps
Custom Development

PHP Runner

A low-code/no-code solution to access and edit databases.

Omes->Application & Data Services->Custom/COTS Apps
Custom Development

Platform Microsoft Endpoint Manager Patch

PC/patch management platform.

Omes->Cyber Command->Defense
Cyber

PostgreSQL

A free and open-source relational database management system
emphasizing extensibility and SQL compliance.

Omes->Application & Data Services->Data Services
SQL Platform

Postman

Collaboration platform for application programming interface (API) development.

Omes->Application & Data Services->Custom/COTS Apps
Omes->Application & Data Services->Service Quality
Service Oklahoma->Application & Data Services->Service Quality
Custom Development **Automated Testing**

Power Automate

Omes->Application & Data Services->Custom/COTS Apps
RPA

Power Query

Query tool.

Omes->Application & Data Services->Data Services
Data Ingest and Pipeline

Power Shell

O/S command line utility.

Omes->Application & Data Services->Data Services
Data Ingest and Pipeline

PowerBI

A Microsoft business analytics service. Provides dashboard and visualization capabilities for reporting.

Omes->Application & Data Services->Data Services
Omes->IT Operations->Change Management/Recovery Services
Service Oklahoma->Application & Data Services->Web and Citizen Experience
Analytics **Reporting** **Self Service** **Data Science** **Advanced Analytics** **Exploration** **Program Management**

PowerFlex

Dell storage solution.

Omes->IT Operations->Disaster Recovery/Business Continuity

Operations

PuTTY

A free and open-source terminal emulator, serial console and network file transfer application.

Omes->Application & Data Services->Application Modernization Services

Application Modernization | Data Mgt and Monitoring

Python

An interpreted high-level, general-purpose programming language.

Omes->Application & Data Services->Data Services
Omes->Application & Data Services->Custom/COTS Apps
Omes->Application & Data Services->Application Modernization Services

Custom Development | Application Modernization | Data Ingest and Pipeline | Data Science | Advanced Analytics | Exploration

Qualtrics

An online survey tool.

Omes->Administration Services->Human Resources
Omes->Application & Data Services->Web and Citizen Experience

CX | Survey

R Studio

An integrated development environment for R, a programming
language for statistical computing and graphics.

Updated:
These are now included in the basic package-

To load data:
googleCloudStorageR (r-project.org)
bigQueryR (r-project.org)
CRAN - Package DBI (r-project.org)
CRAN - Package odbc (r-project.org)
CRAN - Package xlsx (r-project.org)
CRAN - Package foreign (r-project.org)
CRAN - Package haven (r-project.org)
CRAN - Package data.table (r-project.org)

To manipulate, model, and visualize data:
CRAN - Package tidyverse (r-project.org)
CRAN - Package ggvis (r-project.org)
CRAN - Package tidymodels (r-project.org)
CRAN - Package car (r-project.org)
CRAN - Package mgcv (r-project.org)
CRAN - Package mgcViz (r-project.org)
CRAN - Package lme4 (r-project.org)
CRAN - Package nlme (r-project.org)
CRAN - Package randomForest (r-project.org)
CRAN - Package randomForestExplainer (r-project.org)
CRAN - Package multcomp (r-project.org)
CRAN - Package vcd (r-project.org)
CRAN - Package glmnet (r-project.org)
CRAN - Package survival (r-project.org)
CRAN - Package caret (r-project.org)
CRAN - Package caretEnsemble (r-project.org)

For reporting data:
CRAN - Package shiny (r-project.org)
CRAN - Package rmarkdown (r-project.org)
CRAN - Package xtable (r-project.org)

For spatial data:
CRAN - Package sp (r-project.org)
CRAN - Package maps (r-project.org)
CRAN - Package ggmap (r-project.org)

For time series and financial data:
CRAN - Package zoo (r-project.org)
CRAN - Package xts (r-project.org)

Omes->Application & Data Services->Data Services

Data Science | Advanced Analytics | Exploration

RACF

RACF (Resource Access Control Facility) is an access control system for IBM mainframe computers. It provides security and authorization services to protect resources and data within mainframe environments.

Omes->Cyber Command->Cyber Command Operations

Cyber | Mainframe Sec

Redhat

Linux open-source product.

Omes->IT Operations->Servers

Operations

Relativity iCONECT via Managed Service Provider

Omes->Cyber Command->Compliance

Privacy

Salesforce

Customer relationship management (CRM) software.

Omes->Application & Data Services->Custom/COTS Apps

CRM

SAML 2

A version of the SAML standard for exchanging authentication and authorization identities between security domains.

Omes->Cyber Command->Auth

Cyber

SauceLabs

Cloud-based platform for automated continuous testing of web and mobile apps.

Omes->Application & Data Services->Service Quality

Automated Testing

Selenium

Automated testing platform across different browsers.

Omes->Application & Data Services->Service Quality

Automated Testing

SendGrid

A cloud-based SMTP provider.

Omes->Application & Data Services->Custom/COTS Apps

Email Delivery

ServiceNow

Platform as a service providing technical management support such as IT service management, IT operations management and IT business management. Used to define, manage, automate and structure services and production instances.

Omes->Administration Services->Business Administration
Omes->Application & Data Services->Service Quality
Omes->Application & Data Services->Application Modernization Services
Omes->IT Operations->
Omes->IT Operations->Change Management/Recovery Services
Omes->IT Operations->Customer Services
Service Oklahoma->Administration Services->Project Management Office
Service Oklahoma->IT Operations->Customer Services

Application Decommissioning | Operations | Service Delivery | Reporting | Mission Support | Project Management | EA Approvals | CMDB | Change Management | Event Management | Service Desk | Problem Management

ServiceNow Asset Management

Manage all your hardware, software, and cloud IT assets from a single platform. Automate every stage of the IT asset lifecycle at scale while controlling costs and minimizing licensing and leasing risks.

Omes->IT Operations->Customer Services

Asset Management

ServiceNow SPM

ServiceNow Strategic Portfolio Management

Omes->Administration Services->Project Management Office

Project Management

ShareGate Apricot

Platform for automated teams governance.

Omes->IT Operations->Cloud

Operations

SharePoint

Platform for content management and repository.

Omes->Administration Services->Business Administration
Omes->Administration Services->Human Resources
Omes->Application & Data Services->Custom/COTS Apps

Enterprise Records & Content Management

SIEM Plateform Splunk ES

Omes->Cyber Command->Cyber Command Operations

Cyber

SiteImprove

Web accessibility software product.

Omes->Application & Data Services->Web and Citizen Experience
Omes->Application & Data Services->Service Quality

Accessibility **UI/UX** **CX** **Operations**

Slack

A messaging application that can be used across multiple devices and platforms.

Omes->Application & Data Services->Custom/COTS Apps

Custom Development

SOL

Platform for automated testing.

Omes->Application & Data Services->Service Quality

Application Management

Sprout

Social media management platform used for social media analysis and tracking.
Sprout Social, Inc. is a social media management tool that helps brands communicate with customers across social channels, collaborate across teams, and measure the effectiveness of their efforts.

Sprout`s platform integrates with Twitter, Facebook, LinkedIn, Instagram, Google+, Zendesk, UserVoice, Feedly, and Google Analytics. Bambu by Sprout Social, launched in August 2015, is an employee advocacy platform that allows organizations to curate content for employees to read and share on social media.[1]

Omes->Administration Services->Communications/Outreach

Social Media Management

SSO Azure AD

Omes->Cyber Command->Auth

Cyber

Suse

Linux open-source product.

Omes->IT Operations->Servers

Operations

Tenable

Tenable is a cybersecurity company that provides vulnerability management and threat detection solutions. Its products help organizations identify and remediate vulnerabilities, and detect and respond to security threats.

Omes->Cyber Command->Vulnerability Management

Cyber **Vulnerability Management**

The DASH

Custom application that sits on top of the State Data Platform and serves as the central point for getting information from the platform.

Omes->Application & Data Services->Data Services

Data Sharing

Thentia

Occupational licensing software.

Omes->Application & Data Services->Custom/COTS Apps
OMMA->Application & Data Services->Web and Citizen Experience

Application Modernization **Licensing**

Time Clocks - TimeClock Plus

Time reporting tool.

Omes->Application & Data Services->HCM Enterprise Applications

Plugins **HCM**

Toad

A Quest data management tool for the DBAs, architects and developers.

Omes->Application & Data Services->Data Services
Omes->Application & Data Services->Service Quality

Agency Application Support **Data Mgt and Monitoring**

UiPath

A robotic process automation tool that enables users to automate various aspects of business processes.

Omes->Application & Data Services->Custom/COTS Apps

RPA

V3locity (Velocity)

Employee benefits management system.

Omes->Application & Data Services->HCM Enterprise Applications

Benefits Management **EGID**

Veracode

Platform to manage security risk across the entire application portfolio.

Omes->Application & Data Services->Custom/COTS Apps

Custom Development

VerifyOK

Software to verify identity online.

Omes->IT Operations->Identity Management

Operations

Visio

Visio is a diagramming and vector graphics application and is part of the Microsoft Office family

Omes->Administration Services->Enterprise Architecture
Service Oklahoma->Administration Services->Enterprise Architecture

EA Tool

VMware

Enterprise virtual machine software.

Omes->IT Operations->Servers

Operations

VMware SRM

VMware Site Recovery Manager (SRM) provides policy-based management, minimizes downtime in case of disasters via automated orchestration, and enables nondisruptive testing of your disaster recovery plans.

Omes->IT Operations->Disaster Recovery/Business Continuity

Operations

VMware vCenter

Enterprise virtual machine management system on-premises.

Omes->IT Operations->Servers

Operations

Voiceover

Web accessibility software.

Omes->Application & Data Services->Service Quality

Accessibility

Webex

Solution for video conferencing, online meetings, screen share, webinars and collaboration

Omes->Administration Services->Communications/Outreach

Open Meetings

WebFOCUS

Enterprise reporting system.

Omes->Application & Data Services->Data Services

Analytics **Reporting** **Data Mgt and Monitoring**

Workday

Strategic workforce planning software for human capital management (HCM).

Omes->Administration Services->Human Resources
Omes->Application & Data Services->HCM Enterprise Applications

HCM

XAMPP

Provides web, database and FTP server packages, fast and completely portable, for Windows.

Omes->Application & Data Services->Custom/COTS Apps

Custom Development

Zscaler

Cloud security software and system for virtual private network and access.

Omes->Cyber Command->Cyber Command Operations
Omes->Cyber Command->Defense

Cyber

ATTACHMENT D-1

Incident Response Standard

Introduction

The State of Oklahoma handles incidents so as to minimize the impact on the confidentiality, integrity and availability of the state's systems, applications and data. It is especially important that security incidents are promptly communicated to Oklahoma Cyber Command to ensure all appropriate parties are involved early to assist with investigations, communications and reporting.

Purpose

This document establishes the requirements for reporting a security incident.

Definitions

Data breach – The unauthorized access by an unauthorized person that results in access, use, disclosure or theft of non-public data or personal data.

Non-public data – Data, other than personal data, not subject to distribution to the public as public information. It is deemed to be sensitive and confidential by the State of Oklahoma because it contains information exempt by statute, ordinance or administrative rule from access by the general public as public information. Non-public data includes any data deemed confidential by the State of Oklahoma as non-public data, or that a reasonable person would deem confidential.

Personal data – Data containing 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) contains electronic protected health information that is subject to the Health Insurance Portability and Accountability Act of 1996, as amended.

Security incident – The attempted or successful unauthorized access, use, disclosure, modification or destruction of information or interference with confidentiality, integrity and availability of state infrastructure.

Standard

Oklahoma Cyber Command utilizes the National Incident Management System (NIMS) framework for incident responses. NIMS integrates effective practices in emergency response into a comprehensive national framework for incident management.

All state agencies must report all security incidents and potential security incidents to Oklahoma Cyber Command immediately upon discovery. When an incident occurs, it is the responsibility of the agency to notify Oklahoma Cyber Command via email at cybercommand@omes.ok.gov.

All reported incidents are investigated, and prompt and full cooperation is required of agencies and all agency personnel.

As appropriate, Oklahoma Cyber Command acts as a liaison with law enforcement, risk management, legal counsel, agency leadership and state leadership.

Pursuant to 62 O.S. §§ 34.11.10, Oklahoma Cyber Command posts information related to each confirmed security breach on the security.ok.gov website at the conclusion of the investigation.

State agencies reporting an incident must include, at a minimum:

- A summary of the events surrounding the cybersecurity incident including affected assets, systems and services.
- If a ransomware incident, the date on which the state agency most recently backed up its data, the physical location of the backup and whether the backup was created using cloud computing.
- The types of data compromised by the cybersecurity incident.
- The estimated fiscal impact of the cybersecurity incident.

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 Incident Management System (NIMS).
- Oklahoma Cyber Command Cybersecurity Breaches.
- Oklahoma State Government Security Breach Transparency Initiative.

Revision history

This standard is subject to periodic review to ensure relevancy.

Effective date: 4/07/2022	**Review cycle:** Annual
Last revised: 4/07/2022	**Last Reviewed:** 08/23/2024
Approved by: Joe McIntosh, Chief Information Officer	

ATTACHMENT D-1

Decentralized Security Representative (DSR) Standard

Introduction
Office of Management and Enterprise Services Information Services (OMES IS) utilizes a system of decentralized security representatives (DSR) at each agency, which serves as the agency's approval authority for access to the agency's data and network resources.

Purpose
This document outlines the role of the DSR for the State of Oklahoma.

Definitions
Decentralized security representative (DSR) – an individual designated by a state agency to approve user access; communicate security policies, procedures, guidelines and best practices to agency personnel and report on all deviations to security policies, procedures, guidelines and best practices.

DSR appointing authority – the agency DSRs that have been given the approval to appoint additional DSRs.

Emergency – any event resulting in owning agency loss of services.

Hosting state agency – an agency that has physical and operational control of the hardware, software, communications or databases (files) of the owning agency. The hosting agency can also be an owner.

Information – any data or knowledge collected, processed, stored, managed, transferred or disseminated by any method.

Owner – the state agency responsible for producing, collecting and maintaining the authenticity, integrity and accuracy of information.

Sensitive data – Oklahoma statute (74 O.S. 3113.1) defines sensitive data to include "personal information", consisting of the first name, or first initial, and last name of an individual in combination with any one or more of the following data elements, when either the name or the data elements are not encrypted: a) social security number; b) driver license number; or c) account number, credit or debit card number, in combination with any required security code, access code or password that would permit access to the financial account of an individual. This statute also specifies that if such information is reasonably believed to have been acquired by an unauthorized person, then disclosure shall be made in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement (Information Security Policy, Appendix E).

Standard

All information content hosted by a state agency is owned by and is the primary responsibility of the agency responsible for collecting and maintaining the authenticity, integrity and accuracy of information. The objective of the owning state agency is to protect the information from inadvertent or intentional damage as well as unauthorized disclosure or use according to the classification standards and procedural guidelines of the owning state agency. The state agency director whose agency collects and maintains (owns) the information is responsible for interpreting all confidentiality restrictions imposed by laws and statutes as well as establishing information classification and approving information access. The owning agency shall validate user access on an annual basis. Thus, all agencies must designate a security representative whose role shall include granting, on behalf of their agency, user access to system functions and data (Information Security Policy, sections 2.2-2.4).

The commissioner, executive director and employees of the human resources department of the owning state agency are automatically considered a DSR for their agency. Additional employees of the owning state agency may be appointed as DSR by the commissioner or executive director to act on their behalf for their agency. They may also delegate the authority to appoint additional DSRs to specific employees of their agency at their discretion.

DSR appointment occurs by the commissioner, executive director or DSR appointing authority completing the DSR appointment request form via the ticketing system. Such requests are processed by the hosting agency, OMES. OMES maintains the list of appointed DSRs and makes available to owning agencies via the DSR SharePoint site.

Prior to DSR appointment, the appointee must complete the required Decentralized Security Representative 101 training via Workday Learning. Upon DSR appointment, the hosting agency confirms setup to the Agency Appointment Authority (Information Security Policy, section 2.3). DSR renewal training shall be completed by all individuals with DSR authority on an annual basis.

OMES can approve IS staff access to support agencies with the exception of agencies who have sensitive, protected or confidential data which will require approval from that agency DSR. In emergency situations, OMES IS can approve access to return services to an agency. Approval for contractor accounts for IS services is through legal review as agencies authorize support for access in this agreement. Approval for contractor accounts for an agency is approved by the agency DSR.

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

- DSR appointment instructions.
- DSR SharePoint site.
- Information Security Policy.

Revision history

This standard is subject to periodic review to ensure relevancy.

Effective date: 12/21/2023	**Review cycle:** Annual
Last revised: 03/26/2024	**Last reviewed:** 07/15/2024
Approved by: Joe McIntosh, Chief Information Officer	

OKLAHOMA
Office of Management
& Enterprise Services

Data Archiving Standard

Introduction

In order to ensure quality service, appropriate governance and optimized cost, state systems need to store infrequently used data in an archival solution.

Purpose

The purpose of this standard is to provide guidance to agency staff on how to properly identify and implement an archiving solution.

Definitions

Archival Data – Data which has no active use but needs to be kept because it may be subject to Audits, Open Records requests, or similar scenarios.

Historical Data – Data, for which its original use case has been retired, but still needs to be periodically searched. These datasets are no longer changing and no longer queried by other applications.

State Data Platform (SDP) – The State Data Platform is a centralized platform with data storage, management and processing capabilities.

Standard

All Archival Data should be stored on the State Data Platform.

- The SDP provides several cost-effective archive storage options with metadata and access management functionality to ensure the data is properly labeled and locatable.

All Historical Data use cases require engagement from the web and data team to ensure the user can query the data as needed.

- The data team will migrate the data and the web team will develop a front-end to suit the needs of the user.
- By default, historical data use cases should leverage the State Data Platform for storage so that the original storage solution can be properly retired. An exception to this is when the original storage solution is still a supported and maintained technology and it simplifies the development of the front-end.

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: 07/24/2023	**Review cycle:** Annual
Last revised: 07/17/2023	**Last reviewed:** 07/17/2023
Approved by: Joe McIntosh, Chief Information Officer	

ATTACHMENT D-1

OKLAHOMA
Office of Management
& Enterprise Services

Data Retention Standard

Introduction
Data is one of the most valuable resources that the state maintains. As such, it is important to deliberately control how long records are kept and how they should be discarded.

Purpose
The purpose of this standard is to ensure that necessary records are adequately protected and maintained and to ensure that records that are no longer needed are discarded at the proper time.

Definitions
ODL – Oklahoma Department of Libraries.

Tag – a keyword that describes a piece of information.

Record - means all documents including, but not limited to, any book, paper, photograph, microfilm, data files created by or used with computer software, computer tape, disk, record, sound recording, film recording, video record or other material regardless of physical form or characteristic, created by, received by, under the authority of, or coming into the custody, control or possession of public officials, public bodies or their representatives in connection with the transaction of public business, the expenditure of public funds or the administering of public property. For definitions of items that are not records, please see 51 O.S. § 24A.3.

Standard
All records shall be retained in accordance with state and federal statute, agency rule and established ODL retention schedules. No data is to be destroyed without proper authorization.

- Tagging.
  - To the extent allowed by the system where the record is stored, all records must be properly tagged. Minimum tags (meta-data) include ID, description, classification and retention citation.
- ODL responsibilities.
  - With certain statutory exceptions, all state agencies, boards and commissions are required to establish and maintain ongoing “programs for the efficient and economical management of records” and have their programs approved by the Archives and Records Commission (67 O.S. Sec 206, 305).
  - Records disposition schedules are reviewed and approved by the Archives and Records Commission as provided in Chapter 10A of Title 67 of the Oklahoma Statues and in the rules for the commission as set out in Title 60 of the Oklahoma Administrative Code.
- Records destruction.
  - In accordance with Archives and Records Commission Rule OAC 60:10-3-2(b), no records listed in the general records disposition schedule, regardless of format, shall be destroyed until one of the following forms has been submitted to and has been approved by the State Records Administrator or their designee:
    - Notice of Intent to Destroy Records (ARC Form 4).
    - Notice of Intent to Destroy Records That Have Been Imaged (ARC Form 12).

    - Notice of Intent to Destroy Optical Disks (ARC Form 13).
  - Records that have an approved disposition of “Retain in office and destroy after primary use," "Retain in office until no longer required for administrative purposes, then destroy," "Retain in office and destroy upon verification" or "Retain in office until superseded, then destroy” are not subject to the above Notices of Intent to Destroy.

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
- 67 O.S. Sec 206, 305.
- 60 O.A.C.
- 51 O.S. § 24A.3.

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

Effective date: 03/15/2024	**Review cycle:** Annual
Last revised: 03/18/2024	**Last reviewed:** 03/18/2024
Approved by: Joe McIntosh, Chief Information Officer	

OKLAHOMA
Office of Management
& Enterprise Services

Data Storage Standard

Introduction

To ensure quality service and appropriate governance, data should be stored on a narrow set of purpose-built platforms.

Purpose

The purpose of this standard is to provide broad guidance to data owners on where data should be stored.

Definitions

Transactional Data – Data, which is accessed by numerous users to perform fast, simple queries. Typically, data which is directly associated with a user-facing application.

Analytical Data – Multi-dimensional data which is used to drive analytics and insights.

Document Data – Data derived from scanning paper documents.

Archival Data – Data which has no active use but needs to be kept because it may be subject to audits, open records requests or similar scenarios.

Historical Data – Data, for which its original use case has been retired, but still needs to be periodically searched. These datasets are no longer changing and no longer queried by other applications.

State Data Platform (SDP) – The State Data Platform is a centralized platform with data storage, management and processing capabilities.

Standard

Data Characteristics	Data Storage Solution	Details
• Archive or Historical Data	Please see Data Archiving Standard	
• Application or otherwise transactional data	SQL or Oracle database	• Solution and hosting location defined by the Database Administration team
• Operational or Log data	ITOCC	
• Documents	Please see the standard for document storage	
• Analytical, event-based, or any other type of data	State Data platform	• Solution defined by the Data Platform team

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: 07/24/2023	**Review cycle:** Annual
Last revised: 07/20/2023	**Last reviewed:** 07/20/2023
Approved by: Joe McIntosh, Chief Information Officer	

OKLAHOMA
Office of Management
& Enterprise Services

Password Requirements Standard

Introduction

Passwords are an important part of computer security at the State of Oklahoma. They often serve as the first line of defense in preventing unauthorized access to state computers and data. Poor password complexity, including insufficient length or the inclusion of commonly used words, may allow an attacker to guess the password and gain unauthorized access to the state infrastructure. Generally, the more complex and cryptic the password, the more difficult it is for an attacker to guess. As such, the state requires account passwords to comply with state standards to help protect the integrity of state resources and data.

Purpose

This document outlines the complexity requirements and proper management practices of passwords for all computer systems and mobile devices at the State of Oklahoma.

Standard

The State of Oklahoma requires account passwords to comply with state standards to help protect the integrity of state resources and data. All current and new accounts are subject to the following password requirements.

- Passwords must be a minimum length of 8 characters.
- Passwords for elevated privileges to include access to highly regulated data sets (e.g., Federal tax information, criminal justice systems data, etc.) must be a minimum of 15 characters.
- Must contain at least one lower case letter, uppercase letter, numeral and special character.
- Passwords expire in a maximum of 90 days.
- Passwords for elevated privileges are required to change passwords at least every 60 days.
- Passwords are deactivated if not used for a period of 60 days.
- Password reuse is prohibited for 24 generations.

All passwords are treated as sensitive, confidential state information and therefore must be protected as such. Employees and contractors are responsible for keeping passwords secure and confidential. The following principles must be adhered to for creating and safeguarding passwords.

- Passwords cannot be stored or shared in plain text.
- Keep passwords confidential.
- Avoid keeping a paper record of passwords.
- Change passwords whenever there is any indication of possible system or password compromise.
- Select quality passwords with a minimum length of eight characters which are:
    - Easy to remember.
    - Not based on anything somebody else could easily guess or obtain using person related information (e.g., names, telephone numbers and dates of birth).
    - Free of consecutive identical characters or all-numeric or all-alphabetical groups.
- Change passwords at regular intervals.
- Avoid reusing old passwords.
- Change temporary passwords at the first log-on.

- Do not include passwords in any automated log-on process (e.g., stored in a macro or function key).
- Do not share individual user passwords.

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: 04/26/2022	**Review cycle:** Annual
Last revised: 10/18/2022	**Last reviewed:** 08/30/2023
Approved by: Joe McIntosh, Chief Information Officer	

ATTACHMENT D-1

Identity Management Standard

Introduction

User accounts are the only legitimate method by which OMES information systems may be accessed. OMES Information Services actively manages user accounts to prevent illegitimate use of state information systems. The use of authorization, identification and authentication controls ensure that only known users make use of state systems. Without these controls, the potential exists for information systems to be accessed illicitly, and the security of those information systems could be compromised.

Purpose

This document defines the types of user accounts managed by OMES IS.

Definitions

Affiliate – worker who is not a state employee but serves in a supporting role to a state agency's mission, typically at the county, local or municipality level.

Contractor – worker with economic independence who is in business for themselves but has been hired by the state to perform a particular function or produce a desired product.

Decentralized security representative (DSR) – individual, designated by the head of the agency, who is authorized to approve requests for their agency and state resources including creation of new user IDs, modification of user access and termination of user access.

Disabled account – inactive account requiring approval from an agency's DSR to enable.

Employee – worker who is economically dependent on the business of the employer.

Expired account – elapsed account for a contractor that has exceeded the configured expiration date.

Locked-out account – account that is blocked from user access and requires the OMES Service Desk to unlock (e.g. password expiration or a user incorrectly entering a password too many times).

Terminated account – User ID for an inactive affiliate, contractor or employee that has been disabled and had all permissions removed.

User ID – unique login ID assigned to each user of state systems.

Standard

- OMES IS ensures all users (affiliates, contractors and employees) are issued a user ID whose activity is uniquely identifiable on IT systems and is established through an authentication mechanism.
- Generic accounts are not permitted without CIO approval obtained through an exception request. Generic accounts have additional controls in place for accountability and a periodic review for their applicability.

- Access for new user ID access (onboarding) is requested via the OMES IS ticketing system and must be approved by the DSR.
- Access termination requests for departed employees (offboarding) must be submitted by the user's agency at the time of separation of employment and is requested via the OMES IS ticketing system.
- Contractor accounts expire quarterly, at which time the owning agency shall review and verify continued access requirements prior to requesting extension.
- User IDs not using the system for 60 days are verified against agency leave of absence reports prior to being disabled. Following a 30-day period of being disabled, the account is offboarded. Reactivation of the account requires an onboarding ticket to be submitted.
- Offboarded accounts are archived after a period of 30 days.
- To ensure proper access and continuity of business, individual user accounts shall not be used for shared resources, such as email or calendars. A dedicated resource for team or group activities must be requested.

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: 08/08/2023	**Review cycle:** Annual
Last revised: 10/07/2024	**Last reviewed:** 10/07/2024
Approved by: Joe McIntosh, Chief Information Officer	

OKLAHOMA
Office of Management
& Enterprise Services

System and Information Integrity Standard

Introduction

Access to system information owned or operated by the State of Oklahoma is provided to employees and contractors for use to support the mission of the state. As such, system and information integrity must be maintained to ensure the accessed information has not been tampered with or damaged by an error in the information system. System and information integrity guards against improper information modification or destruction.

Purpose

This standard establishes OMES IS policy for managing risks from system flaws, vulnerabilities, malicious code, unauthorized code changes and inadequate error handling through the establishment of an effective system and information integrity program. This standard helps the State of Oklahoma implement security best practices with regards to system configuration, security and error handling.

The scope of this policy is applicable to all information technology resources owned or operated by the State of Oklahoma. Any information not specifically identified as the property of other parties that is transmitted or stored on OMES IT resources (including email, messages and files) is the property of the State of Oklahoma. All users (State of Oklahoma agency employees, contractors, vendors or others) of IT resources are responsible for adhering to this policy.

This standard is consistent with best practices associated with organizational information security management. This standard also establishes a system and information integrity capability throughout state agencies to help implement security best practices with regards to system configuration, security and error handling.

Standard

The State of Oklahoma has chosen to adopt the system and information integrity principles established in NIST SP 800-53 Rev 5.1.1 System and Information Integrity, Control Family guidelines, as the official policy for this domain. The following subsections outline the system and information integrity standards required by the State of Oklahoma. Each State of Oklahoma agency is bound to this requirement and must develop or adhere to a program plan which demonstrates compliance.

- SI-1 system and information integrity procedure – All agencies must develop, adopt or adhere to a formal, documented system and information integrity policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance.
- SI-2 flaw remediation – All agencies must:
    - Identify, report and correct information system flaws.
    - Test software updates related to flaw remediation for effectiveness and potential side effects on organizational information assets before installation.
    - Incorporate flaw remediation into the organizational configuration management process.
- SI-3 malicious code protection – All agencies must:

  - Employ malicious code protection mechanisms at information asset entry and exit points and at workstations, servers, or mobile computing devices (e.g., email, removable media and malicious websites) on the network to detect and eradicate malicious code.
  - Update malicious code protection mechanisms, including signature definitions, whenever new releases are available, in accordance with organizational configuration management requirements.
  - Configure malicious code protection mechanisms (e.g., real-time scans, periodic scans, malicious code detection) to protect state information systems and assets.
  - Address the receipt of false positives during malicious code detection and eradication and resulting potential impact on the availability of the information asset.
- SI-4 information system monitoring – All agencies must:
  - Monitor events on the information asset and detect information asset attacks.
  - Identify unauthorized use of the information assets.
  - Deploy monitoring devises (i) strategically within the information asset to collect organization-determined essential information, and (ii) at ad-hoc locations within the system to track specific types of transactions of interest to the organization.
  - Heighten the level of information asset monitoring activity whenever there is an indication of increased risk to organizational operations and assets, individuals, other organizations, or the nation based on law enforcement information, intelligence information or other credible sources of information.
  - Obtain legal opinion with regards to information asset monitoring activities in accordance with applicable federal laws, directives, policies or regulations.
- SI-5 security alerts, advisories and directives – All agencies must:
  - Receive information asset security alerts, advisories, and directives from designated external organizations on an ongoing basis.
  - Generate internal security alerts, advisories and directives to key system owners and stakeholders.
  - Implement security directives in accordance with established time frames or notifies the issuing organization of the degree of noncompliance.
- SI-6 security functionality verification – All agencies must verify the correct operation of security functions on an annual basis and notify the system administrator when anomalies are discovered to ensure timely corrective action.
- SI-7 software and information integrity – All agencies must detect unauthorized software changes within their information asset.
- SI-8 spam protection – All agencies must employ spam protection mechanisms at information asset entry and exit points and at workstations, servers, or mobile computing devices on the network to detect and take action on unsolicited messages transported by electronic mail, electronic mail attachments, web accesses, or other common means. In addition, state agencies must update spam protection mechanisms (including signature definitions) when new releases are available in accordance with OMES configuration management requirements.
- SI-9 information input restrictions – All agencies must restrict the capability to input information to the information asset to authorized personnel.
- SI-10 information input validation – All agencies must check the validity of information inputs for State of Oklahoma assets.
- SI-11 error handling – All agencies must have information assets that:
  - Identify potentially security-relevant error conditions.
  - Generate error messages that provide information necessary for corrective actions without revealing state sensitive information in error logs and administrative messages that could be exploited by adversaries.
  - Reveal error messages only to authorized personnel.

- SI-12 information output handling and retention – All agencies must handle and retain both information within and output from the information system in accordance with applicable state and federal laws, directives, policies, regulations, standards and operational requirements.

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
- United States Department of Commerce National Institute for Standards and Technology (NIST) Special Publications 800-53 Recommended Security Controls for Federal Information Systems Revision 5.1.1, Operational Controls, System and Information Integrity Control Family, November 2023.
- NIST Special Publications 800-100 Information Security Handbook: A Guide for Manager, March 2007.
- NIST Special Publications 800-40 Rev. 4 Creating a Patch and Vulnerability Management Program, April 2022.
- NIST Special Publications 800-83 Rev. 1 Guide to Malware Incident Prevention and Handling, July 2013.
- NIST Special Publications 800-61 Rev. 2 Computer Security Incident Handling Guide, August 2012.
- NIST Special Publications 800-92 Guide to Computer Security Log Management, September 2006.
- NIST Special Publications 800-94 Guide to Intrusion Detection and Prevention Systems (IDPS), February 2007.
- NIST Special Publications 800-45 Guidelines on Electronic Mail Security, February 2007.

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

Effective date: 12/16/2022	**Review cycle:** Annual
Last revised: 06/19/2024	**Last reviewed:** 09/06/2024
Approved by: Joe McIntosh, Chief Information Officer	

ATTACHMENT D-1

Network Protection Standard

Introduction
Oklahoma Cyber Command is responsible for protecting state networks and the data/applications that flow across them. Oklahoma Cyber Command's top priority is safeguarding the state's data and computer infrastructure against unauthorized data use, disclosure, modification, damage, and loss.

Purpose
This document defines the authority and services provided by Oklahoma Cyber Command.

Standard
Oklahoma Cyber Command is required to provide information security services to all state agencies, as defined in Title 62 O.S. §§ 34.11.1, including, but not limited to the following network protection services:

- Network Flow Visibility Tools.
- Intrusion Prevention/Detection Systems (IPS/IDS).
- Network Detection and Response (NDR).
- Attack Surface Management Tools (ASM).

It is the responsibility of Oklahoma Cyber Command to interpret, design, implement and manage required regulatory controls. Staff performing similar functions within state agencies must collaborate and coordinate all activities with Oklahoma Cyber Command and defer interpretation of regulations and final decisions/solutions to Oklahoma Cyber Command.

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
- Oklahoma OMES Cyber Command.

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

Effective date: 01/92/2024	**Review cycle:** Annual
Last revised: 01/12/2024	**Last reviewed:** 09/19/2024
Approved by: Joe McIntosh, Chief Information Officer	

OKLAHOMA
Office of Management
& Enterprise Services

Media Disposal Standard

Introduction
This document outlines the proper disposal of media to ensure confidential data, sensitive data and licensed software cannot be accessed by unintended persons.

Purpose
This standard establishes clear guidelines for the secure disposal of all forms of media containing sensitive information, with the aim of preventing unauthorized access and potential data breaches.

Definitions
- 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.
- Sensitive data – Confidential information that is stored, processed or managed by an organization that is confidential and only accessible to authorized users with proper permission, privilege or clearance to view.

Standard
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.

According to the Third-Party Cybersecurity Management Standard, the approved media disposal vendor must undergo routine managed assessments to identify any potential risk and ensure appropriate controls are in place to protect sensitive data.

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.

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

- Third-Party Cybersecurity Management Standard.
- NIST 800-88, Rev. 1, Guidelines for Media Sanitization.

Revision history

This standard is subject to periodic review to ensure relevancy.

Effective date: 07/26/2024	**Review cycle:** Annual
Last revised: 07/26/2024	**Last reviewed:** 07/26/2024
Approved by: Joe McIntosh, Chief Information Officer	

ATTACHMENT D-1

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.
- Employees have a responsibility to immediately report the theft, loss of or otherwise compromised personal devices to supervisors and Oklahoma Cyber Command.
    - Supervisors shall escalate as necessary depending on the sensitivity of state records accessed by the personal device.
- Employees may access, use or share state records via personal device only to the extent it is authorized and necessary to fulfill assigned job duties.
- 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.

ATTACHMENT D-1

The following are general security requirements for personal devices.

- All personal devices connecting to state information, accessing state data or state records must comply with state security policies and standards.
- 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	

ATTACHMENT D-1

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	

20. PHYSICAL AND ENVIRONMENTAL SECURITY

- Physical Access Control Standard.
- Physical Security Systems Standard.

21. PROTECTION OF INFORMATION

- Data Storage Standard.
- Data Classification Security Standard.

22. PUBLICLY AVAILABLE SYSTEMS

- Web Content Management System Standard.
- Vulnerability Scanning Standard.
- Insider Threat Standard.

23. REMOVABLE MEDIA

- Removable Media Usage Standard.

24. SECURITY PROGRAM MANAGEMENT

- Security Services Standard.

25. SEGREGATION OF DUTIES

- Information Systems Segregation Standard.

26. SEPARATION OF DEVELOPMENT AND OPERATIONAL FACILITIES

- DevOps Standard.
- Development – Continuous Integration and Continuous Delivery Standard.

27. USE OF SYSTEM UTILITIES

- Use of System Utilities Standard.
- Administrator Account Standard.
- Security Services Standard.

28. TELECOMMUNICATION SECURITY

- Network Acceptable Use Standard.
- Removable Media Usage Standard.
- Personal Device Standard.

OKLAHOMA
Office of Management
& Enterprise Services

Physical Access Control Standard

Introduction

The State of Oklahoma is committed to maintaining security of its facilities through strict control of building access. The state's environment requires controlled access to help ensure the safety of state employees and facilities from unlawful or unauthorized access. It is necessary to take appropriate measures to protect the confidentiality, integrity and availability of state data and resources.

Purpose

The document provides guidance on the layout of physical badges in order to be compatible with the statewide badging access control system and to define the underlining support model.

Standard

Physical access to non-public areas of state facilities is controlled by using state-issued badges that must be compatible with the statewide physical security control system. Badge format is uniform to ensure compatibility with the system, reduce the risk of counterfeit badges and facilitate accurate identification. Oklahoma Cyber Command manages and stores the format for all state-issued badges. Any variance to the approved format requires approval from the state Chief Operating Officer.

Due to the sensitivity of the information, the badge format and requirements are classified as confidential. Access to review the information may be granted as defined in the Confidential Standards Standard.

Additionally, all state facilities must adhere to the Physical Security Systems Standard. Only OMES IS authorized access control systems shall be used on state facilities as defined in the Physical Security Systems Standard. Oklahoma Cyber Command manages the state physical security 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.

References

- Confidential Technology Standard.
- Physical Security Systems Standard – Confidential Standard.

Revision history

This standard is subject to periodic review to ensure relevancy.

Effective date: 03/02/2022	**Review cycle:** Annual
Last revised: 03/02/2022	**Last reviewed:** 08/23/2024
Approved by: Joe McIntosh, Chief Information Officer	

ATTACHMENT D-1

OKLAHOMA
Office of Management
& Enterprise Services

Physical Security Systems Standard

Introduction

The State of Oklahoma has a responsibility to protect state buildings, assets, IT systems, applications and data entrusted to it by its citizens. Therefore, it is necessary to take appropriate measures to ensure the security of these public IT assets. The safety and security of the physical space and assets are a shared responsibility of all agencies in the State of Oklahoma. To meet this obligation, OMES IS has established this standard to outline the hardware and software requirements for access control, video surveillance systems and physical intrusion detection systems. Only OMES IS authorized access control systems, video surveillance systems and physical intrusion detection systems shall be used on state facilities.

Purpose

This document establishes baseline controls to guide state agencies in the purchase and installation of physical security systems and alarms.

Definitions

Integrator – The vendor who is responsible for the installation and configuration of the physical security system.

Networked video recorder – A computer system that records video transmitted over the network from multiple surveillance cameras and saves it to a storage device.

Access control system – A software and hardware system restricting entrance to a property, a building or a room through technological means, typically including automated locks and access cards and management software.

Physical intrusion detection system – A software and hardware system that detects unauthorized physical access to building or room through technological means, typically including motion sensors, door contacts and management software.

Standard

The State of Oklahoma requires licensing for vendors responsible for installation, inspection and testing of security alarm systems. Additionally, vendors installing and/or testing such systems and their employees must undergo a national criminal background check facilitated by a third party or the Department of Labor.

All physical security hardware and software assets must meet the specifications defined in this standard. This document outlines the requirements set forth by OMES IS to implement physical security system controls. The technical specifications for approved physical security systems are available upon request.

OMES IS has an established naming convention for physical security systems with the intent of providing users with intuitive information within the name. Therefore, naming conventions for all equipment must be in a format approved by OMES IS. No variation is allowed unless written approval is obtained from the Chief Information Security Officer.

Power and network telecommunications cabling should be protected from interception, interference or damage. Infrastructure for cabling must be consistent with the following:

- All cables must be installed by one of the following.
  - Integrator responsible for the project
  - Structured cable company approved by OMES.
- No cable is allowed to lay on the dropped ceiling or hard deck. It may be suspended no more than three feet above the ceiling wherever possible. Additionally, NVR cables should be installed in a data cable tray when provided.
- Cable hangers are required.

- For NVR, splicing is not permitted in CAT data cable and the distance cannot exceed 330 feet end-to-end. For electric door hardware and access control, splicing above the ceiling is not permitted except for when there is no access within a reasonable distance of the device. In this scenario, a junction box is required.
- NVR does not require a service loop; however, sufficient slack is recommended. Electric door hardware and access control requires a small service loop above every door. The service loop must not exceed three loops and should be neatly hung above the door and not on the ceiling.

The state's standard platforms for video surveillance, access control systems and physical intrusion detection systems are to be designed and implemented with the assistance of Oklahoma Cyber Command.

- All networked cameras used to record, or monitor must be connected to a separate network on the back of the NVR, as well as connect to a separate NIC. The system must only be accessed by the local NVR authorized users. Additionally, the NVR is used to view and playback data from the cameras.
- It is the security integrators responsibility to design an access control system in compliance with local safety codes. Any variance to the hardware configuration must be provided in writing by the agency prior to awarding a contract.
- It is the security integrator's responsibility to design a physical intrusion detection system in compliance with state and local codes. Any variance to the hardware configuration must be provided in writing by the agency prior to awarding a contract.
- A list of approved products is maintained by OMES Cyber Command.

Compliance

This standard shall take effect upon publication and is made pursuant to Title 62 O.S. §§ 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

- Physical Security System Technical Specifications.

Revision history

This standard is subject to periodic review to ensure relevancy.

Effective date: 12/06/2021	**Review cycle:** Annual
Last revised: 11/30/2023	**Last reviewed:** 08/23/2024
Approved by: Joe McIntosh, Chief Information Officer	

OKLAHOMA
Office of Management
& Enterprise Services

Data Storage Standard

Introduction

To ensure quality service and appropriate governance, data should be stored on a narrow set of purpose-built platforms.

Purpose

The purpose of this standard is to provide broad guidance to data owners on where data should be stored.

Definitions

Transactional Data – Data, which is accessed by numerous users to perform fast, simple queries. Typically, data which is directly associated with a user-facing application.

Analytical Data – Multi-dimensional data which is used to drive analytics and insights.

Document Data – Data derived from scanning paper documents.

Archival Data – Data which has no active use but needs to be kept because it may be subject to audits, open records requests or similar scenarios.

Historical Data – Data, for which its original use case has been retired, but still needs to be periodically searched. These datasets are no longer changing and no longer queried by other applications.

State Data Platform (SDP) – The State Data Platform is a centralized platform with data storage, management and processing capabilities.

Standard

Data Characteristics	Data Storage Solution	Details
• Archive or Historical Data	Please see Data Archiving Standard	
• Application or otherwise transactional data	SQL or Oracle database	• Solution and hosting location defined by the Database Administration team
• Operational or Log data	ITOCC	
• Documents	Please see the standard for document storage	
• Analytical, event-based, or any other type of data	State Data platform	• Solution defined by the Data Platform team

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: 07/24/2023	**Review cycle:** Annual
Last revised: 07/20/2023	**Last reviewed:** 07/20/2023
Approved by: Joe McIntosh, Chief Information Officer	

OKLAHOMA
Office of Management
& Enterprise Services

Data Classification Security Standard

Introduction
The State of Oklahoma requires state-owned data to be classified and labeled based on the potential adverse impact due to loss of data confidentiality, integrity and availability. Classification and labeling are required to identify appropriate data protection measures.

Purpose
This document defines the requirements and guidelines for classifying state owned data.

Definitions
Availability – Ensuring timely and reliable access to and use of information.

Confidentiality – Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information.

Data classification – Organizing and identifying data by relevant categories so it may be used and protected more efficiently.

Integrity – Guarding against improper information modification or destruction and includes ensuring information non-repudiation and authenticity.

Provisional recommendations – A recommendation for impact determination based on information type. Provisional recommendations are subject to review and modification by agency stakeholders.

Standard
The State of Oklahoma's data are essential resources that must be protected from unauthorized use, access, disclosure, modification, loss or deletion. The appropriate level of physical, technical and administrative safeguards necessary to provide protection is relative to the potential impact in the event of loss of data confidentiality, integrity and availability.

Each Oklahoma agency shall classify its data and add metadata tags (labels) in accordance with this standard to ensure appropriate protections and consistence throughout the data life cycle. Data owners at the agency level are responsible for ensuring proper classification of data sets.

To ensure standardization across agencies, data sets shall be classified using high, moderate and low indicators based on potential impact in the event of a loss of confidentiality, integrity and availability. Agencies shall use the classification guidance detailed in the most current revisions of NIST 800-53R, NIST FIPS 199, and NIST 800-60 Volumes I and II.

At a minimum, data classification shall address the items listed below.

- Data type.
- Confidentiality impact.
- Integrity impact.
- Availability impact.
- Disaster Recover (DR) priority.
- Retention requirement – optional but should be included.

ATTACHMENT D-1

Data type

Data classification labels shall be used in each system, application and database having this functionality, and ServiceNow shall be used whenever possible to maximize centralization.

To classify data, the data type must first be identified. Identifying the data type provides information about the value, legal requirements, sensitivity and criticality of the data, which inform impact determinations.

All production level data sets must identify data type/what statutes or regulations apply (e.g., HIPAA, FERPA, IRS Pub.1075, GDPR, PCI requirements). A non-exhaustive list of common data types is included as Attachment 1, and agencies should consult NIST guidance, when classifying data.

Impact levels

Impact Level	**Definitions / Example**
Low	The loss of confidentiality, integrity, or availability could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals. Explanation: A limited adverse effect means that, for example, the loss of confidentiality, integrity, or availability might: (i) cause a degradation in mission capability to an extent and duration that the organization is able to perform its primary functions, but the effectiveness of the functions is noticeably reduced; (ii) result in minor damage to organizational assets; (iii) result in minor financial loss; or (iv) result in minor harm to individuals. *Footnote: Adverse effects on individuals may include, but are not limited to, loss of the privacy to which individuals are entitled under law.
Moderate	The loss of confidentiality, integrity, or availability could be expected to have a serious adverse effect on organizational operations, organizational assets or individuals. Explanation: A serious adverse effect means that, for example, the loss of confidentiality, integrity or availability might: (i) cause a significant degradation in mission capability to an extent and duration that the organization is able to perform its primary functions, but the effectiveness of the functions is significantly reduced; (ii) result in significant damage to organizational assets; (iii) result in significant financial loss; or (iv) result in significant harm to individuals that does not involve loss of life or serious life threatening.
High	The loss of confidentiality, integrity or availability could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets or individuals. Explanation: A severe catastrophic adverse effect means that, for example, the loss of confidentiality, integrity or availability might: (i) cause a severe degradation in or loss of mission capability to an extent and duration that the organization is not able to perform one or more of its primary functions; (ii) result in major damage to organizational assets; (iii) result in major financial loss; or (iv) result in severe or catastrophic harm to individuals involving loss of life or serious life-threatening injuries.

Disaster recovery

Additionally, a disaster recovery tier must be identified for each application as indicated below.

Tier	Definition
Tier 1: Mission Critical	Life safety and extreme business impact. Fundamental, essential business or technology functions or services required for the daily operation of the agency in order to complete their agency mission in part or while. In a disaster recovery mode, these are the first services restored. Failure of these services could result in life or safety issues or loss of revenue, or fines imposed on the agency by outside bodies.
Tier 2: High Priority	Severe business impact. Functions and services that are required for the agency to complete its mission (in part or in whole) but do not result in any life or safety issues. Interruption of these services can cause a hardship to staff and/or the public and prevent the agency from fully serving its business customer base.
Tier 3: Normal Priority	Medium to high business impact. Functions or services that support the agency mission but do not pose an immediate risk to the agency being able to serve its business customer base. Failure of this function or service may cause an inconvenience to staff but does not post any risk to life or safety.
Tier 4: Low Priority	Not critical but impacting. Functions or services that provide supplemental or auxiliary support to the technical or business functions of the agency. These functions and services do not contribute directly to the agency completing its missions but to provide additional detail, information, data or context to mission essential functions or services.

Retention requirements

Although not required for classification of information, documenting records retention/destruction requirements is key to ensuring proper maintenance of the records retention lifecycle.

With certain statutory exceptions, all state agencies, boards and commissions are required to establish and maintain ongoing programs for the efficient and economical management of records and have their programs approved by the Archives and Records Commission (67 O.S. Sec 206, 305).

Records disposition schedules are reviewed and approved by the Archives and Records Commission as provided in Chapter 10A of Title 67 of the Oklahoma Statutes and in the rules for the Commission as set out in Title 60 of the Oklahoma Administrative Code.

The following is an example of data classification.

- Agency A provides health care delivery services to beneficiaries. A data owner at agency A is classifying a data set that contains information about the agency's health care delivery services.
- The data owner must first determine what type of information is contained in the data. They review that data and determine that it contains PHI and is subject to HIPAA requirements.
- The data owner consults NIST SP 800-60 Volume II for guidance on how to classify this information and sees that the provisional recommendation for health care delivery service data is confidentiality of low, integrity of high) and availability of low). However, because the data set is subject to HIPAA, the data owner determines that the confidentiality impact determination should be raised to moderate.

- The data owner tags the data set in the appropriate system as confidentiality of moderate, integrity of high and availability of low. The data owner must also tag the data set with the information the data type/applicable regulation (HIPAA) and must designate a disaster recovery tier for the data or application, as applicable. The data owner consults the disaster recovery tier table in this standard and determines that failure of the application housing the data, would result in a severe business impact, so the data owner designates disaster recovery tier 2 for the application. The data owner should also record the applicable record retention citation.

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

- Oklahoma Libraries Records Management.
- Oklahoma Libraries Records Scheduling.
- Consolidated General Records Disposition Schedule.
- NIST Federal Information Processing (FIPS) 199, Standards for Security Categorization of Federal Information and Information Systems.
- NIST SP 800-60 Vol 1 Rev 1, Guide for Mapping Types of Information and Information Systems to Security Categories.
- NIST SP 800-60 Vol. 2 Rev. 1, Appendices to Guide for Mapping Types of Information and Information Systems to Security Categories.
- NIST Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1.
- NIST Internal Report 8112, Attribute Metadata: A proposed Schema for Evaluating Federated Attributes.
- NIST Privacy Framework: A tool for Improving Privacy Through Enterprise Risk Management, Version 1.0.
- NIST SP 800-53 Rev. 5, Security and Privacy Controls for Information Systems and Organizations.
- NIST SP 800-154, Guide to Data-Centric System Threat Modeling.
- NIST SP 800-171 Rev. 2, Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations.
- NIST SP 800-207, Zero Trust Architecture.

Revision history

This standard is subject to periodic review to ensure relevancy.

Effective date: 04/13/2022	**Review cycle:** Annual
Last revised: 12/12/2022	**Last reviewed:** 08/02/2023
Approved by: Joe McIntosh, Chief Information Officer	

Attachment 1

The following table lists commonly encountered data types along with authorities that protect them, if applicable. This is not an exhaustive list of every data type an agency may encounter or every legal authority that applies. Where the Data Type column notation references a statute or regulation (e.g., DPPA) this is meant as quick reference for information that is subject to that regulation. For example, while Driver's Privacy Protection Act (DPPA) is not itself a data type, the agency data owner is expected to tag information subject to the DPPA with DPPA as an information type.

Additionally, some data may be protected by multiple statutes or regulations.

Data Type	Description/Authority	Citation
Open – public record	Oklahoma Open Records Act	51 O.S. § 24A.1 et seq.
Adult criminal protected information	Adult criminal records protected by state or federal statutes or regulations	*
Public assistance records	Applicant/beneficiary/recipient of public assistance programs	56 O.S. § 183 and 45 CFR § 205.50
APS case information	Adult Protective Services (APS)	43A O.S. §§ 10-110 and 10-110.1
CJIS	Criminal Justice Information Services Information	28 U.S.C. §534 and 28 CFR Part 20
Child welfare/juvenile deprived	Oklahoma Children's Code	10A O.S. §§ 1-2-108 and 1-6-102
Adoption information	Oklahoma Adoption Code	10 O.S. 7505-1.1; § 10 O.S. 7510-1.5
DPPA	Driver's Privacy Protection Act (DPPA)	18 USC §2721, et seq.
FERPA	Family Educational Rights and Privacy Act	20 U.S.C. § 1232g; 34 CFR Part 99
GDPR	General Data Protection Regulation	(EU) 2016/679
Income Information		*
FTI	Federal Tax Information	IRS 1075 Publication Rev 11-2021 / Internal Revenue Code (IRC) § 6103(p)(4)
Juvenile/youthful offender	Youthful Offender Act; also, OSBI records per 74 O.S. §150.9(C)	10A O.S. §§ 2-5-204-205 and 2-6-102; 74 O.S. § 150.9(C)
PCI	Payment Card Industry Data Security Standards	PCI DSS v4.0
PHI - HIPAA	The Health Insurance Portability and Accountability Act	Pub. L. No. 104-191
SSA Data	SSA provided information (PII)	Privacy Act, 5 U.S.C. 552a, section 1106 of the Social Security ACT and SSA's disclosure regulations.

PHI – substance use (federally assisted programs)	Confidentiality of Substance Use Disorder Patient Records	42 C.F.R. Part 2
PHI – mental health/drug or alcohol abuse	Confidentiality of Alcohol and Drug Abuse Patient Records	43A O.S. § 1-109
PII - other	Personally identifiable information	*
PII - Public Health Investigations	Public Health Code	63 O.S. § 1-502.2
PHI - Oklahoma Health Care Information System	Oklahoma Health Care Information System Act	63 O.S. § 1-120

* The agency data owner should determine what legal authorities apply, if any, and provide the applicable citation.

ATTACHMENT D-1

OKLAHOMA
Office of Management
& Enterprise Services

Web Content Management System Standard

Introduction

This standard ensures the enterprise website content management system platform, Adobe Experience Manager, or AEM, is utilized by state personnel and vendors in a standardized way that conforms to state security, branding, development and design policies.

Purpose

The purpose of this standard is to describe the state standard for using AEM. The goal of this document is to control costs, reduce technical debt, maintain security and enhance the state's ability to support websites. Developing on common tools and platforms creates a shared context for understanding state information and communication between citizens and government.

Definitions

AEM – Adobe Experience Manager. Web content management software.

Standard

AEM is the web platform of priority for state use. Other platforms may be considered by OMES IS on a case-by-case basis.

Proper use of environments (production, stage, QA, development) must be utilized according to OMES IS software development standards.

Custom development must use designated state code repositories and follow proper code escalation and OMES IS change management policies when deploying to the environments.

All sites must adhere to the state-issued brand design and any modifications to AEM design templates must be reviewed by OMES IS.

All sites on platform must use the official Oklahoma web domain (Oklahoma.gov) and URLs on platform. Ok.gov may be used for vanity marketing, which must be redirected to a resolved platform URL (e.g. projects.ok.gov to Oklahoma.gov/projects).

Any submission of data using integrated or embedded forms must adhere to strict security protocols and data privacy policies for transmitting for the type of data submitted.

All platform users must be properly provisioned through an AEM user provisioning request and be carried out by OMES IS security provisioning.

Each AEM site must be registered with OMES IS. Each site must have designated agency sponsors for the responsibility of registering users and authors.

It is the responsibility of each agency to maintain accurate, up-to-date website information for their agency's website.

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 branding guidelines.
- Web accessibility statutes.

Revision history

This standard is subject to periodic review to ensure relevancy.

Effective date: 05/06/2022	**Review cycle:** Quarterly
Last revised: 05/06/2022	**Last reviewed:** 12/14/2022
Approved by: Jerry Moore, Chief Information Officer	

OKLAHOMA
Office of Management
& Enterprise Services

Vulnerability Scanning Standard

Introduction

This standard elaborates on the methodology used by Oklahoma Management and Enterprise Services for vulnerability scanning and patch management for all state agency systems that OMES manages or monitors per service level agreement; tracking and reporting those vulnerabilities, and documenting remediation through the patch management process.

Purpose

This document establishes the vulnerability and patch management standard for the State of Oklahoma. By applying security-related software or firmware updates (patches) to applicable IT systems, the expected result is reduced time and money spent dealing with exploits by reducing or eliminating the related vulnerability.

Definition

State systems and assets include, but are not limited to:

- Workstations, such as laptops, desktops, tablets, etc., that are managed by OMES.
- Servers, such as database servers, web servers, virtual servers, etc., internal to the state network. This *excludes* hosted servers or services that lie outside of the internal network.
- Hosted servers or SaaS solutions must provide a vulnerability management solution at least as comprehensive as described in this document and a reporting mechanism back to Oklahoma Cyber Command no less than monthly.

Standard

Vulnerability scans will be conducted monthly on all agency-connected devices and servers for software application and hardware vulnerabilities:

- Vulnerabilities for software or applications, such as CVE's, exploits, or other vulnerabilities.
- Vulnerabilities for hardware, such as drivers, components, etc.
- All currently open ports on the system.
- Missing patches pertaining to software installed on the system being scanned.
- Missing patches for the current OS running on the system being scanned.
- Vulnerability definitions are continuously updated by defensive security tools and automatically distributed to the platform via cloud-based administration.

Vulnerability scan reports are produced automatically from the monthly scans and made available to agency auditing or compliance staff, OMES IS tower leadership (i.e., server team) and select Cyber Command Defense engineers and technicians, as requested. Reports can be downloaded for viewing in several formats. Vendor access to reports must be reviewed and approved on a case-by-case basis.

ATTACHMENT D-1

Reports from past vulnerability scans are archived and available on demand. Available features, upon request include:

- Dashboards to track scan history.
- Scanning for remediation, either on demand or during subsequent scans.

Patch management must be addressed as follows:

- All nonconsolidated agencies must assign a business owner responsible for patch management. OMES is responsible for patch management for all consolidated agencies.
- If patch management is outsourced, service level agreements must be in place addressing the requirements of this standard and outlining responsibilities for patching. If patching is the responsibility of the third party, agencies must verify the patches have been applied.
- Patching must include all application software. This includes enterprise applications, custom applications, commercial off-the-shelf applications, legacy applications and all related software such as operating systems, virtualization, database, etc.
- A process must be in place to manage patches. This process must include the following:
    - Monitoring security sources for vulnerabilities, patch and non-patch remediation and emerging threats. Example security sources are vendor website or notification lists, vulnerability scanners, penetration tests and the National Vulnerability Database.
    - Overseeing patch distribution, including verifying a change control procedure is followed.
    - Testing for stability and deploying patches.
    - Using an automated centralized patch management distribution tool whenever technically feasible. The tool should maintain a database of patches, deploy patches to endpoints and verify the installation of patches.
- Appropriate separation of duties must exist so that the individual(s) verifying patch distribution is not the same individual(s) distributing the patches.
- As per the Information Security Policy Procedures and Guidelines policy, all agencies must maintain an inventory of hardware and software assets. Patch management must incorporate all installed IT assets.
- Patch management must be prioritized based on the severity of the vulnerability the patch addresses. In most cases, severity ratings are based on the Common Vulnerability Scoring System and CISA directives. A CVSS score of 7-10 is considered a high-impact vulnerability, while 4-6.9 is considered a moderate-impact vulnerability and 0-3.9 is considered a low-impact vulnerability. A CISA directive is considered a critical-impact vulnerability.
- The patching process must follow the timeline shown here:

Impact/Severity	Patch Initiated	Patch Completed
Critical	Within **24 hours** of patch release.	Within **1 week** of patch release.
High	Within **24-72 hours** of patch detected in vulnerability management software.	Within **2 weeks** of patch detection.

Impact/Severity	Patch Initiated	Patch Completed
Medium	Within **1 week** of patch release detected in vulnerability management software.	Within **1 month** of patch detection.
Low	Within **1 month** of patch release detected in vulnerability management software.	Within **365 days** during normal maintenance cycles unless ISO determines this an insignificant risk to environment.

- If patching cannot be completed in the specified timeframe, an extension must be requested from the chief information officer and the chief information security officer. The extension request must include:
    1. Detailed explanation of why the patching cannot be completed in the timeframe listed.
    2. List of compensating controls put in place.
    3. Remediation plan for getting the system(s) compliant with specified timeframe(s). **Note: Any system that is noncompliant for more than two periods annually is subject to decommissioning.**
- If a patch requires a reboot for installation, the reboot must occur within the specified timeframe.

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 Special Publications: NIST 800-40.
- Common Vulnerability Scoring System.
- State of Oklahoma Security Policy, Procedures, Guidelines.
- Internal – IS 06.01.01 Change Management Process SOP.

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

Effective date: 05/16/2023	**Review cycle:** Annual
Last revised: 01/12/2024	**Last reviewed:** 01/12/2024
Approved by: Joe McIntosh, Chief Information Officer	

ATTACHMENT D-1

Insider Threat Standard

Introduction
Insider threats pose a significant risk to the State of Oklahoma, but some steps can be taken to mitigate this risk. Establishing and adhering to a comprehensive Insider Threat Program (ITP) is crucial to effectively address this threat.

Purpose
This standard applies to all employees, contractors, and third-party vendors who have access to the organization's systems, networks and data.

Definitions
Insider threat – Any person with authorized access to an organization's systems, data or facilities who risks the confidentiality, integrity or availability of the organization's assets.

Insider Threat Program (ITP) – A structured set of policies, procedures and technologies designed to identify, manage and mitigate insider threats.

Standard
- Access Controls.
  - Cyber Command must establish strict access controls that limit user permissions based on their job responsibilities and work requirements. Access should be granted on a need-to-know basis and should be reviewed and updated regularly.
- Monitoring.
  - Cyber Command must establish monitoring procedures to detect any abnormal behavior or attempts to access unauthorized information. Cybercommand must employ technical and behavioral monitoring tools to detect abnormal activities. Monitoring should be conducted in a manner that is consistent with applicable laws, State of Oklahoma policies, procedures and regulations and should respect employee privacy.
- Background checks.
  - The ITP should require thorough background checks before hiring new employees to ensure they have no history of malicious activity or other red flags. Ongoing background checks should also be conducted for employees with access to sensitive information.
- Education and awareness.
  - Cyber Command must include education and awareness programs for employees to cover the various types of insider threats and provide guidance on how to identify and report suspicious activity. The programs should be regularly updated to reflect changes in the threat landscape.
- Audits and reviews.
  - Cyber Command must establish procedures for regular audits and reviews to identify potential vulnerabilities and ensure continued compliance with security protocols.

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
- Background Check Standard.
- Identity Management Standard.
- Simulated Phishing Standard.
- Security Awareness Standard.

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

Effective date: 11/01/2023	**Review cycle:** Annual
Last revised: 11/01/2023	**Last reviewed:** 09/06/2024
Approved by: Joe McIntosh, Chief Information Officer	

OKLAHOMA
Office of Management
& Enterprise Services

Removable Media Usage Standard

Introduction

Oklahoma Cyber Command is responsible for protecting state users, their managed devices, and connectivity to data and applications. Oklahoma Cyber Command's top priority is safeguarding the state's data and computer infrastructure against unauthorized data use, disclosure, modification, damage and loss.

Purpose

This document establishes acceptable use requirements for sharing, receiving or storing state data utilizing removable media devices.

Microsoft OneDrive is the preferred alternative to using any form of removable media device for sharing, receiving or storing state data. OneDrive for Business is provided to all state employees and contractors as the approved storage solution. OneDrive has been vetted for the protection of state data and users' privacy (Reference Workstation Data Storage Standard).

Definitions

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.

Standard

Oklahoma Cyber Command is required to provide information security services to all state agencies, as defined in Title 62 O.S. § 34.11.1, including establishment of data protection controls.

Unmanaged usage of removable media devices creates increased risk of sensitive data disclosure either inadvertently through loss or theft of the device or by purposeful data exfiltration. To assist in mitigating sensitive data disclosure risks, Oklahoma Cyber Command shall implement technological-based procedures to disallow regular usage of removable media devices not previously approved for use within our managed enterprise environment.

For a removable media device to receive regular usage approval:

- The device must be a state-owned asset. Personally owned devices shall not be utilized to share, receive or store state data.
- The device must be capable of hardware encryption that meets or exceeds applicable regulatory compliance requirements (generally FIPS 140-2, level 2 or 3 will cover the most stringent requirements).
- The device must internally contain and report an individual vendor/model/serial number which provides an inventory control mechanism.
- Vendor devices meeting this criterion are listed below. Please confer with Oklahoma Cyber Command for review and approval of comparable devices outside this list.
    - Secure Data.
    - Apricorn.
    - Data Locker.
    - Kanguru.

After each use-case for sharing, receiving or storing state data has been completed, data must be purged from the removable device in accordance with any and all applicable state and federal regulations.

Exceptions to removable media device regular usage approval must be requested with a documented business justification for CIO review.

It is the responsibility of Oklahoma Cyber Command to interpret, design, implement and manage required regulatory controls. Staff performing similar functions within state agencies must collaborate and coordinate all activities with Oklahoma Cyber Command and defer interpretation of regulations and final decisions/solutions to Oklahoma Cyber Command.

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

- Workstation Data Standard.
- Oklahoma State Statute, Title 62.
- National Institute of Standards and Technology.

Revision history

This standard is subject to periodic review to ensure relevancy.

Effective date: 06/04/2024	**Review cycle:** Annual
Last revised: 06/07/2024	**Last reviewed:** 09/19/2024
Approved by: Joe McIntosh, Chief Information Officer	

ATTACHMENT D-1

OKLAHOMA
Office of Management
& Enterprise Services

Security Services Standard

Introduction

Oklahoma Cyber Command is responsible for protecting state users and their devices, networks, data and applications. Oklahoma Cyber Command's top priority is safeguarding the state's data and computer infrastructure against unauthorized data use, disclosure, modification, damage and loss. The OMES IS division supports Cyber Command's vision to provide leadership in the development, delivery and maintenance of cybersecurity, information security, risk management, enterprise fraud, physical security systems, compliance and privacy programs.

Purpose

This document defines the authority and services provided by Oklahoma Cyber Command.

Standard

Oklahoma Cyber Command is required to provide information security services to all state agencies, as defined in Title 62 O.S. §§ 34.11.1, including, but not limited to the following.

- Defensive services:
  - Endpoint management.
  - Virtual Desktop Infrastructure (VDI).
  - Endpoint Detection and Response (EDR).
  - Endpoint encryption.
  - Security assessment.
  - Secure Mail Gateway (SMG).
  - Secure Web Gateway (SWG).
  - Virtual Private Network (VPN).
  - Intrusion Prevention/Detection Systems (IPS/IDS).
  - Multi-Factor Authentication (MFA).
  - Privilege Access Management (PAM).
- Security education:
  - Security Education and Awareness Training (SEAT).
  - Simulated phishing campaigns.
- Offensive services:
  - Access control.
  - Threat intelligence collection, analysis, exploitation and production.
  - Forensics.
  - Investigations.
  - Threat assessments.
  - Threat monitoring and analysis.
  - Security Information and Event Management (SIEM).
  - Incident response.
  - Security assessment.
  - Facility Access Management Systems (FAMS).
  - Surveillance systems.
  - Physical Intrusion Detection Systems (IDS).
  - Facility project support.
  - Fraud prevention, detection, and investigation.
  - Third-party risk management.
  - Information sharing and analysis.

It is the responsibility of Oklahoma Cyber Command to interpret, design, implement and manage required regulatory controls. Staff performing similar functions within state agencies must collaborate and coordinate all activities with Oklahoma Cyber Command and defer interpretation of regulations and final decisions/solutions to Oklahoma Cyber Command. Through the Oklahoma Information Sharing and Analysis Center (OK-ISAC), Oklahoma Cyber Command maintains relationships and facilitates information sharing between regulatory bodies, including federal partners, industry oversight bodies and state/local law enforcement agencies to monitor cyber trends and help reduce the risk of cyber threats.

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

- Oklahoma OMES Cyber Command.
- OMES Unified but not Consolidated.

Revision history

This standard is subject to periodic review to ensure relevancy.

Effective date: 04/07/2022	**Review cycle:** Annual
Last revised: 08/25/2023	**Last reviewed:** 08/26/2024
Approved by: Joe McIntosh, Chief Information Officer	

ATTACHMENT D-1

OKLAHOMA
Office of Management
& Enterprise Services

Information Systems Segregation Standard

Introduction

This security standard aims to provide guidelines and best practices governing the separation of information system environments. At minimum, information systems in the State of Oklahoma should have segregated development (Dev) and production (Prod) environments. Separation is essential to maintain security, integrity, and operational stability and to prevent unauthorized access and accidental disruptions.

Purpose

This standard applies to all employees, contractors and third-party vendors with access to the State of Oklahoma's systems, networks and data.

Standard

- 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.

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

Effective date: 05/13/2024	**Review cycle:** Annual
Last revised: 05/13/2024	**Last reviewed:** 09/06/2024
Approved by: Joe McIntosh, Chief Information Officer	

OKLAHOMA
Office of Management
& Enterprise Services

DevOps Standard

Introduction

The State of Oklahoma has made a commitment to develop software using a DevOps philosophy.

With DevOps, quality assurance and security teams become more tightly integrated with development and operations throughout the application lifecycle.

Teams that follow DevOps practices automate processes that historically have been manual and slow. They use a technology stack and tooling which helps them operate and evolve applications quickly and reliably.

Purpose

The purpose of this standard is to provide guidance to vendors who are selected to create or modify custom solutions for the state.

Standard

- Code repository.
    - GitHub is the code repository used by the state. Vendors must request access to the state's repository and store all project code there.
    - Azure DevOps Repos is an acceptable alternative for GitHub Enterprise for code storage and source control.
- Testing and building source code.
    - Azure DevOps or Github Actions are used to build, test and deploy application source code.
- Each project has at a minimum, a develop branch and a production branch.
- The default branch for a repository should be called develop and not master.
- Each project should have a basic continuous integration/continuous deployment workflow that tests the basic build function of the project.

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: 05/24/2022	**Review cycle:** Annual
Last revised: 05/24/2022	**Last reviewed:** 7/28/2022
Approved by: Joe McIntosh, Chief Information Officer	

OKLAHOMA
Office of Management
& Enterprise Services

Development – Continuous Integration and Continuous Delivery Standard

Introduction
Continuous integration and either continuous delivery or continuous deployment are important pieces of the modern development workflow.

Purpose
The purpose of this document is to establish a standard for OMES development around the testing and deployment of applications and to establish the tools and products used for this part of the development workflow.

Definitions
Continuous delivery – Continuous delivery automatically deploys all code changes that have passed continuous integration into a testing and/or production environment after the build stage. Typically, these changes are grouped together and then released as a standard release every two weeks.

Continuous deployment – A more advanced concept where all changes in the code repository are automatically moved to production without going to a testing environment first. Instead of code being released during release days, every code change results in a corresponding release.

Continuous integration – The step during the development process where tests are run (typically automatically) as code is checked into a code repository.

Standard
Any tool that has been approved for CI/CD on the OMES reference architecture is allowed. If there is no specific tool listed on the reference architecture, it is expected that the development group should use either GitHub Enterprise or Azure DevOps tools for CI/CD in their development.

All new applications created after the establishment of this standard must implement at least the most basic form of CI/CD in that they must:

- Keep their code in a Git repository in either GitHub Enterprise or Azure DevOps.
- Add a basic build test for CI purposes to make sure the app can build before it can be deployed.
- Connect the Git repository to the deployment space with a code pipeline using the available CD tools so code that has passed approval and testing can be deployed.

It is acceptable for code that has been tested and passed automated approval to be “gated” or held for deployment approval until a pipeline approver has approved it to be deployed. It is also acceptable for code to be deployed from development to test to production or any other branching standard set by the repository admin.

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:** Quarterly
Last revised: 04/05/2022	**Last reviewed:** 06/29/2022
Approved by: Jerry Moore, Chief Information Officer	

OKLAHOMA
Office of Management
& Enterprise Services

Use of System Utilities Standard

Introduction
The State of Oklahoma controls and restricts many system utilities to ensure the safety and security of state systems and data. Most computer installations have one or more system utility programs that might be capable of overriding system and application controls. Use of these system utility programs must be restricted and tightly controlled.

Purpose
This document provides system control options to protect State of Oklahoma assets.

Definitions
System utilities – Software programs that perform specific tasks related to the operation and maintenance of a computer system.

Standard
The following controls should be considered to protect State of Oklahoma assets:

- Use of authentication procedures for system utilities.
- Segregation of system utilities from applications software.
- Limitation of the use of system utilities to the minimum practical number of
- trusted authorized users.
- Authorization for ad hoc use of systems utilities.
- Limitation of the availability of system utilities, e.g. for the duration of an authorized change.
- Logging of all use of system utilities.
- Defining and documenting of authorization levels for system utilities.
- Removal of all unnecessary software-based utilities and system software.

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
- Information Security Policy, Procedures and Guidelines.

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

ATTACHMENT D-1

Effective date: 09/06/2024	**Review cycle:** Annual
Last revised: 09/06/2024	**Last reviewed:** 09/06/2024
Approved by: Joe McIntosh, Chief Information Officer	

ATTACHMENT D-1

OKLAHOMA
Office of Management
& Enterprise Services

Administrator Account Standard

Introduction

Pursuant to 62 O.S. §§ 34.11.1 and 34.12, OMES Information Services is responsible to direct the development, implementation and management of appropriate standards, policies and procedures to ensure success of state information technology initiatives and to establish and enforce minimum mandatory standards for information security and internal controls.

Such authority and responsibility are critical to the mission of OMES IS established therein. Accordingly, this standard applies to all State of Oklahoma employees, wherever located.

The consolidation of information technology infrastructure, data and computer systems presents unique possibilities and challenges for the State of Oklahoma. As a result of consolidation, advancements and an ever-evolving information ecosystem, new approaches to cybersecurity are required. The impact to citizens, the economy of Oklahoma and the nation depend on the cybersecurity posture of the state's IT infrastructure and computer systems. Attacks such as malicious code attacks, directed attacks by hackers and foreign governments, Advanced Persistent Threats, criminal enterprise, espionage and employee misconduct have advanced to the realm of technically proficient attackers and those with the motivation to succeed at all costs.

Purpose

This document establishes the requirements for administrator rights for state employees.

Standard

OMES does not allow for administrator access by users or super users. A user may request an exception; however, only OMES IS employees are eligible for elevated privileges.

When users are granted an administrator account, these additional responsibilities apply.

- Employees must not use the administrator account to browse the web (unless directly for the correction or facilitation of assigned work duties).
- Employees must not use the administrator account as a normal login for daily systems use. Additionally, the account shall be used only for items that require administrative access to correct issues or resolve problems.
- Employees shall not use the administrator account to change or modify any portion of the systems to bypass or circumvent security controls and all usage as an administrator account must be in accordance with this standard, as well as all federal, state and local laws.
- Employees shall not install unapproved software on state-owned assets and must follow current established procedures for permission to install software through the OMES Service Desk.
- Employees shall not install personal applications on state-owned assets – free software is not free. The tracking and usage taken from the systems violates state confidentiality and privacy laws and could lead to a compromise of state and federal data.
- Employees shall avoid reusing or cycling old passwords; a new password cannot be the same as the previous 24.
- Employees shall create a password with a minimum length of 15 characters.
- Passwords shall include at least one lowercase letter, uppercase letter, numeral and special character.
- Employees with administrator accounts are required to change their passwords at least every 60 days.
- Administrators must utilize a strong two-factor authentication hardware token.

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

- Background Check Standard.

Revision history

This standard is subject to periodic review to ensure relevancy.

Effective date: 10/21/2013	**Review cycle:** Annual
Last revised: 12/01/2023	**Last Reviewed:** 09/06/2024
Approved by: Joe McIntosh, Chief Information Officer	

ATTACHMENT D-1

OKLAHOMA
Office of Management
& Enterprise Services

Security Services Standard

Introduction

Oklahoma Cyber Command is responsible for protecting state users and their devices, networks, data and applications. Oklahoma Cyber Command's top priority is safeguarding the state's data and computer infrastructure against unauthorized data use, disclosure, modification, damage and loss. The OMES IS division supports Cyber Command's vision to provide leadership in the development, delivery and maintenance of cybersecurity, information security, risk management, enterprise fraud, physical security systems, compliance and privacy programs.

Purpose

This document defines the authority and services provided by Oklahoma Cyber Command.

Standard

Oklahoma Cyber Command is required to provide information security services to all state agencies, as defined in Title 62 O.S. §§ 34.11.1, including, but not limited to the following.

- Defensive services:
  - Endpoint management.
  - Virtual Desktop Infrastructure (VDI).
  - Endpoint Detection and Response (EDR).
  - Endpoint encryption.
  - Security assessment.
  - Secure Mail Gateway (SMG).
  - Secure Web Gateway (SWG).
  - Virtual Private Network (VPN).
  - Intrusion Prevention/Detection Systems (IPS/IDS).
  - Multi-Factor Authentication (MFA).
  - Privilege Access Management (PAM).
- Security education:
  - Security Education and Awareness Training (SEAT).
  - Simulated phishing campaigns.
- Offensive services:
  - Access control.
  - Threat intelligence collection, analysis, exploitation and production.
  - Forensics.
  - Investigations.
  - Threat assessments.
  - Threat monitoring and analysis.
  - Security Information and Event Management (SIEM).
  - Incident response.
  - Security assessment.
  - Facility Access Management Systems (FAMS).
  - Surveillance systems.
  - Physical Intrusion Detection Systems (IDS).
  - Facility project support.
  - Fraud prevention, detection, and investigation.
  - Third-party risk management.
  - Information sharing and analysis.

It is the responsibility of Oklahoma Cyber Command to interpret, design, implement and manage required regulatory controls. Staff performing similar functions within state agencies must collaborate and coordinate all activities with Oklahoma Cyber Command and defer interpretation of regulations and final decisions/solutions to Oklahoma Cyber Command. Through the Oklahoma Information Sharing and Analysis Center (OK-ISAC), Oklahoma Cyber Command maintains relationships and facilitates information sharing between regulatory bodies, including federal partners, industry oversight bodies and state/local law enforcement agencies to monitor cyber trends and help reduce the risk of cyber threats.

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

- Oklahoma OMES Cyber Command.
- OMES Unified but not Consolidated.

Revision history

This standard is subject to periodic review to ensure relevancy.

Effective date: 04/07/2022	**Review cycle:** Annual
Last revised: 08/25/2023	**Last reviewed:** 08/26/2024
Approved by: Joe McIntosh, Chief Information Officer	

ATTACHMENT D-1

OKLAHOMA
Office of Management
& Enterprise Services

Network Acceptable Use Standard

Introduction
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 the resources in an effective, ethical and lawful manner.

Purpose
This document defines acceptable network use for State of Oklahoma network resources.

Standard
Excessive or inappropriate use of the network and network resources may result in network access restriction, revocation of access privileges entirely or further sanctions.

Users of state information technology resources, specifically those using the state's network are authorized to use only network devices authorized by OMES. Prohibited devices include hubs, switches, repeaters, routers, network modems and wireless access points. These devices may be incorrectly configured or incompatible with the state network causing outages and reliability problems to all or part of the network.

Devices not approved for use on the network will be disabled and confiscated to ensure the stability and availability of the network.

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: 4/4/2022	**Review cycle:** Annual
Last revised: 10/18/2022	**Last Reviewed Date:** 09/21/2023
Approved by: Joe McIntosh, Chief Information Officer	

OKLAHOMA
Office of Management
& Enterprise Services

Removable Media Usage Standard

Introduction

Oklahoma Cyber Command is responsible for protecting state users, their managed devices, and connectivity to data and applications. Oklahoma Cyber Command's top priority is safeguarding the state's data and computer infrastructure against unauthorized data use, disclosure, modification, damage and loss.

Purpose

This document establishes acceptable use requirements for sharing, receiving or storing state data utilizing removable media devices.

Microsoft OneDrive is the preferred alternative to using any form of removable media device for sharing, receiving or storing state data. OneDrive for Business is provided to all state employees and contractors as the approved storage solution. OneDrive has been vetted for the protection of state data and users' privacy (Reference Workstation Data Storage Standard).

Definitions

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.

Standard

Oklahoma Cyber Command is required to provide information security services to all state agencies, as defined in Title 62 O.S. § 34.11.1, including establishment of data protection controls.

Unmanaged usage of removable media devices creates increased risk of sensitive data disclosure either inadvertently through loss or theft of the device or by purposeful data exfiltration. To assist in mitigating sensitive data disclosure risks, Oklahoma Cyber Command shall implement technological-based procedures to disallow regular usage of removable media devices not previously approved for use within our managed enterprise environment.

For a removable media device to receive regular usage approval:

- The device must be a state-owned asset. Personally owned devices shall not be utilized to share, receive or store state data.
- The device must be capable of hardware encryption that meets or exceeds applicable regulatory compliance requirements (generally FIPS 140-2, level 2 or 3 will cover the most stringent requirements).
- The device must internally contain and report an individual vendor/model/serial number which provides an inventory control mechanism.
- Vendor devices meeting this criterion are listed below. Please confer with Oklahoma Cyber Command for review and approval of comparable devices outside this list.
    - Secure Data.
    - Apricorn.
    - Data Locker.
    - Kanguru.

After each use-case for sharing, receiving or storing state data has been completed, data must be purged from the removable device in accordance with any and all applicable state and federal regulations.

Exceptions to removable media device regular usage approval must be requested with a documented business justification for CIO review.

It is the responsibility of Oklahoma Cyber Command to interpret, design, implement and manage required regulatory controls. Staff performing similar functions within state agencies must collaborate and coordinate all activities with Oklahoma Cyber Command and defer interpretation of regulations and final decisions/solutions to Oklahoma Cyber Command.

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

- Workstation Data Standard.
- Oklahoma State Statute, Title 62.
- National Institute of Standards and Technology.

Revision history

This standard is subject to periodic review to ensure relevancy.

Effective date: 06/04/2024	**Review cycle:** Annual
Last revised: 06/07/2024	**Last reviewed:** 09/19/2024
Approved by: Joe McIntosh, Chief Information Officer	

ATTACHMENT D-1

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.
- Employees have a responsibility to immediately report the theft, loss of or otherwise compromised personal devices to supervisors and Oklahoma Cyber Command.
    - Supervisors shall escalate as necessary depending on the sensitivity of state records accessed by the personal device.
- Employees may access, use or share state records via personal device only to the extent it is authorized and necessary to fulfill assigned job duties.
- 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.

ATTACHMENT D-1

The following are general security requirements for personal devices.

- All personal devices connecting to state information, accessing state data or state records must comply with state security policies and standards.
- 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	

APPENDIX A: REVISIONS

This document is to be reviewed at least once per fiscal year. If operational need or system/environmental changes require more frequent changes, these are permitted if the annual cadence does not drop below once per year.

Version Number	Change Request Number (if applicable)	Accepted Date	Author	Summary of Changes
2.0	N/A		Cyber Command	Document rewrite. Removed all sections not part of Information Security. Condensed summary information and provided links to published standard. Corrected formatting.

650 Castro St. Ste 120-387
Mountain View, CA 94041
www.upguard.com

Software-as-a-Service Schedule

This Software-as-a-Service Schedule ("**SAAS Schedule**") is a Contract document in connection with a contract awarded by the Office of Management and Enterprise Services on behalf of the State of Oklahoma.

In addition to other terms contained in an applicable Contract document, Supplier and State agree to the following terms governing the State's access and use of Supplier's software as a service platform.

NOW, THEREFORE, the parties hereby agree as follows:

1. DEFINITIONS

In addition to the terms defined elsewhere in the Contract, for all purposes of this SAAS Schedule, the following terms have the meanings set forth in this Section 1.

1.1. "**Authorized User**" means a Customer's employee or contractor who provides services to Customer such that access to the Services is required.

1.2. **"Customer"** means the entity receiving access to the SAAS contemplated under the Contract and this Schedule.

1.3. **"Company Data"** means Company's proprietary data and proprietary information provided to Customer in connection with Customer's use of the Services, including, without limitation, reports, evaluations and/or security scores regarding Monitored Organizations that are accessible through the Services.

1.4. **"Customer Data"** means Customer's proprietary data and proprietary information input into and/or stored by the Services or provided by Customer to Company in connection with the Services.

1.5. "**Documentation**" means the then-current standard user documentation for the Services that Company makes generally available to its customers at https://help.upguard.com/en/.

1.6. "**Intellectual Property Rights**" means patent rights (including, without limitation, patent applications and disclosures), copyrights, trademarks, trade secrets, moral rights, know-how, and any other intellectual property rights recognized in any country or jurisdiction in the world.

1.7. "**Maintenance Services**" means the maintenance and support services for the Services described in this Schedule.

1.8. "**Monitored Organization**" means any organization tracked or monitored by the Services.

1.9. "**Order Form**" means the document on which Customer orders access to the Services.

1.10. **"Reseller"** means a third-party entity that sells the Services directly to Customer.

1.11. **"Software as a Service"** or **"SAAS"** means the subscription-based, cloud-hosted, on-demand software offered on a one-to-many basis, and includes any and all applications, documentation, information, reports, output, assessments or related products arising from or related to the SAAS and provided by Supplier under this Schedule and as further described in an applicable Order Form.

1.12. "**Software**" means any Company or third-party software used by Company to provide the SAAS.

1.13. **"State"** means the government of the state of Oklahoma, it's employees and authorized representatives, including without limitation any department, agency or other unit of the government of the state of Oklahoma.

1.14. **"Supplier"** or "**Company"** means UpGuard, Inc. For the avoidance of doubt, any reference to "Company" in this Schedule or associated documentation shall be deemed a reference to Supplier.

1.15. **"Usage Data"** means data regarding usage of the SAAS collected by or provided to Company, including, without limitation, log data, Monitored Organization counts, number of accounts, login credentials, and usage statistics collected by the SAAS or otherwise provided by Customer and/or Authorized Users to the Company relating to the SAAS.

2. ACCESS TO SOFTWARE-AS-A-SERVICE

2.1. Right to Use. Subject to Customer's compliance with the terms and conditions of the Contract(including, without limitation, payment of the applicable Fees), commencing on the start date set forth in the Order Form and continuing for the Term, Company grants Customer a non-exclusive right to access the SAAS as further specified in the executed Order Form, solely for Customer's internal business purposes and limited to the number of Authorized Users and Monitored Organizations set out in the Order Form, as applicable.

2.2. Restrictions. Customer shall not attempt to interfere with or disrupt the SAAS or the Software or attempt to gain access to any systems or networks that connect thereto (except as required to access and use the SAAS). Customer shall not allow access to or use of the SAAS by anyone other than Authorized Users. Customer will not and will not allow any Authorized Users to: (a) copy or modify any portion of the SAAS or the Software, (b) distribute, transfer, sublicense, lease, lend or rent any portion of the SAAS or the Software to any third party, (c) use or deploy the SAAS on any Monitored Organization in excess of those for which the Customer has paid the relevant Fees, (d) alter or remove any proprietary notices in the SAAS or the Software, (e) use the SAAS or Software for any unlawful purpose or in a manner to adversely affects the availability of the SAAS or the Software or in contradiction of the Documentation or (f) with regards to any testing conducted on the SAAS, disclose to any third party or publish the results of such testing. Customer acknowledges and agrees that portions of the SAAS and the Software constitute or contain trade secrets of Company and its licensors. Accordingly, Customer agrees not to disassemble, decompile or reverse engineer the SAAS or the Software, or permit or authorize a third party to do so, except to the extent such restrictions are prohibited by applicable law.

2.3. Limited Rights. Customer's rights in the SAAS will be limited to access expressly granted in **Section 2.1** of this Schedule. Company reserves all rights and licenses in and to the SAAS not expressly granted to Customer under this Schedule.

2.4. Maintenance Services**.** Company will provide Customer with the Maintenance Services described in **Section 7 below** in accordance with the terms of this Schedule.

2.5. Company APIs**.** Company may, from time to time, provide access to certain of Company's APIs to enable dynamic access to the SAAS. Subject to Customer's compliance with the terms and conditions of this Schedule and the Documentation, to the extent Company makes access to such APIs (the "**Company APIs**") available to Customer, Company hereby grants to Customer during the Subscription Term, a non-exclusive, non-transferrable, non-assignable, non-sublicensable license to use the APIs to enable dynamic access to the SAAS for Customer internal purposes only and for no other purposes. To the extent Company grants such license, the Company APIs will be deemed to be "Software" for the purposes of **Section 2.2** only, and notwithstanding anything to the contrary in this Schedule, the Company APIs are provided on an as-is basis, and Company may revoke the license granted under this Section at any time. Customer's rights in the Company APIs will be limited to access expressly granted in **Section 2.5** of this Schedule. Company reserves all rights and licenses in and to the Company APIs not expressly granted to Customer under this Schedule.

3. CUSTOMER OBLIGATIONS

3.1. Cooperation and Assistance. As a condition to Company's obligations contained in this Schedule, Customer shall at all times: (a) provide Company with good faith cooperation and assistance and make available such information, and personnel as may be reasonably required by Company in order to provide the SAAS and Maintenance Services; (b) provide such personnel assistance and other Customer personnel, as may be reasonably requested by Company from time to time; and (c) carry out in a timely manner all other Customer responsibilities set forth in this Schedule.

3.2. Enforcement. Customer shall ensure that all Authorized Users comply with the terms and conditions of this Schedule. Customer shall promptly notify Company of any suspected or alleged violation of the terms and conditions of this Schedule and shall cooperate with Company with respect to: (a) investigation by Company of any suspected or alleged violation of this Schedule and (b) any action by Company to enforce the terms and conditions of this Schedule. Company may suspend or terminate any Authorized User's access to the SAAS in the event that Company reasonably determines that such Authorized User has violated the terms and conditions of this Schedule. Customer will at all times be responsible for all actions taken by or on behalf of an Authorized User, whether such action was authorized by an Authorized User. Customer shall be liable for any violation of the terms and conditions of this Schedule by any Authorized User.

3.3. Telecommunications and Internet Services. Customer acknowledges and agrees that Customer's and its Authorized Users' use of the SAAS is dependent upon access to telecommunications and Internet services. Customer shall be solely responsible for acquiring and maintaining all telecommunications and Internet services and other hardware and software required to access and use the SAAS, including, without limitation, any and all costs, fees, expenses, and taxes of any kind related to the foregoing. Company shall not be responsible for any loss or corruption of data, lost communications, or any other loss or damage of any kind arising from any such telecommunications and Internet services.

4. ORDERS

4.1. Order Form. Each Customer may execute an Order Form(s) with Company to purchase access to the SAAS. Each Order Form shall describe the SAAS, the associated fees and the date on which Customer's access to the SAAS shall begin and the date on which such access shall end "the Subscription Term." No Order Form will be deemed accepted by Company unless and until Company accepts such Order Form in writing. Any terms and conditions contained in any Order Form that are inconsistent with or in addition to the terms and conditions of this Schedule or the Contract will be deemed stricken from such Order Form, unless expressly stated that such terms supersede this Schedule or the Contract.

4.2. Delivery. Company will deliver the SAAS to Customer by permitting Customer and its Authorized Users to access SAAS through delivery of login credentials.

5. CONFIDENTIALITY

5.1. Definition. "**Confidential Information**" means any business or technical information disclosed by one Party to the other Party that: (i) if disclosed in writing, may be marked "confidential" or "proprietary" at the time of disclosure; (ii) if disclosed orally, is identified as "confidential" or "proprietary" at the time of disclosure; or (iii) under the circumstances, a person exercising reasonable business judgment would understand or would have reason to believe the information to be confidential or proprietary. For clarity, (a) Customer Data is considered to be Confidential Information of Customer, and (b) Company Data and the SAAS are Company's Confidential Information. Nothing in this section shall limit or otherwise be construed to conflict with the Customer's obligations under the Oklahoma Open Records Act.

5.2. Exclusions. The obligations and restrictions set forth in **Section 5.3** will not apply to any information that: (i) is or becomes generally known to the public through no fault of or breach of this Schedule by the receiving Party; (ii) is rightfully known by the receiving Party at the time of disclosure; (iii) is independently developed by the receiving Party without use of the disclosing Party's Confidential Information; or (iv) the receiving Party rightfully obtains from a third party who has the right to disclose such information without breach of any confidentiality obligation to the disclosing Party.

5.3. Use and Nondisclosure. A receiving Party will not use the disclosing Party's Confidential Information except as necessary for the performance or enforcement of this Schedule and will not disclose such Confidential Information to any third party except to those of its employees and subcontractors who have a bona fide need to know such Confidential Information for the performance or enforcement of this Schedule; provided that each such employee and subcontractor is bound by a written agreement that contains use and disclosure restrictions consistent with the terms set forth in this Section. Each receiving Party will protect the disclosing Party's Confidential Information from unauthorized use and disclosure using efforts equivalent to the efforts that the receiving Party ordinarily uses with respect to its own confidential information and in no event less than a reasonable standard of care. The provisions of this **Section 5.3** will remain in effect during the term of the Contract and for a period of three (3) years after the expiration or termination of Contract, provided that, as to any Confidential Information that the Disclosing Party maintains as a trade secret, the Receiving Party's obligations under this **Section 5** will remain in effect for as long such Confidential Information remains a trade secret.

5.4. Permitted Disclosures. The provisions of this **Section 5** will not restrict either Party from disclosing Confidential Information pursuant to the order or requirement of a court, administrative agency, or other governmental body; provided that, if legally permissible, the Party required to make such a disclosure gives reasonable notice to the other Party to enable it to contest such order or requirement or limit the scope of such request. The Party responding to such an order or requirement will only disclose that information that is expressly required. Either Party may disclose the terms and conditions of this Schedule to such Party's advisors, accountants, attorneys, investors (and prospective investors), and prospective acquirers as have a reasonable need to know such information, before they may access such information, any such third parties are, either: (a) bound by a written agreement to keep such information confidential; or (b) subject to a professional obligation to maintain the confidentiality of such information.

5.5. Equitable Relief. Each Party acknowledges that a breach by the other Party of any confidentiality or proprietary rights provision of this Schedule may cause the non-breaching Party irreparable damage, for which the award of damages would not be adequate compensation. Consequently, the non-breaching Party may institute an action to enjoin the breaching Party from any and all acts in violation of those provisions, which remedy shall be cumulative and not exclusive, and a Party may seek the

entry of an injunction enjoining any breach or threatened breach of those provisions, in addition to any other relief to which the non-breaching Party may be entitled at law or in equity.

6. OWNERSHIP

6.1. SAAS, Maintenance Services, and Company Data. Subject to the rights granted to the Customer per clause 2.1, as between Company and Customer, the SAAS, Maintenance Services, Company Data, and all related Intellectual Property Rights, are and shall remain the exclusive property of Company or its licensors.

6.2. Customer Data. Company acknowledges that, as between Customer and Company, Customer owns all worldwide right, title and interest in and to all Customer Data and Company will not obtain any ownership rights in such data. Customer hereby grants to Company a royalty free, non-exclusive, revocable license during the Subscription Term to use the Customer Data (i) to provide the SAAS and Maintenance Services to Customer; and (ii) to improve the SAAS.

6.3. Usage Data. Customer acknowledges and agrees that Company may collect or receive Usage Data in connection with Customer's use of the SAAS and that such Usage Data is and will remain the sole and exclusive property of Company. Company may use the Usage Data for its business purposes, including, without limitation, to improve and market Company's products and services provided that such data is not distributed or otherwise conveyed to any third parties (except subcontractors) in a context that could reasonably identify Customer as its source. For clarity, Usage Data is not Customer Data.

6.4. Suggestions. Customer hereby grants to Company a royalty free, non-exclusive, irrevocable, worldwide license to use any suggestions, comments, feedback or the like that the Customer has provided to the Company relating to the SAAS for its business purposes.

7. MAINTENANCE SERVICES

7.1 Updates. Company will provide Customer with error corrections, bug fixes, patches and workarounds (collectively, "***Error Corrections***") and updates, modifications and other enhancements (collectively, "***Updates***") for the SAAS as generally made available by Company to its other customers of the SAAS at no additional cost. Company does not promise that it will provide any, or a certain minimum number of, Updates during the Subscription Term.

7.2 Help Desk Support. Company will provide help desk support via telephone, chat, and email. Help desk support consists of consultation in English with a qualified technician in regard to the proper use of the SAAS, the provision of Error Corrections for

reported operating problems in the SAAS, and remedial software maintenance as required to restore the SAAS to operability.

7.3 Support Levels Response Times

Error Severity Level	Expression	Description	Time for Company to Acknowledge
1	Blocker	In this class, the errors lead to a complete loss of the productive system. It is no longer possible to carry out tasks which should be carried out through the use of the SAAS.	Not to exceed 2 Hours
2	Critical	The production is significantly impaired or Company's performance is greatly reduced.	Not to exceed 6 hours
3	Major	The full use of the program functions is altered but alternative possibilities are available.	Not to exceed 12 hours
4	Minor	There are only slight or "cosmetic" problems but the SAAS' performance is not affected.	Not to exceed 2 business days

(a) The Parties may, on a case-by-case basis, agree in writing to a reasonable extension of the Support Level response times.

(b) Company will diagnose the issue and identify the severity level of any reported issues, and provide Customer a diagnosis of the applicable error.

(c) Company shall provide Customer regular updates of the nature and status of its efforts to correct (or, where, relevant, mitigate) any applicable errors.

8. WARRANTY

8.1. SAAS Warranty. Company warrants to the Customer that the SAAS will perform under normal use in all material respects with the Documentation. Company's sole obligation under the limited warranty set forth in this **Section 8.1** is to use its reasonable efforts to correct or replace any non-conforming SAAS or, at Company's sole discretion, to terminate the applicable Order Form and Company shall refund fees paid by Customer on a pro-rata basis from the date of termination of the SAAS.

8.2. Exclusions. The warranties under **Section 8.1** do not apply to any: (a) use of the SAAS not in accordance with this Schedule, including Customer operation or use of the SAAS other than in accordance with applicable Documentation; (b) modification, damage, misuse or other unauthorized action of Customer or any third-party or; (c) combination of the SAAS with any goods, services or other items provided by Customer or any third party.

8.3. Disclaimer. EXCEPT AS EXPRESSLY PROVIDED IN **SECTION 8.1**, COMPANY MAKES NO REPRESENTATIONS OR WARRANTIES OF ANY KIND WHATSOEVER, EXPRESS OR IMPLIED, IN CONNECTION WITH THIS SCHEDULE OR THE SAAS. WITHOUT LIMITING THE FOREGOING, EXCEPT AS EXPRESSLY PROVIDED IN **SECTION 8.1**, COMPANY DISCLAIMS ANY WARRANTY THAT THE SAAS WILL BE ERROR FREE OR UNINTERRUPTED OR THAT ALL ERRORS WILL BE CORRECTED. COMPANY FURTHER DISCLAIMS ANY AND ALL WARRANTIES WITH RESPECT TO SAAS AS TO MERCHANTABILITY, ACCURACY OF ANY INFORMATION PROVIDED, FITNESS FOR A PARTICULAR PURPOSE, OR NON-INFRINGEMENT. COMPANY FURTHER DISCLAIMS ANY AND ALL WARRANTIES ARISING FROM COURSE OF DEALING OR USAGE OF TRADE. NO ADVICE OR INFORMATION, WHETHER ORAL OR WRITTEN, OBTAINED FROM COMPANY OR ELSEWHERE SHALL CREATE ANY WARRANTY NOT EXPRESSLY STATED IN THIS SCHEDULE.

9. GENERAL

9.1. Survival. The rights and obligations of Company and Customer contained in **Sections 4** (Orders), **5** (Confidentiality), **6** (Ownership), and **9** (General) shall survive any expiration or termination of this Schedule.

9.2. Waiver. The waiver by either Party of any default or breach of this Schedule shall not constitute a waiver of any other or subsequent default or breach.

9.3. Severability. In the event any provision of this Schedule is held to be invalid or unenforceable, the remaining provisions of this Schedule shall remain in full force and effect.

9.4. Compliance with Laws. Each Party agrees to comply with all applicable laws and regulations with respect to its activities hereunder, including, but not limited to, any export laws and regulations of the United States.

9.5. Headings. The headings in this Schedule are for the convenience of reference only and have no legal effect.

(Signatures on following page.)

650 Castro St. Ste 120-387
Mountain View, CA 94041
www.upguard.com

In Witness Whereof, the Parties have caused this Schedule to be signed by their duly authorized representatives.

COMPANY: UPGUARD, INC.	**CUSTOMER:**
Signature: Casey Altieri (Feb 13, 2025 17:59 EST)	Signature: Dan Cronin (Feb 14, 2025 11:39 CST)
Name: Casey Altieri	Name: Dan Cronin
Title: SVP of Sales Americas	Title: Chief Information Officer
Date: Feb 13, 2025	Date: Feb 14, 2025

EXHIBIT 02 - PRICING

Company Name:

State of Oklahoma - Third Party Risk Management System

System Component	Description	Unit of Measure	List Price	% off List	Oklahoma Cost
Vendor Risk: Corporate	**Third Party Risk**	**Attack surface management**	**$89,999.00**	**20%**	**$72,000.00**
Vendor Risk: Enterprise	**Third Party Risk**	**Attack surface management**	**$139,999.00**	**20%**	**$112,000.00**
Vendor Risk: Enterprise +	**Third Party Risk**	**Attack surface management**	**$209,999.00**	**20%**	**$168,000.00**
Maintenance and Support	Year 2	Year 3	**Year 4**		

Pricing should have definitions to fully describe what is included - including minimum orders and volume discounts.
Prices must remain firm for the duration of the term of the PO/contract.
Hourly costs are to be Not To Exceed (NTE) pricing.

UpGuard

UpGuard Corporate Plan for State of Oklahoma

Prepared For:

Dustin Gregory

dustin.gregory@omes.ok.gov

State of Oklahoma

Prepared By:

Mike Moore

mike.moore@upguard.com

UpGuard

Date Issued	Expiry Date	Order Number
Feb 7, 2025	Feb 15, 2025	ORD-F5ZGDBD

Bill to	Ship to
State of Oklahoma Attn: Dustin Gregory Address : 6501 Broadway Extension Oklahoma City OK United States 73116	State of Oklahoma Attn: Dustin Gregory Address : 6501 Broadway Extension Oklahoma City OK United States 73116

Contract Terms

Start Date	End Date	Billing Frequency	Payment Method	Payment Term
Feb 18, 2025	Feb 17, 2026	Yearly	Invoice	Net 30 Days

ATTACHMENT E-3

SKU	Name	Price (USD)	QTY	Discount	Subtotal
UGC-23	UpGuard Corporate	$89,999.00	1	$17,999.00	$72,000.00
				Total (USD)	$72,000.00

PLAN INCLUSIONS

UpGuard Corporate:

Attack surface management

- Unlimited domains for your organization
- Executive reporting
- First-party security rating
- Risk profile
- Internal risk remediation workflows and risk waivers
- External facing vulnerability scanning
- Identity breach detection
- Infostealer domain monitoring (1 domain)
- Typosquatting protection
- Data leak detection (25 keywords)

Third-party risk management (500 vendors)

- Executive reporting
- Vendor security ratings
- Portfolio risk profile
- Vendor risk profiles
- Vendor external facing vulnerability scanning
- Remediation workflows
- Unlimited security questionnaires, access to security questionnaire library and questionnaire builder
- Risk assessment workflows and additional evidence
- Concentration risk monitoring
- Co-branding

25 vendor snapshots, 10 users and standard support

Audit log, templates, and scheduled reports

SSO and API access

UpGuard Signature: Casey Altieri
Casey Altieri (Feb 13, 2025 17:59 EST)

Date: Feb 13, 2025

Customer Signature: Dan Cronin
Dan Cronin (Feb 14, 2025 11:39 CST)

Date: Feb 14, 2025

Print Name Dan Cronin

Remittance Information	Details
Bank Account Name	UpGuard Inc
Bank Name	JPMorgan Chase Bank, N.A.
Remittance Email	finance@upguard.com
ABA/Routing - US ACH/Direct Deposit	322271627
ABA/Routing - Wire	021000021
Account Number	932821579
SWIFT ID	CHASUS33
Bank/Branch	270 Park Ave., New York, NY 10017
Bank Country	USA
CURRENCY	USD
Remittance Address	PO Box 738226, Dallas, TX, 753738226, USA

Remittance Contact	Details
Contact	Maripet Macabantad
Phone Number	+1 (650) 437-7389
Email	finance@upguard.com

TERMS AND CONDITIONS

License Terms Apply

The products listed in this Order Form are licensed subject to UpGuard's Hosted Services Agreement unless an agreement mutually acceptable to both parties has been executed by the authorised representatives of the Customer and UpGuard ("HSA").

Regardless of the above, no terms, provisions or conditions of any purchase order, or terms and conditions of purchase, will have any impact on the obligations of the parties under the HSA, or otherwise modify the terms of the HSA. For the avoidance of doubt, the HSA will supersede and exclude any terms and conditions found on the Customer's Purchase Order.

Order Form, Pricing and Scope of Offer

Pricing and terms included in this Order Form is an offer for the product quantities and term specified in this Order Form only. Nothing in this Order Form will impact pricing for previously purchased Services and/or any renewals. The price for individual items, and/or quantities different from those contained in this Order Form may vary.

*If this Order Form is executed (or a Purchase Order, which must reference the Order Form, is accepted by UpGuard) after the Start Date, the Start Date shall be deemed to be the business day following such execution or acceptance.

Fees

Customer will pay all fees specified in the Order Form. Except as otherwise set forth in the HSA, or as otherwise specified herein: i)payment obligations are non-cancelable, fees paid are non-refundable, and (ii) quantities purchased cannot be decreased during the relevant subscription term.

Payments that are not made via ACH or Wire in accordance with the remittance information provided above may be subject to additional processing fees.

Users

Unless expressly noted otherwise, the number of "users" specified in the Order Form refers to users with "Administrator" or "Standard" roles described here. Additional Administrator or Standard users may be purchased for an additional cost.

Delivery Obligations

Customer agrees that purchases under this order are not contingent on the delivery of any future functionality or features, and are not dependent on any oral or written comments made by UpGuard regarding future functionality or features.

Shipping Terms

FCA Origin. Electronic delivery.

Taxes

Unless taxes are expressly stated as a line item in this Order Form, all Fees payable under this Agreement are net amounts payable in full, without deduction for taxes or duties of any kind. Customer will be responsible for, and will promptly pay, all taxes and duties of any kind (including but not limited to sales, use and withholding taxes) associated with this Order Form and Customer's receipt or use of the Services and Maintenance Services. In the event that Company or Reseller is required to collect any tax for which Customer is responsible, Customer will pay such tax directly to Company or Reseller. If Customer pays any withholding taxes that are required to be paid under applicable law, Customer will furnish Company or Reseller with written documentation of all such tax payments, including receipts.

The Customer obligation does not include Corporate Income Tax, Payroll Tax, and other State Franchise Tax due in the normal course of business by UpGuard.

Amendments

The Order Form states UpGuard's entire commitment to Customer with regard to the services described and may only be modified by written amendment signed by an authorized representative of both parties.