STATE OF OKLAHOMA STATEWIDE CONTRACT WITH GL SUITE, INC. DBA GL SOLUTIONS

This State of Oklahoma Statewide Contract #1041 - Software Value Added Reseller is entered into between the State of Oklahoma by and through the Office of Management and Enterprise Services and GL Suite, Inc. dba GL Solutions ("Supplier") and is effective as of the date of last signature to this Contract. The initial Contract term shall be one (1) year, beginning on the date of last signature ("Effective Date") of the Contract, and there will be four (4) one-year options to renew.

Purpose

The State is awarding this Contract to Supplier as a statewide contract on behalf of the Office of Management and Enterprise Services for software and services to support State agencies and other eligible Oklahoma Interlocal Entities. The Supplier will provide software, training, pre-sales assistance, documentation, installation, maintenance, support, configuration, customization, and license agreement administration. This bid supports both SaaS Cloud Based Solutions and On-Prem Software Solutions, as more particularly described in certain Contract Documents. Supplier submitted additional terms and Supplier requested confidential matters to be considered. This Contract memorializes the agreement of the parties with respect to the 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 EVENT NO. 00000640, Attachment A;
   2.2. General Terms, Attachment B;
   2.3. Statewide Contract Terms, Attachment C;
   2.4. Information Technology Terms, Attachment D;
   2.5. Portions of the Bid, Attachment E
   2.6. GL Suite Software Agreement, Attachment E-1;
   2.7. End User License Agreement, Attachment E-2;
   2.8. Pricing, Attachment E-3;
   2.9. Value Add, Attachment E-4

2.10. NA, Attachment E-5; and
2.11. Template Statement of Work, Attachment E-6.

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 a 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. In the event of any conflict in terms, or inconsistencies, between Attachment E-1 through E-6, and the States terms in Attachments A-D, the State's terms in Attachments A-D shall Prevail. The State does not agree to any additional duties, obligations, or liabilities, other than the negotiated exceptions.

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

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

[REMAINDER OF PAGE LEFT INTENTIONALLY BLANK]

Signatures

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

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

By: Dan Cronin (Oct 23, 2025 06:55:38 EDT)

Name: Dan Cronin

Title: Chief Information Officer/Chief Transformation Officer

Date: Oct 23, 2025

GL SUITE, INC. DBA GL SOLUTIONS

By: William S Mosley (Oct 22, 2025 15:03:02 MDT)

Name: William S Mosley

Title: CEO

Date: Oct 22, 2025

ATTACHMENT A

SW1041 Software Value Added Reseller

EVENT NO. 00000640

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

PURPOSE

The Contract is awarded as a statewide contract on behalf of the Office of Management and Enterprise Services for software and services to support State agencies and other eligible Oklahoma Interlocal Entities. The Supplier will provide software, training, pre-sales assistance, documentation, installation, maintenance, support, configuration, customization, and license agreement administration. This bid supports both SaaS Cloud Based Solutions and On-Prem Software Solutions.

1. Contract Term and Renewal Options

The initial Contract term, which begins on the effective date of the Contract and there will be four (4) annual renewals remaining.

This RFP is a supplemental solicitation to Solicitation 0900000176 to add additional suppliers within scope. **If your company already holds an award under SW1041 you do not need to respond to this solicitation.**

ATTACHMENT B

STATE OF OKLAHOMA GENERAL TERMS

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

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

1 Scope and Contract Renewal

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

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

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

1.4 The State may extend the Contract for ninety (90) days beyond a final renewal term at the Contract compensation rate for the extended period. If the State

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

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

2 Contract Effectiveness and Order of Priority

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

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

A. any Addendum;

B. any applicable Solicitation;

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

D. the terms contained in this Contract Document;

E. any successful Bid as may be amended through negotiation and to the extent the Bid does not otherwise conflict with the Solicitation or applicable law;

F. any statement of work, work order, or other similar ordering document as applicable; and

G. other mutually agreed Contract Documents.

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

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

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

3 Modification of Contract Terms and Contract Documents

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

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

4 Definitions

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

4.1 **Acquisition** means items, products, materials, supplies, services and equipment acquired by purchase, lease purchase, lease with option to purchase, value provided or rental under the Contract.

4.2 **Addendum** means a mutually executed, written modification to a Contract Document.

4.3 **Amendment** means a written change, addition, correction or revision to the Solicitation.

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

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

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

4.7 **Contract Document** means this document; any master or enterprise agreement terms entered into between the parties that are mutually agreed to be applicable to the Contract; any Solicitation; any Contract-specific terms; any Supplier's Bid as may be negotiated; any statement of work, work order, or other similar mutually executed ordering document; other mutually executed documents and any Addendum.

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

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

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

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

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

4.13 **Moral Rights** means any and all rights of paternity or integrity of the Work Product and the right to object to any modification, translation or use of the Work Product and any similar rights existing under the judicial or statutory law of any country in the world or under any treaty, regardless of whether or not such right is denominated or referred to as a moral right.

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

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

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

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

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

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

4.20 **Supplier Confidential Information** means certain confidential and proprietary information of Supplier that is clearly marked as confidential and agreed by the State Purchasing Director or Customer, as applicable, but does not include information excluded from confidentiality in provisions of the Contract or the Oklahoma Open Records Act.

4.21 **Work Product** means any and all deliverables produced by Supplier under a statement of work or similar Contract Document issued pursuant to this Contract, including any and all tangible or intangible items or things that have been or will be prepared, created, developed, invented or conceived at any time following the Contract effective date including but not limited to any (i) works of authorship (such as manuals, instructions, printed material, graphics, artwork, images, illustrations, photographs, computer programs, computer software, scripts, object code, source code or other programming code, HTML code, flow charts, notes, outlines, lists, compilations, manuscripts, writings, pictorial materials, schematics, formulae, processes, algorithms, data, information, multimedia files, text web pages or web sites, other written or machine readable expression of such works fixed in any tangible media, and all other copyrightable works), (ii) trademarks, service marks, trade dress, trade names, logos, or other indicia of source or origin, (iii) ideas, designs, concepts, personality rights, methods, processes, techniques, apparatuses, inventions, formulas, discoveries, or improvements, including any patents, trade secrets and know-how, (iv) domain names, (v) any copies, and similar or derivative works to any of the foregoing, (vi) all documentation and materials related to any of the foregoing, (vii) all other goods, services or deliverables to be provided by or on behalf of Supplier under the Contract and (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.

5 Pricing

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

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

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

6 Ordering, Inspection, and Acceptance

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

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

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

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

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

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

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

7 Invoices and Payment

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

The following terms additionally apply:

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

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

C. Payment of all fees under the Contract shall be due NET 45 days. Payment and interest on late payments are governed by 62 O.S. §34.72. Such interest is the sole and exclusive remedy for late payments by a State agency and no other late fees are authorized to be assessed pursuant to Oklahoma law.

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

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

F. Supplier shall have no right of setoff.

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

H. The Supplier shall accept payment by Purchase Card as allowed by Oklahoma law.

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

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

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

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

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

B. Commercial General Liability Insurance covering the risks of personal injury, bodily injury (including death) and property damage, including coverage for contractual liability, with a limit of liability of not less than $5,000,000 per occurrence;

C. Automobile Liability Insurance with limits of liability of not less than $5,000,000 combined single limit each accident;

D. Directors and Officers Insurance which shall include Employment Practices Liability as well as Consultant's Computer Errors and Omissions Coverage, if information technology services are provided under the Contract, with limits not less than $5,000,000 per occurrence;

E. Security and Privacy Liability insurance, including coverage for failure to protect confidential information and failure of the security of Supplier's computer systems that results in unauthorized access to Customer data with limits $5,000,000 per occurrence; and

F. Additional coverage required in writing in connection with a particular Acquisition.

8.2 Supplier shall be entirely responsible during the existence of the Contract for the liability and payment of taxes payable by or assessed to Supplier or its employees, agents and subcontractors of whatever kind, in connection with the Contract. Supplier further agrees to comply with all state and federal laws applicable to any such persons, including laws regarding wages, taxes, insurance, and Workers' Compensation. Neither Customer nor the State shall be liable to the Supplier, its employees, agents, or others for the payment of taxes or the provision of unemployment insurance and/or Workers' Compensation or any benefit available to a State or Customer employee.

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

9 Compliance with Applicable Laws

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

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

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

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

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

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

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

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

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

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

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

9.2 The Supplier's employees, agents and subcontractors shall adhere to applicable Customer policies including, but not limited to acceptable use of Internet and electronic mail, facility and data security, press releases, and public relations. As applicable, the Supplier shall adhere to the State Information Security Policy, Procedures, Guidelines set forth at https://omes.ok.gov/sites/g/files/gmc316/f/InfoSecPPG_0.pdf. Supplier is responsible for reviewing and relaying such policies covering the above to the Supplier's employees, agents and subcontractors.

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

9.4 In addition to compliance under subsection 9.1 above, Supplier shall have a continuing obligation to comply with applicable Customer-specific mandatory

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

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

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

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

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

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

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

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

10 Audits and Records Clause

10.1 As used in this clause and pursuant to 67 O.S. §203, "record" includes a document, book, paper, photograph, microfilm, computer tape, disk, record, sound recording, film recording, video record, accounting procedures and practices, and other data, regardless of type and regardless of whether such items are in written form, in the form of computer data, or in any other form. Supplier agrees any pertinent federal or State agency or governing entity of a Customer shall have the right to examine and audit, at no additional cost to a Customer, all records relevant to the execution and performance of the Contract except, unless otherwise agreed, costs of Supplier that comprise pricing under the Contract.

10.2 The Supplier is required to retain records relative to the Contract for the duration of the Contract and for a period of seven (7) years following completion or termination of an Acquisition unless otherwise indicated in the Contract terms. If a claim, audit, litigation or other action involving such records is started before the end of the seven-year period, the records are required to be maintained for two (2) years from the date that all issues arising out of the action are resolved, or until the end of the seven (7) year retention period, whichever is later.

10.3 Pursuant to 74 O.S. §85.41, if professional services are provided hereunder, all items of the Supplier that relate to the professional services are subject to examination by the State agency, State Auditor and Inspector and the State Purchasing Director.

11 Confidentiality

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

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

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

11.3 Supplier shall immediately report to the Customer any and all unauthorized use, appropriation, sale, assignment, conveyance, provision, release, access, acquisition, disclosure or other dissemination of any State or citizen data or records of which it or its parent company, subsidiaries, affiliates, employees, officers, directors, assignees, agents, representatives, independent contractors, and subcontractors is aware or have knowledge or reasonable should have knowledge. The Supplier shall also promptly furnish to Customer full details of the unauthorized use, appropriation, sale, assignment, conveyance, provision, release, access, acquisition, disclosure or other dissemination, or attempt thereof, and use its best efforts to assist the Customer in investigating or preventing the reoccurrence of such event in the future. The Supplier shall cooperate with the Customer in connection with any litigation and investigation deemed necessary by the Customer to protect any State or citizen data and records and shall bear all costs associated with the investigation, response and recovery in connection with any breach of State or citizen data or records including but not limited to credit monitoring services with a term of at least three (3) years, all notice-related costs and toll free telephone call center services.

11.4 Supplier further agrees to promptly prevent a reoccurrence of any unauthorized use, appropriation, sale, assignment, conveyance, provision, release, access, acquisition, disclosure or other dissemination of State or citizen data and records.

11.5 Supplier acknowledges that any improper use, appropriation, sale, assignment, conveyance, provision, release, access, acquisition, disclosure or other dissemination of any State data or records to others may cause immediate and irreparable harm to the Customer and certain beneficiaries and may violate state or federal laws and regulations. If the Supplier or its affiliates, parent company, subsidiaries, employees, officers, directors, assignees, agents,

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

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

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

12 Conflict of Interest

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

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

13 Assignment and Permitted Subcontractors

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

13.2 Notwithstanding the foregoing, the Contract may be assigned by Supplier to any corporation or other entity in connection with a merger, consolidation, sale of all equity interests of the Supplier, or a sale of all or substantially all of the assets of the Supplier to which the Contract relates. In any such case, said corporation or other entity shall by operation of law or expressly in writing assume all obligations of the Supplier as fully as if it had been originally made a party to the Contract. Supplier shall give the State and all affected Customers prior written notice of said assignment. Any assignment or delegation in violation of this subsection shall be void.

13.3 If the Supplier is permitted to utilize subcontractors in support of the Contract, the Supplier shall remain solely responsible for its obligations under the terms of the Contract, for its actions and omissions and those of its agents, employees and subcontractors and for payments to such persons or entities. Prior to a subcontractor being utilized by the Supplier, the Supplier shall obtain written approval of the State of such subcontractor and each employee, as applicable to a particular Acquisition, of such subcontractor proposed for use by the Supplier. Such approval is within the sole discretion of the State. Any proposed subcontractor shall be identified by entity name, and by employee name, if required by the particular Acquisition, in the applicable proposal and shall include the nature of the services to be performed. As part of the approval request, the Supplier shall provide a copy of a written agreement executed by the Supplier and subcontractor setting forth that such subcontractor is bound by and agrees, as applicable, to perform the same covenants and be subject to

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

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

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

14 Background Checks and Criminal History Investigations

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

15 Patents and Copyrights

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

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

16 Indemnification

16.1 Acts or Omissions

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

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

16.2 Infringement

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

16.3 Notice and Cooperation

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

16.4 Coordination of Defense

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

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

16.5 Limitation of Liability

A. With respect to any claim or cause of action arising under or related to the Contract, neither the State nor any Customer shall be liable to Supplier for lost profits, lost sales or business expenditures, investments, or commitments in connection with any business, loss of any goodwill, or for any other indirect, incidental, punitive, special or consequential damages, even if advised of the possibility of such damages.

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

C. The limitation of liability and disclaimers set forth in the Contract will apply regardless of whether Customer has accepted a product or service. The parties agree that Supplier has set its fees and entered into the Contract in reliance on the disclaimers and limitations set forth herein, that the same reflect an allocation of risk between the parties and form an essential basis of the bargain between the parties. These limitations shall apply notwithstanding any failure of essential purpose of any limited remedy.

17 Termination for Funding Insufficiency

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

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

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

18 Termination for Cause

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

18.2 The State may terminate the Contract in whole or in part immediately without a thirty (30) day written notice to Supplier if (i) Supplier fails to comply with confidentiality, privacy, security, environmental or safety requirements applicable to Supplier’s performance or obligations under the Contract; (ii) Supplier’s material breach is reasonably determined to be an impediment to the function of the State and detrimental to the State or to cause a condition precluding the thirty (30) day notice or (iii) when the State determines that an administrative error in connection with award of the Contract occurred prior to Contract performance.

18.3 Upon receipt of notice of a termination, Supplier shall immediately comply with the notice terms and take all necessary steps to minimize the incurrence

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

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

19 Termination for Convenience

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

19.2 Upon receipt of notice of such termination, Supplier shall immediately comply with the notice terms and take all necessary steps to minimize the incurrence of costs allocable to the work affected by the notice. If a purchase order or other payment mechanism has been issued and a product or service has been accepted as satisfactory prior to the effective date of termination, the termination does not relieve an obligation to pay for the product or service but

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

20 Suspension of Supplier

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

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

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

21 Certification Regarding Debarment, Suspension, and Other Responsibility Matters

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

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

22 Certification Regarding State Employees Prohibition From Fulfilling Services

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

23 Force Majeure

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

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

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

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

24 Security of Property and Personnel

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

25 Notices

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

If sent to the State:
State Purchasing Director
2401 North Lincoln Boulevard, Suite 116
Oklahoma City, Oklahoma 73105

With a copy, which shall not constitute notice, to:
Purchasing Division Deputy General Counsel
2401 North Lincoln Boulevard, Suite 116
Oklahoma City, Oklahoma 73105

26 Miscellaneous

26.1 Choice of Law and Venue

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

26.2 No Guarantee of Products or Services Required

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

26.3 Employment Relationship

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

26.4 Transition Services

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

26.5 Publicity

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

26.6 Open Records Act

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

26.7 Failure to Enforce

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

26.8 Mutual Responsibilities

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

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

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

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

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

26.9 Invalid Term or Condition

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

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

26.10 Severability

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

26.11 Section Headings

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

26.12 Sovereign Immunity

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

26.13 Survival

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

26.14 Entire Agreement

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

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

26.15 Gratuities

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

26.16 Import/Export Controls

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

ATTACHMENT C

OKLAHOMA STATEWIDE CONTRACT TERMS

1. Statewide Contract Type

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

1.2 The Contract is a firm, fixed price contract for indefinite delivery and quantity for the Acquisitions available under the Contract.

2. Orders and Addendums

2.1 Unless mutually agreed in writing otherwise, orders shall be placed directly with the Supplier by issuance of written purchase orders or by Purchase Card by state agencies and other authorized entities. All orders are subject to the Contract terms and any order dated prior to Contract expiration shall be performed. Delivery to multiple destinations may be required.

2.2 Any ordering document shall be effective between Supplier and the Customer only and shall not be an Addendum to the Contract in its entirety or apply to any Acquisition by another Customer.

2.3 Additional terms added to a Contract Document by a Customer shall be effective if the additional terms do not conflict with the General Terms and are acceptable to Supplier. However, an Addendum to the Contract shall be signed by the State Purchasing Director or designee. Regarding information technology and telecommunications contracts, pursuant to 62 O.S., §34.11.1, the Chief Information Officer acts as the Information Technology and Telecommunications Purchasing Director.

3. Termination for Funding Insufficiency

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

4. Termination for Cause

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

5. Termination for Convenience

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

6. Contract Management Fee and Usage Report

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

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

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

6.3 All Contract Usage Reports shall meet the following criteria:

i. Electronic submission in Microsoft Excel format to **strategic.sourcing@omes.ok.gov**;

ii. Quarterly submission regardless of whether there were transactions under the Contract during the applicable quarterly reporting period;

iii. Submission no later than forty-five (45) days following the end of each calendar quarter;

iv. Contract quarterly reporting periods shall be as follows:

a. January 01 through March 31;

b. April 01 through June 30;

c. July 01 through September 30; and

d. October 01 through December 31.

v. Reports must include the following information:

a. Procuring entity;
b. Order date;

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

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

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

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

ATTACHMENT D

STATE OF OKLAHOMA INFORMATION TECHNOLOGY TERMS

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

1 DEFINITIONS

1.1 **Customer Data** means all data supplied by or on behalf of a Customer in connection with the Contract, excluding any confidential information of Supplier. 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 **Security Incident** means the attempted or successful unauthorized access, use, disclosure, modification, loss, theft, or destruction of information or interference with the Hosted environment used to perform the services.

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

1.9 **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.

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

2 TERMINATION OF MAINTENANCE AND SUPPORT SERVICES

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

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

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

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

3 COMPLIANCE AND ELECTRONIC AND INFORMATION TECHNOLOGY ACCESSIBILITY

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

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

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

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

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

5 OFFSHORE SERVICES

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

6 COMPLIANCE WITH TECHNOLOGY POLICIES

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

Supplier's employees and subcontractors shall adhere to the applicable State IT

Standards, policies, procedures and architectures as set forth at https://oklahoma.gov/omes/services/information-services.html or as otherwise provided by the State.

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

7 EMERGING TECHNOLOGIES

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

8 EXTENSION RIGHT

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

9 SOURCE CODE ESCROW

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

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

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

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

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

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

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

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

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

10 COMMERCIAL OFF THE SHELF SOFTWARE OR SUPPLIER TERMS

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

11 OWNERSHIP RIGHTS

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 therein, including but not limited to all source data, information and materials furnished to the State, together with all plans, system analysis, and design specifications and drawings, completed programs and documentation thereof, reports and listing, all data and test procedures and all other items pertaining to the work and services to be performed pursuant to this Contract including all copyright and proprietary rights relating thereto. With respect to Supplier Intellectual Property, the Supplier grants the State, for no additional consideration, a perpetual, irrevocable, royalty-free license, solely for the internal business use of the State, to use, copy, modify, display, perform, transmit and prepare derivative works of Supplier Intellectual Property embodied in or delivered to the State in conjunction with the products.

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

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

Supplier shall assist the State and its agents, upon request, in preparing U.S. and foreign copyright, trademark, and/or patent applications covering software developed, modified or customized for the State 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 WorkProduct 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 Hosting Customer Data or providing products or services pursuant to an Acquisition, contributes to, or directly causes a Data Breach or a Security Incident. Likewise, Supplier shall be responsible for the obligations set forth in in this Contract, including those obligations related to breach reporting and associated costs when a Supplier's affiliate or subcontractor contributes to, or directly causes a Data Breach or a Security Incident.

14 CHANGE MANAGEMENT

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

15 SERVICE LEVEL DEFICIENCY

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

16 OWNERSHIP OF IT AND TELECOMMUNICATION ASSETS

Notwithstanding any other provision in the Contract and pursuant to the Oklahoma Information Technology Consolidation and Coordination Act, all information technology and telecommunication assets and contracts on behalf of appropriated agencies of the State belong to OMES-IS. OMES-IS allows other State agencies to use the assets while retaining ownership and the right to reassign the assets, at no additional cost, upon written notification to Supplier.

17 CUSTOMER DATA

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

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

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

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

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

18 DATA SECURITY

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

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

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

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

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

18.6 Supplier shall allow the Customer to audit conformance to the Contract terms. The Customer may perform this audit or contract with a third party at its discretion and at Customer's expense.

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

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

19 SECURITY ASSESSMENT

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

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

20 SECURITY INCIDENT OR DATA BREACH NOTIFICATION

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

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

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

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

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

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

21 DATA BREACH NOTIFICATION AND RESPONSIBILITIES

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

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

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

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

22 SUPPLIER REPRESENTATIONS AND WARRANTIES

Supplier represents and warrants the following:

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

22.2 Supplier will protect Customer's Non-Public Data and Personal Data from unauthorized dissemination and use with the same degree of care that each such party uses to protect

its own confidential information and, in any event, will use no less than a reasonable degree of care in protecting such confidential information.

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

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

23 INDEMNITY

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

24 TERMINATION, EXPIRATION AND SUSPENSION OF SERVICE

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

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

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

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

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

c. a combination of the two immediately preceding options.

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

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

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

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

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

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

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

25 GENERAL INFORMATION SECURITY REQUIREMENTS

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

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

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

25.4 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

26 HIPAA REQUIREMENTS

26.1 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).

26.2 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.

26.3 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.

26.4 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

p. 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.

26.5 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. § 164.502(d)].

26.6 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.

26.7 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)-(iii) & 164.314 (a)(2)(i)(C).

26.8 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.

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

27.1 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 Agreement. Contractor accepts the responsibilities for providing adequate administrative supervision and training to their employees and agents to ensure

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

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

27.3 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. Contractor agrees that such protected information shall not be available or accessible to staff in general and shall not be used for punishment or prosecution of any kind;

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

27.5 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).

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

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

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

27.9 Agrees to make available its internal practices, books, and records, including policies and procedures, relating to the use and disclosure of protected information received from the

State of Oklahoma agency or created or received by the Contractor on behalf of the State of Oklahoma agency, to the State of Oklahoma agency and to the Secretary of the Department of Health and Human Services for purpose of the Secretary determining the giving party's compliance with HIPAA;

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

28 DATA SECURITY

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

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

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

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

29 FEDERAL TAX INFORMATION REQUIREMENTS IRS PUBLICATION 1075

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

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

29.3 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.

29.4 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.

29.5 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.

29.6 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.

29.7 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.

29.8 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.

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

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

29.11 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.

29.12 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.

29.13 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.

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

30 CRIMINAL/CIVIL SANCTIONS

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

30.2 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.

30.3 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.

30.4 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.

30.5 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.

31 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.

32 SSA REQUIREMENTS

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

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

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

32.4 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.

32.5 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.

32.6 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.

32.7 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.

32.8 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.

32.9 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.

32.10 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 Agreement, and thereafter at SSA's request, the applicable State of Oklahoma agency shall obtain from the Contractor a current list of the employees of such Contractor with access to SSA data and provide such list to the SSA.

32.11 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 Agreement.

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

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

32.14 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.

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

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

33 CRIMINAL/CIVIL SANCTIONS

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

33.1 Civil Remedies

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

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

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

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

33.2 Criminal Penalties

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

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

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

34 CHILD SUPPORT FPLS REQUIREMENTS

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

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

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

35 FERPA REQUIREMENTS

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

36 CJIS REQUIREMENTS

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

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

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

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

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

transmitted over the Oklahoma Law Enforcement Telecommunications System ("OLETS") which is operated by DPS.

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

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

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

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

37 NOTICES

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

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

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

Attachment E: Response to Specifications and Requirements

i The portion of the Bid to be inserted in this section shows the ability of the Bidder to meet or exceed any Acquisition specifications and requirements in Exhibit #2 Requirements

From Exhibit #2 Requirements:

C.1. Experience

Bidders must provide a brief written narrative describing experience as a Supplier for software products, cloud products and associated services for all areas that the Bidder is responding with. The narrative should be no longer than 2 pages in length.

Experience as a Supplier of Software Products, Cloud Products, and Associated Services

GL Solutions has a proven track record spanning 25 years in delivering reliable, secure, and scalable software solutions, particularly within the public sector. We specialize in providing cloud-based systems that streamline regulatory workflows, enhance compliance, and improve user experiences for both applicants and government staff.

Our flagship solution, GL Suite, has been successfully implemented across numerous state agencies, including regulatory bodies and departments responsible for licensing, inspections, and case management.

Our software products and services are designed with flexibility and scalability in mind, ensuring that agencies can adapt to evolving needs without the burden of custom coding. GL Suite, now in its seventh iteration, is a fully configurable platform that allows state agencies to automate manual processes and replace outdated systems with modern, integrated solutions. It provides seamless user access, mobile compatibility, and enhanced data security—all built on a secure cloud infrastructure.

Core Features & Services:

- **Cloud-based Solution:** GL Suite is hosted on industry-leading, secure platforms such as Microsoft Azure, ensuring high availability, redundancy, and end-to-end encryption.
- **Workflows & Automation:** Our robust business rules engine automates task routing and streamlines case management, reducing operational complexity and increasing efficiency.
- **Licensing & Compliance:** We automate license processing, track expirations, and send renewal alerts to ensure compliance across multiple regulatory domains.
- **Advanced Security:** With pending StateRAMP certification and features like Multi-Factor Authentication (MFA), Role-Based Access Control (RBAC), and compliance with major standards (FIPS, HIPAA, PCI-DSS), our platform ensures the highest level of security for sensitive government data.
- **Integration Capabilities:** GL Suite integrates seamlessly with third-party systems using standards like XML and JSON, ensuring smooth data exchange and operational continuity.

In addition to our software, GL Solutions offers comprehensive support throughout the implementation lifecycle, including training, system configuration, and post-deployment maintenance. We are committed to providing a solution that meets each agency's unique requirements while maintaining a focus on sustainability, data integrity, and user satisfaction.

Proven Success Across Multiple Domains: GL Solutions has worked with numerous state agencies to replace legacy systems with fully integrated case management, licensing, and workflow automation solutions. Our experience spans various sectors including gaming regulation, medical licensing, inspections, and financial oversight. The versatility of

GL Suite has been a key differentiator, allowing us to tailor our solutions to the specific needs of each client, regardless of the complexity of their operations.

Commitment to Quality and Innovation: We continuously invest in enhancing GL Suite's capabilities to meet the ever-changing demands of regulatory agencies. Our team's commitment to innovation and excellence ensures that our clients are always equipped with the best tools for their operational needs.

GL Solutions is excited about the opportunity to provide the State with a modern, secure, and highly configurable solution that will support regulatory objectives and improve service delivery for residents.

C.2. Renewal Process

Bidder must provide a brief written narrative describing the company's processes for renewal notifications. Please explain what is included in the services and what value-added services can be included.

GL Solutions follows a structured and proactive contract renewal process to ensure smooth and timely renewals. Our process is designed to minimize disruption and provide value-added services to support ongoing system use and enhancement.

Renewal Notification and Initiation:

- GL Solutions initiates contract renewal discussions only at the direction of the CEO.
- Renewal tasks are initiated five-months before the contract expiration date to allow adequate time for negotiation and planning.
- During regular client status meetings, GL Solutions gathers any new, key information, including:
    - Desired plan level and invoicing frequency.
    - Procurement, legal, and agency contacts (names, phone numbers, and emails).
    - A brief overview of the procurement steps required to execute the contract.

Client Engagement and Plan Adjustment:

- Clients are provided with detailed support plan options, including the benefits and costs of changing levels of service, scaling up or scaling down as required.
- GL Solutions discusses future goals, potential system improvements, and agency challenges to identify opportunities for added value.
- Strategic planning includes discussions about critical dates, legislative changes, and future projects to ensure alignment with agency priorities.

Wish List and Business Process Enhancements:

- GL Solutions Account Partners (APs) actively gather and document client feedback on desired new functionalities and business processes during regular client meetings.
- The "wish list" includes enhancements that can improve system efficiency and user experience.
- APs work with the client to prioritize and escalate wish list items, ensuring alignment with strategic goals.

E.g., if a client's inspection process is slowed by manual data entry, GL Solutions may recommend implementing mobile forms to improve efficiency.
- If a client frequently updates correspondence, GL Solutions may suggest the End User Training service to empower the client to manage updates more efficiently.
- GL Solutions incorporates these insights into future planning, identifying opportunities to integrate improvements into contract renewal discussions.

Ongoing Support and Payment Monitoring:

- GL Solutions reviews upcoming invoices and helps clients resolve any issues to prevent payment delays or service disruptions.
- Regular meetings are scheduled to maintain communication and address any new or evolving agency needs.

C.3. Performance and Escalation

Bidder must provide a brief written narrative describing the company's performance levels and outlining the escalation process.

The authorized Bidder shall meet customer service expectations, including but not limited to dedicated representation and timely response, problem escalation, providing service level performance standards, etc.

GL Solutions is committed to maintaining high performance and ensuring customer satisfaction through defined service levels and a structured escalation process. Our Service Level Agreement (SLA) outlines specific performance guarantees tailored to different service tiers, ensuring that our clients receive appropriate support based on their selected level of service.

Performance Levels: GL Suite offers three service tiers, each with its own uptime guarantee and performance standards:

- **Standard Tier:** 95% uptime guarantee
- **Professional Tier:** 99.9% uptime guarantee
- **Enterprise Tier:** 99.9% uptime guarantee

These performance levels ensure that GL Suite is highly reliable, with a clear framework for maintaining system performance. Our SLA includes scheduled maintenance windows, response times for addressing issues, and notification requirements for any planned system changes. We also incorporate several key performance safeguards:

- **Automated Monitoring and Incident Detection:** Our system is continuously monitored for performance, with automated alerts for any potential issues.
- **Security and Compliance:** GL Suite undergoes monthly vulnerability scans and quarterly penetration testing to identify and mitigate potential security risks.
- **Disaster Recovery:** Our solution includes a disaster recovery plan with defined recovery times ranging from 14 days to as little as 1 hour, depending on the service tier.

Escalation Process: GL Solutions follows a well-structured escalation process to ensure that issues are resolved promptly and efficiently. The escalation process includes:

1. **Initial Triage and Investigation:** Upon receiving an issue, our support team assesses the severity and begins troubleshooting immediately.
2. **Assignment of Appropriate Resources:** We assign the necessary resources based on the severity of the issue, ensuring that the right expertise is applied.
3. **Client Notification:** The client is notified at key points during the resolution process, keeping them informed of progress.
4. **Resolution or Workaround Implementation:** Our team works to resolve the issue or provide an immediate workaround to minimize impact.
5. **Follow-up:** After resolution, we follow up with the client to confirm that the issue has been fully addressed and that no further action is required.

Response Times Based on Service Tier:

- **Standard Tier:** 3-hour response
- **Professional Tier:** 1-hour response
- **Enterprise Tier:** 15-minute response

Our issues are tracked through the GL Portal, which enables automatic logging, monitoring, and resolution of incidents, ensuring full transparency and timely resolution.

Through these performance guarantees and the escalation process, GL Solutions ensures that client issues are addressed quickly and effectively, maintaining a high level of service and minimizing downtime.

Preferred Documentation

Any Bid should include, as applicable, hosting provisions, Service Level Agreements (SLA's), Billing Information, Documentation, Training, Account Team/Support Provision, Escalation Process and Pricing for each service. Such provisions, Statements of Work (SOW's), SLA's and other information are subject to negotiation and additional provisions related to hosting services and SLA's may be required prior to any award being issued.

• A Service Level Agreement (SLA) outlines the minimum service that a customer may expect for services, warranties and support. The SLA should include an example performance report and a matrix for service credits that relate to the Suppliers performance under the SLA.

- ***SLA Provided in Attachment A***
- ***SOW Provided in Attachment B***
- ***EULA Provided in Attachment C***
- ***VPAT Provided in Attachment D***
- ***DRP Provided in Attachment E***
- ***IRP Provided in Attachment F***

• Account Team and Support Provisions outline the Suppliers capabilities of providing world class support and account service.

Account Team and Support Provisions

GL Solutions provides a robust support structure to ensure seamless service and continuous system performance. We organize our support team with dedicated roles for specialized tasks:

- **Account Manager:** A dedicated account manager, who we call an Agency Partner (AP), ensures that all aspects of the client's needs are managed with personalized attention.
- **Technical Support Team:** Our team consists of highly qualified technical experts who handle troubleshooting, system configuration, and ongoing maintenance.
- **Help Desk Support:** We offer a **24/7 help desk** to address urgent issues, ensuring clients can reach out at any time for immediate assistance.

Expertise: Our support team comprises professionals with a strong technical background and extensive experience in system implementation and maintenance. The team includes certified professionals in relevant technologies and has a proven track record of working with similar clients, ensuring top-tier expertise in managing complex systems.

Communication and Issue Tracking: GL Solutions ensures a seamless one-stop communication, project management, payment, and task coordination center through our integrated communication management tool, **GL Portal**.

GL Portal is an all-in-one communications center that supports all interactions between authorized staff and GLS personnel. It enables stakeholders to:

- Approve tasks and projects
- Monitor task and project metrics
- Communicate directly with GLS personnel
- Submit issues and request enhancements
- Visually monitor project milestones and deadlines

Key features of GL Portal include:

- **Structured Tracking Process:** Our system provides a systematic approach for users to address issues and defects within the software, allowing them to easily view and monitor tasks, whether open or completed.
- **Power BI Dashboard:** The built-in Power BI dashboard offers administrators a comprehensive overview of system metrics, including the percentage of plans remaining and the number of open tasks/projects.
- **Issue Reporting and Monitoring:** Users can submit new issue reports, track the status of previously reported defects, and verify the resolution of completed items, ensuring transparency throughout the process.
- **Calendar Feature:** The GL Portal includes a calendar feature to track upcoming meetings with GLS, task and project deadlines, and overall schedule management.
- **Real-Time Communication:** Authorized users can communicate directly with GLS personnel, including the Project Manager during installation and the Agency Partner during maintenance and support.

Business Continuity

GL Solutions has robust Incident Response and Disaster Recovery Plans in place to ensure continuity of service even in the event of unforeseen disruptions. The IRP focuses on quick containment, eradication, and recovery from incidents, while the DRP provides a detailed framework for data recovery and system restoration, ensuring minimal impact on agency operations.

Availability and Uptime Requirements

GL Solutions guarantees a robust data protection strategy to ensure continuous system performance and reliability, supporting the States needs for high availability and disaster recovery. GL Suite, hosted by GL Solutions, includes comprehensive backup and recovery capabilities designed to minimize downtime and safeguard data integrity.

Backup and Data Protection

The GL Suite application creates nightly backups of all system data, encompassing the following key components:

- **Transactional Data**
- **Report Data**
- **Document Repository**
- **Correspondence Templates**
- **Reports**
- **Persisted Customizations**
- **Automated Database Jobs**
- **Interface Applications**
- **Files**

These backups are stored at an offsite location connected via a private network, with all data backed up every 24 hours. We maintain 21 days of backups to ensure historical recovery and regular monitoring of jobs and tasks to confirm the restorability of data, minimizing the risk of data loss.

In the event of hardware failure or a disaster, GL Solutions' infrastructure supports rapid recovery. Our system is designed with redundancy and failover mechanisms to ensure that data is restored within minutes, minimizing downtime and ensuring business continuity.

Data Protection Strategies

GL Solutions employs a variety of strategies to protect your data:

- **Off-site Data Replication**: Data is replicated to an off-site location, which minimizes the need for data restoration and allows for faster recovery of systems.
- **High Availability Systems**: Data and systems are continuously replicated off-site, ensuring uninterrupted access.
- **Wide Area Network Optimization**: This technology enhances disaster recovery capabilities by maintaining data movement even in case of network disruptions.

Azure Hosting and Disaster Recovery

When hosting with Azure, GL Solutions integrates Microsoft Data Protection Manager (DPM), a key tool for backup and recovery within our disaster recovery framework. Here's how DPM enhances our disaster recovery capabilities:

- **Data Backup and Recovery**: DPM automates regular backups of critical data, including databases, application configurations, and system states, storing them on disk, tape, or cloud (via Azure Backup). Multiple recovery points are created, allowing for rapid restoration of data in the event of data loss or corruption.
- **Granular Recovery**: DPM enables granular recovery down to the file or item level, ensuring quick rectification of smaller data losses without the need for full system restoration.

High Availability and Business Continuity

DPM supports high availability through:

- **Automated Failover**: If the primary system node fails, a backup node automatically takes over to maintain system operations.
- **Quick Recovery**: Leveraging incremental backups, DPM enables rapid data restoration, ensuring quick recovery times (RTO) and minimal data loss (RPO).

Cloud-Based Disaster Recovery

Incorporating Azure Site Recovery, DPM enables cloud-based disaster recovery by replicating critical systems and data in Azure. This integration ensures that in the event of a regional disaster or system failure, your data and systems are available for recovery, with geo-redundant storage ensuring off-site protection.

Monitoring and Alerts

Real-time monitoring and alerts are built into the DPM system to notify administrators of backup issues or replication failures, allowing for proactive issue resolution. This ensures data protection measures are continuously monitored for reliability and security.

Support for Various Workloads

DPM supports protection for a broad range of workloads, including:

- **SQL Server Databases**
- **File Systems**
- **Hyper-V Virtual Machines**
- **Exchange Servers**
- **SharePoint Data**

This integration of backup, disaster recovery and high availability measures within the Availability and Uptime Requirements section ensures that GL Solutions' offerings meet and exceed the needs of clients requiring robust data protection, minimizing the risk of data loss and ensuring service continuity.

With the appropriately selected GL Simple plan, GL Solutions guarantees an uptime of 99.9% for GL Suite, ensuring that the system is available 24/7/365 for both agency staff and customers. Our infrastructure is designed with

redundancy measures to ensure continuity and reliability, meeting the industry standard of 99.999% uptime. This

commitment ensures that state agencies and its users experience minimal downtime, even in the event of technical failures.

Our staff is always available during Department business hours to provide ongoing support and maintain service excellence. Additionally, agencies can contact GL Solutions 24/7/365 via phone, email, or GL Portal for any urgent issues or inquiries.

Our Incident Response Plan (IRP) and Disaster Recovery Plan (DRP) are integral to maintaining the availability and uptime guarantees. These plans ensure a rapid and coordinated response to any incidents or disruptions, minimizing downtime and ensuring business continuity.

Escalation Process: If issues are not resolved promptly, they are escalated to the appropriate level, ensuring that all concerns are addressed in a timely manner. Our structured tracking system allows authorized users to view and monitor tasks and projects, and if an issue is unresolved within the expected timeframe, it is escalated based on priority levels.

In the event of a critical incident, the **I**ncident Response Plan (IRP) is activated to ensure rapid mitigation and resolution. Our Disaster Recovery Plan (DRP) ensures that in the case of any system failure, recovery processes are swiftly executed to restore services within the specified downtime window."

Service Reviews: We monitor system performance closely and provide regular performance reviews with clients. GL Portal includes a built-in Power BI dashboard that offers a comprehensive overview of system metrics, such as the percentage of tasks completed and the number of open tasks/projects. This allows both clients and our team to review progress and ensure that all tasks are on track. Additionally, we schedule regular meetings to discuss ongoing service quality and system performance.

Customer Service Expectations

GL Solutions ensures consistent service through dedicated customer support and ongoing performance management:

- Dedicated account management for ongoing support and relationship management.
- 24/7 emergency support for Professional and Enterprise tiers.
- Defined service credits for failure to meet SLA targets.
- Continuous monitoring and logging of system performance and user activity to identify and resolve issues proactively.

Billing Information

GL Solutions provides flexible billing options tailored to meet the specific needs of each client. Billing frequency is determined based on the terms of the agreement and may vary by client, including:

- **Monthly billing** – Regular invoicing on a monthly cycle.
- **Milestone-based billing** – Payment issued upon successful completion of defined deliverables.

Invoices are generated and sent electronically to the designated billing point of contact (POC) at the agency. The POC on the GL Solutions side is typically our Analysis, Measurements, and Results Coordinator, who ensures accurate and timely processing of invoices.

Agencies may submit payments electronically or by check. Credit card payments are not accepted. GL Solutions maintains detailed billing records and provides transparency into all charges and payment activity to support accurate financial tracking and reconciliation.

• Training outlines the general requirements for providing training for implementing and using the solution at the End-User level and at Administrative/Operational Personnel levels.

Training
GL Solutions provides a comprehensive training program designed to equip client staff with the knowledge and skills necessary to effectively use and administer the GL Suite system. Our training methodology follows a structured "show, tell, practice, and repeat" approach, ensuring trainees gain mastery through guided instruction and hands-on experience.

Training Approach
Training is delivered at key stages of the software development lifecycle:

- **Initiation** – Introduces project goals, scope, and system overview.
- **Design** – Covers system configuration and functionality.
- **User Testing** – Focuses on end-user system operation and workflow validation.
- **Go Live (Production Use)** – Prepares users for live system operation with final training sessions.
- **Post-Implementation** – Provides follow-up training and support as needed.

GL Solutions develops a detailed training plan in collaboration with the client, covering:

- Training requirements and objectives
- Methodology and delivery format (onsite or remote)
- Facilities and equipment needed
- Number of sessions, dates, and times

Training Delivery
Final training is conducted just before go-live. If on-site training is desired, our trainer remains onsite afterward to provide immediate guidance as users transition to daily operations. Training can also be delivered remotely for pre-navigation or follow-up sessions as needed.

We also offer a train-the-trainer program, where a Subject Matter Expert (SME) or Super User within the client's team is trained to lead internal training sessions and provide ongoing support. This approach empowers the client's staff to manage training continuity and knowledge transfer internally.

Training Program – Materials and Courseware
GL Solutions develops tailored training materials aligned with the client's business processes and system configuration. Courseware includes:

- **Program Guide** – Overview of the training program, roles, and learning objectives.
- **Lesson Plan** – Course structure and timeline.
- **Skills Activities List** – Step-by-step guidance on key system functions.
- **Individual Training Record** – Tracks individual progress and mastery.
- **Hands-On Exercises** – Real-world scenarios to reinforce learning.
- **Self-Assessment and Evaluation** – Feedback on training effectiveness and learning outcomes.

Training materials are provided in MS Word format and available in both hardcopy and electronic formats.

Training Environment
GL Solutions recommends a dedicated training room with:

- An **Instructor Station** equipped with a projector, computer, and internet access.
- **Trainee Stations** with computers and internet access, shared by no more than one other trainee.
- Class size should be limited to **25–30 trainees** for effective instruction. For larger organizations, GL Solutions can divide training into smaller sessions to maintain quality instruction.

GL Solutions' training program ensures client staff are fully equipped to operate and manage GL Suite effectively, supporting a smooth transition and long-term system success.

D.1.7. Cost Savings - The Bidder will work in the best interest of the state and its customers to leverage volume or enterprise license agreements and maximize cost savings through better pricing, publisher's promotions, or other savings opportunities.

GL Solutions will work with the state and its customers to leverage volume or enterprise license agreements, maximizing cost savings.

As referenced in subsection 8.2.H, a VPAT; Security Certification and Accreditation Assessment; service level agreements and proposed first draft of Statement of Work, are requested to be included in the Bid.

GL Solutions has provided a VPAT in ***Attachment D*** as well as in the following link:

GL Solutions VPAT 09.29.24.docx

SOW Provided in Attachment B

Security Assessment provided in Attachment 08_-_FY24_State_of_Oklahoma_Vendor_Security_Assessment

Point by point response to bid requirements:

Information Security Requirements – Attachment D-1

GL Solutions' Compliance with Oklahoma Information Security Requirements

GL Solutions is committed to maintaining the highest standards of information security and regulatory compliance. Our system adheres to the security policies and requirements outlined by the State of Oklahoma, including those related to HIPAA, CJIS, and Federal Tax Information (FTI), as applicable. We achieve compliance through strict access controls, encryption, background checks, secure data handling, detailed audit logging, and incident response protocols. Compliance ensures data protection, mitigates risk, builds client trust, and maintains uninterrupted service, reinforcing our position as a secure and reliable partner.

1. General Information Security Requirements
GL Solutions ensures that no employee or subcontractor is granted access to State of Oklahoma agency information systems without prior completion and approval of the required logon authorization and acceptable use requests. We follow strict access control measures in compliance with client security policies. We promptly notify relevant agencies upon the termination of any employee or subcontractor who previously had access to agency systems. In

the event of a suspected security breach, we will disclose the incident to the client without unreasonable delay and fully cooperate during the investigation and resolution process. GL Solutions complies with the State of Oklahoma's "Information Security Policy, Procedures, and Guidelines" to ensure a secure operating environment.

2. HIPAA Requirements

GL Solutions complies with the HIPAA Privacy Rule (45 C.F.R. Parts 160 and 164) by ensuring that Protected Health Information (PHI) is used and disclosed strictly in accordance with HIPAA regulations. Our security framework safeguards PHI and prevents unauthorized access. If applicable, we will sign and adhere to a Business Associate Agreement (BAA) to ensure that PHI is used solely for contractual purposes, safeguarded against misuse, and handled in full compliance with HIPAA.

3. FERPA Compliance

GL Solutions complies with the Family Educational Rights and Privacy Act (FERPA) by implementing strict security measures to protect the privacy of student education records. Access to education records is restricted through Role-Based Access Control (RBAC), allowing only authorized personnel to access sensitive data. All education data is encrypted at rest and in transit to prevent unauthorized disclosure. Detailed audit logs track data access and modifications to ensure compliance with FERPA regulations and facilitate oversight.

4. Federal Tax Information (FTI) Requirements

GL Solutions complies with IRS Publication 1075 to safeguard Federal Tax Information (FTI). We implement strict access controls, conduct background checks, and ensure that FTI is used only for contract-related purposes. FTI is securely stored, processed, and properly disposed of after contract completion. All systems handling FTI meet IRS security standards, and any subcontracting involving FTI requires prior IRS approval. The agency may terminate the contract if FTI safeguard requirements are not met.

5. CJIS Requirements

GL Solutions is CJIS compliant and ensures that all software and equipment handling Criminal Justice Information (CJI) adhere to the most current version of the FBI CJIS Security Policy. We implement administrative, procedural, and technical safeguards to protect CJI and work closely with agencies to ensure compliance and facilitate audits. If required, we will complete Appendix H of the CJIS Security Policy and ensure that any third parties with access to CJI adhere to these security requirements.

Attachment E-1

GL Suite Software Agreement

General Terms

1. **Reserved.**

2. **Contract Purpose**. The purpose of this contract is to provide for the installation, hosting and servicing of a business process automation software application known as GL Suite in accordance with the terms of this contract

3. **Reserved.**

4. **Term**. The Agreement shall expire concurrently upon the expiration of all GL Simple plans. GL Simple plans are offered only for the most current and immediately prior version of the Software in effect at the time the GL Simple plan is purchased.

5. **Reserved.**

6. **Assignments by Company.** Any and all rights and interests of Company under this Contract may be assigned, either in whole or in part, without notice to Licensee, and Licensee agrees that its rights under this Contract are expressly subject and subordinate to any and all security interests which may now or hereafter be placed by Company or its assigns upon the Software. All references in this subparagraph to assignment shall be deemed also to include any pledge, mortgage, transfer or other disposition. Subject always to the foregoing provisions of this section, this Contract shall inure to the benefit of, and shall be binding upon, the successors and assigns of the parties hereto and, where appropriate, their heirs, legatees and personal representatives. The

   Company will provide Licensee with no less than a ninety (90) calendar day notice of impending cessation of its business.

7. *Reserved.*

8. **Payments.** Licensee shall make payments to Company in accordance with the SW1041 payment terms during the installation and prior to the first day of a GL Simple plan period. Licensee may elect quarterly or annual billing for the GLSimple plan fees. If the Licensee fails to make timely payment for a quarterly invoice, Company shall require annual payment of GL Simple plan fees. Company may prorate GL Simple fees to coincide with the end of a quarter or the Licensee's fiscal year.

   a. Irrespective of any language on or accompanying a payment, Company shall apply all payments received

to the oldest invoice due.

9. *Reserved.*

- Transition Upon Termination - During any GL Simple Plan and upon an appropriate service request by Licensee, Company shall provide services under a GL Simple plan for an effective and efficient transition of service with minimal disruption to the Licensee including cooperation and assistance to ensure that all Licensee data is securely transferred to Licensee, within thirty (30) calendar days of the request. The services provided shall assist Company's successor with a successful transition to the new service and/or equipment, with minimal downtime and adverse effect on the Licensee. Licensee Data will be transferred in SQL Server Database Backup format via a SFTP site specified by Licensee or through other media as required by the size of the data. During any GL Simple plan, the Company will provide a written statement or certificate to the Licensee stating that all Licensee data has been transferred or deleted or disposed of as directed by the Licensee.

10. **Notices.** Any and all notices ("Notices") which either party hereto may desire to give to the other party hereunder shall be deemed to be duly given if and only if mailed by registered or certified mail, postage prepaid, addressed to the other party at its address as set forth below or at such other address as such party may designate to the other party in writing from time to time. Notification by any other means shall be considered a service request and a waiver of any related breach of contract dispute until such time as the party provides notice in accordance with this paragraph.

If to Company: GL Suite, Inc.
555 Corporate Dr
Suite 301
Kalispell, MT 59901

If to Licensee: Mailing address identified by Licensee on Licensee's public web site.

GL Suite Software

1. Software License. Company grants to Licensee and Licensee accepts from Company a non-exclusive, non- transferrable, terminal license and right to use GL Suite software for each named individual for whom Licensee purchases a GL Simple support plan. GL Suite is a software application designed to automate business processes in specific industries such as risk management, claim and government regulations (the "Software") on the terms and conditions set forth in this Contract, exclusively for the following purposes defined in this section. The license shall terminate concurrently with any GL Simple plan.

- Licensee may use the Software to support customers, licensees, and other third parties for the purpose of providing these persons the ability to make payments, apply, renew licenses, verify requirements, report enforcement actions and related information and documents. Licensee may connect third-party software to the Software through Company provided interfaces to support the use identified in this paragraph.
- For the duration of this Contract, Company licenses to Licensee the rights to develop new customized functionality for the exclusive use of Licensee. All such developments by Licensee shall be considered part of the "Software."
- Company designed the Software for the purpose of meeting multiple Licensee needs without modification of software code distributed to all Licensees. Company retains the right to determine whether the functionality requirements shall be provided by configuration of the Software or by modifications to the Software distributed

to all licensees.
- Software includes all new releases and versions, and deliverables provided as a service in a GL Simple plan.

2. License Limitations. The Software license granted by this Contract is limited.

- Licensee may not use, copy, modify, or transfer the Software, or any copy, in whole or in part, except as expressly provided for in this Contract.
- Licensee may copy the Software only for backup purposes, provided that Licensee reproduces all copyright and other proprietary notices that are on the original copy of the Software provided to Licensee.

- Company retains all rights, title and interest in and to all software, documentation, derivative works and other intellectual property developed, designed, created or contributed by Company pursuant to this Contract, excluding Licensee's domain name, and excluding the graphics and data supplied by Licensee.
- Licensee may transfer the Software and all rights under this Contract to another party together with a copy of this Contract if the other party agrees to accept the terms of this Contract and Licensee receives written authorization directly from Company prior to any such transfer. If Licensee transfers the Software, Licensee must at the same time either transfer all copies whether in printed or machine-readable form to the same party or destroy any copies not transferred. Any attempt to transfer any of the rights, duties, or obligations hereunder except as expressly provided for in this Contract is void.
- Licensee may not rent, lease, loan, resell for profit, distribute, or network the Software except as otherwise provided in this Contract.
- Licensee agrees not to disassemble, decompile, translate or convert into human readable form or into another computer language, reconstruct or decrypt, or reverse engineer, all or any part of the Software to develop new software with some or all of the functions of the Software.
- In the event Company ceases to exist and fails to assign its rights in the Software to another entity, Licensee shall have the right to make modifications of the Software source code notwithstanding the terms of this section.
- Licensee shall not donate, distribute, license, sell or otherwise authorize the use or possession of modifications to any person other than Licensee's employees.
- Any software, reports, data structures, and other work product, not containing Customer Data, created as a consequence of GL Simple plan service shall become the exclusive property of Company. Company licenses without additional charge Custom Programs to Licensee. License shall include all rights granted under the Software License and the additional rights to decompile and modify the software, reports, data structures, and other work product created as a consequence of software maintenance.

3. **Software Component Licenses.** Software includes the distribution of other licensed software code subject to the limitations noted below:

- The Alex FTPS Client is distributed under the GNU Library General Public License (LGPL). Therefore, the licensee is entitled to all rights under that license to the Alex FTPS Client software assemblies only.
- Json.net Copyright (c) James Newton-King from Newtonsoft is provided under the MIT Free Software license. Therefore, the licensee is entitled to all rights under that license to Newtonsoft assembly only.
- The Sphorium Technologies Webdav.Net is distributed under the GNU Library General Public License (LGPL). Therefore, the licensee is entitled to all rights under that license to the Sphorium Technologies Webdav.Net software assemblies only.
- Software redistributes Telerik Rad Controls, Telerik. All rights reserved, for Ajax under license with Telerik. Licensee may not develop new software utilizing Telerik's software libraries without first obtaining a Telerik Developer's License. Licensee may configure and utilize Software features without a Telerik Developer's License.

4. Intellectual Property Protection. This Contract does not provide Licensee with title to or ownership of the Software, but only a right of limited use. Company shall have sole and exclusive ownership of all right, title and interest in and to the

Software, all copies thereof, all derivative works, Program Concepts, and all related works and materials (including ownership of all copyrights, trademarks and other intellectualproperty rightspertaining thereto), in any media now existing or subsequently developed, whether created by Company or any other party, subject to the rights of Licensee expressly granted herein. Licensee agrees to protect Company's interest in the Software, as follows.

- Licensee agrees to allow access or use of the Software only by employees of Licensee or by contractors under a written Contract, which preserves Company's rights to the Software and that prevents contractors from using, redistributing, disclosing or otherwise violating the rights of Company.
- Licensee agrees to maintain the confidentiality of the Software including all concepts, documentation, methods, processes and ideas, and the structure, sequence, and organization, designs, data models, tables and set- ups, and interfaces embodied, or expressed therein (the "Program Concepts") and to use same only as expressly authorized in this License. Licensee shall not disclose, provide, or make the Software or Program Concepts available in any form or medium to any person, in whole or in part, except on a confidential basis to such of Licensee's employees and consultants who need to access the Software to enable Licensee to exercise its rights under this License. Licensee shall take reasonable steps to ensure that such employees and consultants will keep the Software and Program Concepts confidential, and Licensee shall be liable for any breach of this Contract by such employees or consultants.
- Licensee shall include all proprietary, copyright, trademark, design right and trade secret legends, in the same form and location as the legend appearing on the Software on all authorized backup and archival copies of the Software. Further, Licensee shall not remove any proprietary, copyright, trademark, design right or trade secret legend from the Software.
- Licensee shall, at its own expense, keep the Software free and clear of all levies, liens and encumbrances. Licensee shall give Company immediate notice of any attachment or other judicial process affecting the Software.

Project Management

Management Plan. Within 30 days following contract execution and annually thereafter, Licensee and Company shall Accept a Management Plan, which describes the project management methodology including scope, schedule, change, risk, deliverable review and communication management activities.

Company's Duties. Company shall provide the services identified in the Management Plan and those listed in this section during the installation and for the term of any GL Simple plan.

- Conversion – Company will to transfer legacy data from delimited or fixed length ASCII text files or an ODBC compliant data source to the Software. Transfer of data means the manipulation of data from a data source to the table structure utilized by Software. Conversion Services does not include the identification or correction of data-entry or normalization errors present in legacy systems.
- Design – Company shall gather business requirements from Licensee and create designs and specifications that describe the Software functionality that accomplishes the business requirements gathered. Software may accomplish the functional outcomes of the Legacy System using alternate controls, steps and procedures, some of which may be faster or slower for users to execute in the Software than in the legacy Software.
- Development – Company shall configure and program the Software to operate in accordance to Accepted specifications.
- Testing – Company shall perform unit and system tests to ensure the development conforms to the Accepted specifications.
- Training – Company shall provide end user training on how to use the software as described in Accepted specifications.
- Project Management – Company shall perform project scope, schedule, change, conflict, risk, deliverable review,

and communication management activities.

Licensee's Duties. Licensee shall provide the services identified in the Management Plan and those listed in this section for the term of any GL Simple plan. Licensee agrees that Company's performance is dependent upon Licensee's timely and effective cooperation with Company. Accordingly, Licensee acknowledges that any delay by Licensee waives any requirement for Company's timely performance; waives Licensee's rights to liquidated damages, cause by Licensee's delay, if any; may cause delay in the first production use of the software and subsequent delivery of a GL Simple plan services. Performance by Licensee of the provisions of this section shall be an essential element of this contract.

- Conversion - Licensee shall produce legacy data along with documentation that describes the Legacy Data structure, relationships, fields and tables in detail sufficient to enable Company to convert the data to a format utilized by Software
- Subject Matter Expertise - Licensee shall provide all necessary staff required by Company to assist Company with the design. Staff shall possess subject matter expertise on Licensee's operations and business requirements.
- Change Management – Licensee shall provide all executive and management necessary to manage change and redirect or redefine the use of resources, business process, budget allocations, or other modes of operation necessary to ensure an effective and smooth software installation. Licensee will counter resistance from employees and align them to overall project objectives. The leading risk to software installations is inadequate personnel leadership and supervision. Licensee will provide effective communication that informs project stakeholders of the reasons for the change, the benefits of successful implementation as well as the details of the change.
- Design – Licensee shall allocate necessary staff resources to provide detailed business requirement descriptions, review deliverables, and answer clarifying business requirement questions in accordance with the Management Plan.
- Communication Management - An employee of Licensee with direct supervisory authority over Software users shall attend all project management status meetings throughout the project.
- Training – Licensee shall require training attendance and participation by Software users. Licensee shall provide one or more employees with responsibility for retraining users and providing personal direction to employees requiring additional assistance.
- UAT - Licensee shall conduct UAT testing exclusively by following written process instructions and flow diagrams provided by Company and developed for each business process identified in the Goal and Scope Document. Licensee shall allocate necessary staff resources to complete UAT exit criteria in the UAT Plan including testing all processes during the UAT period.
- Licensee shall allocate necessary staff resources including, but not limited to, provide detailed business requirement descriptions, review deliverables, answer clarifying business requirement questions, perform UAT testing, and manage staff and process change within Licensee's organization.

Project Management Tools. Company and Licensee agree to use GL Portal, an online, web-based project management system developed by Company to store project deliverables, communicate schedules, provide Acceptance of specifications and other deliverables, answer clarifications, report defects, and provide notifications.

- Company will issue Licensee a unique login and access to GL Portal for each person authorized by Licensee.
- Licensee will authorize Company to grant GL Portal access only to Licensee agents with authority to act on behalf of Licensee.
- Company shall utilize Microsoft Word, Excel, PowerPoint and Visio to develop written project documents.
- Company shall provide project management forms for acceptance, deliverable review reporting defects, etc. No other project management software or forms shall be used.

Requirements Refinement. Software functionality required by this contract shall be clarified through a process of refinement. The refinement begins with the adoption of a Goal and Scope Document which describes the business processes, interfaces, outputs and legacy data sources required prior to production use of the software. Subsequently to the first production use of the system, a Goal and Scope document shall be adopted for each GL Simple Project.

Order of Precedence. When determining software functionality only, required by this contract, the following documents shall have precedence in the order listed:

- Specifications which includes detailed design documents including Self-Documenting Specifications, Report, Correspondence and Subform Designs, Web Page Specifications, and Security Specifications

    - Business Process Design or Web Site Design
    - Goal and Scope Document
    - Change Requests
    - Contract, as amended
    - Company's Offer, as amended
    - Licensee's RFP, as amended, if any

Specification and Document Deliverable Review. Company shall create specifications and other documentation, such as project management documents, training, and software documentation, to support the Goal and Scope Document.

- Company shall submit specifications and documentation to Licensee for Acceptance using GL Portal. Company shall specify which contract requirements are met by the specification or documentation.
- Licensee shall review the specification or documentation to determine whether the document, if developed per the specification, fulfills the contract requirement specified by Company.
- Licensee shall respond to Company's request for approval by:

1. Accepting the submitted specification or documentation within seven business days,
2. Rejecting the specification or documentation within seven business days, or
3. Not responding to the Acceptance request within seven business days. Not responding to the Acceptance request within seven business days constitutes Licensee's Acceptance of the specification or documentation.

- If the specification or documentation does not conform to the Contract, Licensee shall notify Company using GL Portal and forms provided by Company specifying the specific contract exceptions which cause the specification or documentation to be unacceptable. All such deficiencies within the specification or documentation must be noted during Licensee's initial review of the specification or documentation.
- Company shall correct the deficiencies and resubmit the specification or documentation within seven calendar days from the receipt of the rejection.
- Licensee shall have seven calendar days to re-inspect, test and reevaluate the resubmitted specification or documentation to determine whether deficiencies initially noted are corrected.
- Additional cycles may be added until all deficiencies initially noted are corrected.
- During any re-inspection by Licensee, the Licensee may not report any new deficiency not reported during the initial rejection of the specification or documentation.
- Acceptance of a specification or documentation constitutes Acceptance that Company's development and implementation of the software according to the specification or documentation satisfies Company's performance obligations with respect to the corresponding contract requirement identified. Acceptance of a software deliverable constitutes Acceptance that the Software performs as specified.

Delivery. Delivery of a project artifact, deliverable or software occurs upon any of the earliest of any of the following events:

- Delivery scheduled in a project plan, Goal and Scope Document, Management Plan, UAT Plan;
- Notification of delivery in GL Portal; or,
- Actual notification of delivery by email or phone.

Acceptance. Any the following conditions constitute acceptance ("Acceptance") of a project document, specification, software, Software, sub-deliverable or deliverable by Licensee, in the form delivered by Company:

- Written acceptance by Licensee;
- Production use of the Software in a live environment; or

Failure to test, inspect and report specific defects regarding the Software or any contract deliverable within seven

businessdays after delivery by Company to Licensee.

UAT Plan. No later than 30 days prior to the planned commencement of User Acceptance Testing for the initial product usage of the Software, Licensee and Company shall adopt a UAT Plan, which describes the objective, measurable criteria for beginning and successfully exiting UAT. Successful performance of the UAT exit criteria constitutes Licensee's direction to complete the migration and deliver the Software to the production environment.

GL Simple

GL Simple Plan. Company offers licensing, hosting, software, maintenance and warrant services as annual support plans. ("GL Simple"). Licensee's right to purchase a GL Simple plan from Company expires five years from execution of this Contract, unless otherwise extended by mutual agreement between the parties. GL Simple plansmust be purchased for consecutive time periodsbeginning with the first production useof the software. Failure by Licensee to purchase a GL Simple plan for any period of time terminates Licensee's right to purchase a GL Simple plan under this Contract.

- The annual cost of a GL Simple plan is based on the tier and number of named Licensee employees or contractors with access to the Software whether or not such usage is concurrent as shown in the Pricing Addendum. Licensee shall purchase the same GL Simple-Tier plan for all named-users.
- Certain GL Simple services require the use of a Task or Project.
  - **(1)** Projects – A project includes a request for a GL Simple service with any of the following characteristics: 1) functionality requests that require coordination between Company and a third-party; 2) functionality requests with three or more finite deliverables which must be delivered in a specific sequence to meet the Licensee's business requirements; 3) functionality which may impact other aspects of the configured Software and therefore require a system test of an entire business process; or 4) service or functionality which requires the presence of a Company employee onsite at Licensee's place of business.
  - **(2)** Tasks – A task is a single request for a GL Simple plan service except requests that are a project.
- At the Company's sole discretion, Company may establish and modify reasonable policies affecting the definition of GL Simple services, the concurrency of item fulfillment, the definition of projects and tasks, and the request timing required to perform requests within a GL Simple plan.
- Company may determine that a request is more than one project if the activities are designed to produce more than one specific final output; the activities may start and stop independently of one another; an output is being produced for more than one internal or external customer; or, the process steps substantially vary to produce the specific final output. Company may determine a request for a public web site enhancement is more than one project if the site includes alternate processing steps for ownership or employment changes, address change, names changes, status changes, fees, or license input based on license type or status or other license criteria.
- Changing Company or software industry standards may require the use of a project prior to update an existing web site or business process to conform to the new standard.
- All GL Simple plans shall be purchased for an annual term. Upon the expiration of any annual term, the GL Simple plan tier then in effect for Licensee shall be automatically renewed for an additional annual term, unless Licensee has provided Company 90-day's written notice of non-renewal or request to change GL Simple plan tier prior to the date of current GL Simple plan expiration.

GL Simple Plan Tiers.

- GL Simple plans are offered in three tiers: Standard, Professional and Enterprise. Prior to the first production use

of the Software, Company shall provide an unlimited number of Tasks and Projects in support of Licensee's installation. Following the first production use of the software, Company shall provide "Tasks" and "Projects" specified for the tier in the chart below.

GL Simple Tier	Tasks for Services	Projects for Services
Standard	None included	None included
Professional	2 tasks/user/year or 24 tasks per year, whichever is greater; max 200	One concurrent project, no limit on total
Enterprise	4 tasks/user/year or 48 tasks per year, whichever is greater; max 400	Three concurrent projects, no limit on total

- Licensee shall purchase a GL Simple – Enterprise tier plan for all named users until the first production usage of the Software. Licensee may select a subsequent GL Simple plan tier upon the first product usage of the Software and annually thereafter by notifying Company in writing of the desired tier. Licensee shall pay a fee designed in the Pricing Addendum for the corresponding tier. Company may increase the cost of any item in the Pricing Addendum by a percentage not to exceed the consumer price index for urban dwellers of the most recent twelve-month period reported by the United States Department of Labor. Company shall notify Licensee not less than three months prior to any price change.
- Licensees purchasing the Standard tier must purchase GL Simple for a minimum of 25 named Licensee employees or contractors with access to the Software. Licensees purchasing the Professional tier must purchase GL Simple for a minimum of 8 named Licensee employees or contractors with access to the Software. Licensees purchasing the Enterprise tier must purchase GL Simple for a minimum of 2 named Licensee employees or contractors with access to the Software.
- Licensee may incrementally increase the number of Tasks or concurrent Projects in a GL Simple tier by paying an "Escalation Fee" in the amount applicable for each task or project pursuant to the Pricing Addendum.

GL Simple Services.

Company offers GL Simple services as labeled in the first row in the GL Simple Service table below. The columns to the right of the service determine whether the service is offered to the GL Simple plan tier.

- Services with a "$" mark are available to the tier through escalated Tasks and/or Projects only.
- Services with a check mark without the symbol "ŧ" are provided are provided without limitation.
- Services noted with the symbol "ŧ" utilize a Task or Project.
- Services without any mark for the tier are not available to that tier.

GL Simple Service Table

GL Simple Service	GL Simple Standard	GL Simple Professional	GL Simple Enterprise
Account Management			
Schedule Management	✓	✓	✓
Scope Management	✓	✓	✓
Risk Management	✓	✓	✓
Communication Management	✓	✓	✓
Client Engagement	✓	✓	✓
Project Initiation	✓	✓	✓
Change Management	✓	✓	✓
Critical Project Monitoring		✓	✓
Critical Task Prioritization		✓	✓
Technical Support			
Emergency Support (24 X 7 X 365)	✓ 3 hr response	✓ 1 hr response	✓ 15 min response
User Questions	✓	✓	✓
Design Review	✓	✓	✓
Developer Support	$	✓t	✓t
Hardware, Network and Security Support	$	✓t	✓t
Architecture and Best Practice Guidance		✓t	✓t
Training and Documentation			
Design Training	✓	✓	✓
User Training	✓	✓	✓
Developer Training	$	✓t	✓t

GL Simple Service	GL Simple Standard	GL Simple Professional	GL Simple Enterprise

Administrator and Configuration Training	$	✓ t	✓ t
Administrator and Configuration Documentation	✓	✓	✓
User Conference	✓	✓	✓
Software Patches and Releases for Core Software			
Software Releases	✓	✓	✓
Software Patches	✓	✓	✓
Software Release Installation	$	✓ t	✓ t
Software Patch Installation	✓	✓	✓
Warranty and Enhancements			
Lifetime Defect Correction	✓	✓	✓
Configuration and Customization	$	✓ t	✓ t
Data Center and Security			
Compliance Audit (PCI, NIST, HIPAA)	✓	✓	✓
Site Setup	✓	✓	✓
Hosting	✓	✓	✓
Server Move	$	✓ t	✓ t
Configuration Management (Tiered Environments: Dev, Sys, UAT and Prod)	✓	✓	✓
Background Checks	$	✓ t	✓ t
On-Premise Hosting Option		✓ t	✓ t
Security Assessment		✓ t	✓ t
Custom Network Isolation and Management		✓ t	✓ t
Multi-Factor Authentication			✓
Uptime Guarantee		95%	99.9%
Disaster Recovery			
Data Export Service	$	✓ t	✓ t
Site Health Dashboard		✓	✓

GL Simple Service	GL Simple Standard	GL Simple Professional	GL Simple Enterprise

Hardware Redundancy		✓	✓
Automated Job and Interface Monitoring/Response			✓
Automated Site Monitoring/Response			✓
Disaster Plan Testing			✓
Backups	7 days	14 days	3 months
Disaster Recovery	within 14 days	within 3 days	within 1 hour
Mobile Inspections			
Mobile Inspection Service – per device	$	$	$
Mobile Inspection Form Development		✓ t	✓ t
Mobile Inspection Dispatch Service		✓ t	✓ t
On-Premise Mobile Dispatch and Synchronization DB		✓ t	✓ t
Business Intelligence			
Power BI - Visual and interactive reports and dashboards for business analytics	$	✓ t	✓ t
Self-Service Administration (by Licensee)			
User Security Administration	✓	✓	✓
Ticket and Project Tracking Portal	✓	✓	✓
Automated Task and Project Promotion Between Environments	✓	✓	✓
Business Rule Configuration	✓	✓	✓
Output Modification	✓	✓	✓
Access your data using alternative tools (e.g. SQL Server Management Studio)			✓
Power BI Professional license for authoring and publishing			✓

Hosting – GL Simple plans include hosting of Software on servers owned, operated, housed, and maintained by Company and access to the hosted Software by Licensee through the Internet. Company shall acquire any and all license rights necessary and appropriate for Company to provide the Software as obligated by the Contract.

- Company shall maintain sufficient hardware capacity to satisfy the technical requirements and the bandwidth and required storage capacity required to meet the Contract.
- Company shall be responsible for all telecommunication connections from the server hosting the Software to the Internet.
- Company may collect user-specific data only as necessary to provide services authorized under the Contract. No information regarding Licensee or any Software user shall be disclosed, provided, rented or sold to any third party for any reason unless required by law or regulation or by an order of a court of competent jurisdiction. This obligation shall extend beyond the term of the Contract.
- The Software will available to Licensee twenty-four (24) hours a day, seven (7) days a week ("Uptime") less

Excusable Downtime for at least the percentage of time indicated for the "Uptime Guarantee" corresponding to Licensee's GL Simple plan tier in the GL Simple Service Table.

- For the purposes of this Contract, "Excusable Downtime" is defined as that period of time when the Licensed Services are not available to Licensee due to scheduled network, hardware or service maintenance and/or upgrades. Except in cases of emergency, Licensee shall be provided a two (2) business day advance notification of such maintenance and/or upgrade. In cases of emergency, Company will use its best efforts to notify Licensee of a planned Downtime as soon as practicable. Maintenance or upgrades shall not occur Monday through Friday, between the hours of 6:00 a.m. and 8:00 p.m. Eastern Time. Excusable Downtime shall not include (i) an electronic hardware failure, (ii) a failure in the Software, (iii) an electric utility failure at a Company's owned or leased facility where the Software is hosted, or (iv) a network failure up to, but not including, the interconnection point of Company's network to the public switched telephone network.
- Company shall take reasonable efforts to notify Licensee at least thirty (30) days prior to of any planned change(s) or update(s) to the Software; its functionality; content storage/ backup/disaster recovery, including physical location; security architecture, features or settings; terminations and/or replacement of any Company subcontractor. The planned changes or updates include any change(s) that would potentially impact the secure and efficient use of the Software, as understood and agreed to between Company and Licensee.
- Company shall provide a secure environment and any hardware and software, including servers, network and data components provided by Company as part of its performance under this Contract. Company shall provide a secure environment for Content and any hardware and software in accordance with NIST 800-53 in order to prevent unauthorized access to and use or modification of, and to protect, the Software and Licensee data. Company agrees that all data entered by Licensee in the Software is intended solely for the business of Licensee and is considered private data.
- Company shall implement user identification and access controls designed to limit access to users in accordance with the principles of least privilege.
- Company shall ensure that all personnel with physical or logical access to the software will receive industry standard annual security awareness training.
- Company shall ensure that the Software is capable of auditing the following events: Successful and unsuccessful account logon events, account management events, object access, policy change, privilege functions, process tracking, and system events, all administrator activity, authentication checks, authorization checks, data deletions, data access, data changes, and permission changes.
- Company shall ensure that the Software employs automated mechanisms to centrally review, analyze and correlate audit and log records from multiple components of the Software to support organizational processes for investigation, alerting and response to suspicious activities.
- Company shall ensure that the Software supports exporting of log files to the Licensee for review and analysis.
- Company shall provide evidence of a comprehensive continuous monitoring program encompassing all systems with access to Licensee data.
- Company shall ensure that all changes to proposed Software or Hosting services are authorized according to change management policies.
- Company shall provide and maintain a backup of Software and Licensee data that can be recovered in an orderly and timely manner within a predefined frequency consistent with recovery time and recovery point objectives, as specified in the GL Simple Service table. Company shall store a backup of Content, at least daily, in an off-site "hardened" facility, located within the continental United States, maintaining the security of the Software and Licensee data.
- Company shall implement a contingency plan designed to maintain the access to the Software and to prevent the unintended destruction or loss of Content. This plan should provide a predefined frequency, consistent with recovery time and recovery point objectives for disaster recovery and archival purposes of Software at a secure facility located within the continental United States.
- Company shall maintain an incident response program that implements incident handling for security incidents that includes preparation, detection and analysis, containment, eradication, and recovery processes. Incident response must have the capability to support automated mechanisms for supporting incident handling

processes.

- Company shall perform quarterly scans using an Intrusion Detection System (IDS) and Intrusion Prevention System (IPS).
- Company shall support physical security measures, including securing Software on a secure server, in locked data cabinets within a secure facility located within the continental United States.
- Company shall ensure that access to facilities housing Software are restricted to only allow access to Company's personnel and agents who have a need to know in connection with operation and support of the Software.
- Company shall ensure that the Software, operating systems, middleware, applications, and interfaces will be scanned for vulnerabilities every 30 days.
- Company shall conduct monthly vulnerability scans against all public-facing interfaces with access to the Software.
- Company shall ensure that Software is stored, processed and maintained within the continental United States at all times.
- Company shall, at all times, remain compliant with the privacy and security requirements mandated by federal, state and local laws and regulations.
- Company shall ensure performance of a security audit at least once annually of the Software.
- Company shall ensure that external connections incorporated into the Software have appropriate security controls including industry standard intrusion detection and countermeasures that will detect and terminate any unauthorized activity prior to entering the firewall maintained by Company.

(aa) Company shall ensure that the Software will utilize industry standard firewalls regulating all data entering the internal data network from any external source which will enforce secure connections between internal and external systems and will permit only authorized data to pass through.

(bb) Company shall ensure that the Software will use industry standard encryption techniques to protect Content that is transmitted or stored on behalf of the Licensee.

(cc) Company shall utilize industry standard malware protection, incorporating both signature and non- signature-based detection mechanisms, on all systems with access to Software. Company shall ensure that malware protection will be centrally managed and receive regular automatic updates to malicious code protection mechanisms and data files from the software vendor.

Warranties

Software Warranties.

- Company warrants that Company has the full power and authority to grant the rights granted Licensee hereunder with respect to the Software, and neither the license or use by Licensee of the Software, as permitted under this License, will in any way constitute an infringement or other violation of any copyright, patent, trade secret, trademark or any other intellectual property right of any third party.
- In the event Software requires updating due to Federal, State statutory or regulatory requirements affecting Licensee, the Company's Software development department shall give its highest priority to the implementation of such updates, but Company does not warrant that all such updates will be completed, or that any updates will be completed by a certain time.
- In the event that the Software is, in the opinion of the Company, likely to or does become the subject of a claim for copyright or other intellectual property rights infringement, Company may, at its option and expense, either (1) procure for Licensee, the right under such third-party rights to use the Software; or (2) replace or modify the Software, or parts thereof, with other suitable and reasonable equivalent technology so that the Software becomes non-infringing; or (3) if it is not commercially reasonable to take actions specified in (1) and (2) immediately preceding, terminate this Contract and refund all license fees to Licensee.

GL Simple Service Warranty. During any GL Simple plan, Company warrants that the Software configuration will perform in material conformity with Accepted specifications. Company will cure all breaches of the foregoing warranty reported in GL Portal by Licensee during a GL Simple plan.

Hosting Service Warranty. Licensee assumes total responsibility for Licensee's use and users' use of the Software on any equipment provided by Company, if any, and the Internet. Licensee understands and agrees further that the Internet is accessible by persons who may attempt to breach the security of Company and/or Licensee's networks. Company has no control over and expressly disclaims any liability or responsibility whatsoever for such actions and Licensee and Licensee's end users access the service at Licensee's own risk. Hosting Services provided by Company are provided on an "as is" and "as available" basis without warranties of any kind, either express or implied, including but not limited to warranties of title, merchantability or fitness for a particular purpose. No advice or information given by Company, its affiliates or contractors or their respective employees, create a warranty. Some states do not allow the limitation of implied warranty, and therefore certain provisions may not apply to Licensees located in those states.

Warranty and Remedy Limitations. EXCEPT AS EXPRESSLY SET FORTH IN THIS SW1041 CONTRACT, COMPANY MAKES NO OTHER WARRANTIES OF ANY KIND, AND EXPRESSLY DISCLAIMS ANY AND ALL OTHER WARRANTIES, EXPRESS AND IMPLIED, AS TO ANY MATTER WHATSOEVER, INCLUDING, WITHOUT LIMITATION, THE SUITABILITY OR THE CONDITION OF THE SOFTWARE, OR ITS FITNESS OR SAFETY FOR ANY PARTICULAR PURPOSE OR USE, OR AS TO ITS MERCHANTABILITY. COMPANY MAKES NO WARRANTY REGARDING THE USABILITY OR CONVERTIBILITY OF ANY OF LICENSEE'S DATA, THE SUITABILITY OF THE SOFTWARE FOR LICENSEE'S NEEDS, OR ANY PERFORMANCE PROBLEM, OR OTHER MATTER ATTRIBUTABLE TO ANY USE OR MODIFICATION OF THE SOFTWARE, OR COMBINATION OF THE SOFTWARE WITH ANY OTHER SOFTWARE OR COMPUTER PROGRAM OR COMMUNICATIONS DEVICE, NOT EXPRESSLY AUTHORIZED BY COMPANY IN WRITING.

IN WITNESS WHEREOF, the parties hereto have caused this Contract to be duly executed the day and year first above written.

GL Suite, Inc.

By_____

Signature, Title Date

Licensee

By_____

Signature, Title Date

Attachment E-2: End User License Agreement (EULA)

GL Suite End User License Agreement

Contract

Parties. Parties to this GL Suite End User License Agreement ("Contract") include GL Suite, Inc. (dba GL Solutions), a Montana corporation ("Provider"), and the ordering entity receiving benefits as defined in SW1041 ("Customer").

Order of Precedence. When determining software functionality required by this contract only, the following documents shall have precedence in the order listed:

a) Specifications which include detailed design documents including Self-Documenting Specifications, output and web page specifications, and other specifications;
b) Process guides or process flow diagrams;
c) Goal and Scope Document
d) Change Requests
e) Scope of Work
f) This contract, as amended

The foregoing paragraph shall apply to software functionality only, and no provision therein shall be interpreted to mean that any document shall have precedence over SW1041 terms. contract terms.

Scope of Permitted Use

Software License. The purpose of this contract is to provide Customer with a regulatory business process automation software application known as GL Suite, including related setup, access, and support services. GL Suite is a software application designed to automate business processes in government regulatory agencies (the "Software"). The Provider grants Customer a non-exclusive, non-transferable, revocable, limited right to access and use the Software as a Service (SaaS) during the Term of this Agreement, solely for the Customer's internal business purposes and in accordance with Provider documentation of the same. Provider offers this SaaS contract along with licensing, customer service and support for Software in annual support plans referred to herein as "GL Simple plans".

User Licenses. Customer may authorize up to the number of named users specified in a purchase order or other contract document to access and use the SaaS. Customer is responsible for ensuring that all users comply with the terms and conditions of this contract.

Third-Party Users. Customer may not sublicense, resell, lease, rent, or otherwise make the SaaS available to any third party, except to entities not employed by the agency in conjunction with the Customer's regulatory activities such as applications, renewals, complaints, investigations, inspections and other regulatory activities carried out by Customer. Customer may also connect third-party software to the Software through Provider provided interfaces to support the use identified in this paragraph.

License Limitations. Customer may not use the SaaS for any unlawful, fraudulent, or malicious purposes, or in any manner that violates any applicable laws, regulations, or industry standards. Customer may not use the SaaS to interfere with or disrupt the operation of the Provider's systems or networks, or attempt to gain unauthorized access to the Provider's systems or networks. Customer may not modify, reverse engineer, decompile, disassemble, or create derivative works of the SaaS or any part thereof.

Updates. The license granted by this contract is limited to the most current and immediately prior version of the Software. Provider shall determine the functionality of the Software, which may be configured to meet Customer's specific business requirements. Provider shall take reasonable efforts to notify Customer at least thirty (30) days prior to of any planned change(s) or update(s) to the Software; its functionality; security architecture, features or settings. The planned changes or updates include any change(s) that would potentially impact the secure and efficient use of the Software, as understood and agreed to between Provider and Customer.

Confidentiality. Customer, subject to all state and federal law, rule, and regulation, including but not limited to the Oklahoma Open Records Act ("ORA"), agrees to maintain the confidentiality of the Software including all concepts, documentation, methods, processes and ideas, and the structure, sequence, and organization, designs, data models, tables and set-ups, and interfaces embodied, or expressed therein and to use same only as expressly authorized in this License.

Term and Termination

Agreement Term. This Agreement shall be effective during the term of any GL Simple Plan. ("Term of this Agreement")

Contract Renewal. Upon the expiration of any annual term, the GL Simple plan tier then in effect for Customer shall be automatically renewed for an additional annual term, unless Customer has provided Provider 30-day's written notice of non-renewal or request to change GL Simple plan tier prior to the date of current GL Simple plan expiration. Customer's right to purchase a GL Simple plan from Provider expires five years from execution of this Contract, unless otherwise extended by mutual agreement between the parties. GL Simple plans must be purchased for consecutive time periods. Failure by Customer to purchase a GL Simple plan for any period of time terminates Customer's right to purchase a GL Simple plan under this Contract.

Transition Upon Termination. Provider shall provide services under a GL Simple plan for an effective and efficient transition of service with minimal disruption to the Customer including cooperation and assistance to ensure that all Customer data is securely transferred to Customer. Customer data includes transactional data and images, but not data about the configuration of Software. Customer Data will be transferred in Microsoft SQL Server Database Backup or native image format via a SFTP site specified by Customer or through other media as required by the size of the data within 30 days of termination of the contract. Should data transfer require greater than 30 days, GL solutions will provide KDHE written confirmation that the data transfer process has been initiated, and provide a reasonable estimate of when it will be completed. Within 90 days following termination, Provider will provide a written certificate to Customer stating that all Customer data has been transferred or deleted or disposed of as directed by the Customer.

Remedies. In the event either party terminates the Contract for breach by the other, the non-breaching party shall have the right to exercise any and all available remedies provided by law.

Waiver. The waiver by either party, or the failure by either party, to claim a breach, or give notice with respect thereto, of any provision of this Contract shall not be, or be held to be, a waiver of any subsequent breach, or as affecting in any way the effectiveness, of such provision.

Data Ownership and Security

Customer Data. Customer shall retain ownership of all data entered by Customer or authorized third parties. Customer provided domain names, file uploads, and graphics belong to the customer. These data and files are collectively referred to as "Customer Data."

Use of Customer Data. Provider may collect Customer Data only as necessary to provide services authorized under the Contract. No Customer Data shall be disclosed, provided, rented or sold to any third party for any reason unless authorized by Customer, required by law or regulation or by an order of a court of competent jurisdiction.

Security. The Software Subject to this SaaS contract shall be provide by Provider in a secure environment. Provider shall provide good faith efforts to meet applicable NIST 800-53, SOC I and SOC II standards to prevent unauthorized access to and use or modification of, and to protect, the Software and Customer data.

- Provider shall implement user identification and access controls designed to limit access to users in accordance with the principles of least privilege.
- Provider shall ensure that all personnel with physical or logical access to the Software will receive industry standard annual security awareness training.
- Provider shall ensure that the Software is capable of auditing the following events: Successful and unsuccessful account logon events, account management events, object access, policy change,

privilege functions, process tracking, and system events, all administrator activity, authentication checks, authorization checks, data deletions, data access, data changes, and permission changes.

- Provider shall ensure that the Software employs automated mechanisms to centrally review, analyze and correlate audit and log records from multiple components of the Software to support organizational processes for investigation, alerting and response to suspicious activities.
- Provider shall ensure that the Software supports exporting of log files to the Customer for review and analysis.
- Provider shall provide evidence of a comprehensive continuous monitoring program encompassing all systems with access to Customer data.
- Provider shall ensure that all changes to proposed Software or Hosting services are authorized according to change management policies.
- Provider shall provide and maintain a backup of Software and Customer data that can be recovered in an orderly and timely manner within a predefined frequency consistent with recovery time and recovery point objectives. Provider shall store a backup of Content, at least daily, located within the continental United States, maintaining the security of the Software and Customer data.
- Provider shall implement a contingency plan designed to maintain the access to the Software and to prevent the unintended destruction or loss of Content. This plan should provide a predefined frequency, consistent with recovery time and recovery point objectives for disaster recovery and archival purposes of Software at a secure facility located within the continental United States.
- Provider shall maintain an incident response program that implements incident handling for security incidents that includes preparation, detection and analysis, containment, eradication, and recovery processes. Incident response must have the capability to support automated mechanisms for supporting incident handling processes.
- Provider shall perform quarterly scans using an Intrusion Detection System (IDS) and Intrusion Prevention System (IPS) and provide Customer with the results of those scans.
- Provider shall support physical security measures, including securing Software on a secure server, in locked data cabinets within a secure facility located within the continental United States.
- Provider shall ensure that access to facilities housing Software are restricted to only allow access to Provider's personnel and agents who have a need to know in connection with operation and support of the Software.
- Provider shall ensure that the Software, operating systems, middleware, applications, and interfaces will be scanned for vulnerabilities every 30 days.
- Provider shall conduct monthly vulnerability scans against all public-facing interfaces with access to the Software.
- Provider shall ensure that Software and Customer Data is stored, processed and maintained within the continental United States at all times. Provider shall further ensure that no Software or Customer Data is accessed by Provider’s employees, contractors, or any other individuals under Provider’s control from outside of the United States.
- Provider shall, at all times, remain compliant with the privacy and security requirements mandated by federal, state and local laws and regulations.
- Provider shall ensure performance of a security audit at least once annually of the Software.
- Provider shall ensure that external connections incorporated into the Software have appropriate security controls including industry standard intrusion detection and countermeasures that will detect and terminate any unauthorized activity prior to entering the firewall maintained by Provider.
- Provider shall ensure that the Software will utilize industry standard firewalls regulating all data entering the internal data network from any external source which will enforce secure connections between internal and external systems and will permit only authorized data to pass through.
- Provider shall ensure that the Software will use industry standard encryption techniques to protect Content that is transmitted or stored on behalf of the Customer.
- Provider shall utilize industry standard malware protection, incorporating both signature and non-signature-based detection mechanisms, on all systems with access to Software. Provider shall ensure

that malware protection will be centrally managed and receive regular automatic updates to malicious code protection mechanisms and data files from the software vendor.

Pricing and Payments

This Agreement is Contingent on the Availability of State and Federal Funds.

Due Dates. Payment for Setup Services and Escalated Projects are due upon Acceptance of the deliverables or Escalated Project. Payment for Escalated Tasks are due when ordered by Customer. Payment for GL Simple Plans are due prior to the first day of the GL Simple plan term. Annual GL Simple plans may be paid for in quarterly installments or in increments that coincide with the end of Customer's fiscal year. Irrespective of any language on or accompanying a payment, Provider shall apply all payments received to the oldest invoice due.

Setup Services

Setup Services. To enable Customer specific uses of the Software, Provider shall provide the services described in the Setup Services – Statement of Work attached for the fees specified.

Project Management. Within 30 days following contract execution and annually thereafter, Customer and Provider shall agree to a Management Plan, which describes the project management methodology including scope, schedule, change, risk, deliverable review and communication management activities. Provider and Customer shall perform project scope, schedule, change, conflict, risk, deliverable review, and communication management activities consistent with the Management Plan.

Project Management Tools. Provider and Customer agree to use GL Portal, an online, web-based project management system developed by Provider to store project deliverables, communicate schedules, provide Acceptance of specifications and other deliverables, answer clarifications, report defects, and provide notifications. Provider will issue Customer a unique login and access to GL Portal for each person authorized by Customer. Customer will authorize Provider to grant GL Portal access only to Customer agents with authority to act on behalf of Customer. Provider shall utilize Microsoft Word, Excel, PowerPoint and Visio to develop written project documents. Provider shall provide project management forms for acceptance, deliverable review reporting defects, etc. No other project management software or forms shall be used.

Conversion. Customer shall produce legacy data along with documentation that describes the Legacy Data structure, relationships, fields and tables in detail sufficient to enable Provider to convert the data to a format utilized by Software. Provider will transfer legacy data from delimited or fixed length ASCII text files or an ODBC compliant data source to the Software. Transfer of data means the manipulation of data from a data source to the table structure utilized by Software. Conversion Services does not include the identification or correction of data-entry or normalization errors present in legacy systems.

Requirements Refinement. Software functionality required by this contract shall be clarified through a process of refinement. The refinement begins with the adoption of a Goal and Scope Document which describes the business processes, interfaces, outputs and legacy data sources required prior to production use of the software. A Goal and Scope document shall be adopted for each GL Simple Project as required to modify, add or delete Customer business process functionality.

Configuration. Customer shall provide all necessary staff required by Provider to assist Provider with the design, review deliverables, and answer clarifying business requirement questions. Staff shall possess subject matter expertise on

Customer's operations and business requirements. Provider shall gather business requirements from Customer and create designs and specifications that describe the Software requirements functionality that accomplishes the business requirements gathered. Provider shall configure the Software to operate in accordance to Customer Accepted specifications. Provider shall perform unit and system tests to ensure the development conforms to the Accepted specifications.

Deliverable Review. Provider shall create specifications and other documentation, such as project management documents, training, and software documentation, to support the Goal and Scope Document. Provider shall submit specifications and documentation to Customer for Acceptance using GL Portal. Provider shall specify which contract requirements are met by the specification or documentation. Customer shall review the specification or documentation to determine whether the document, if developed per the specification, fulfills the contract requirement specified by Provider. Customer shall respond to Provider's request for approval by:

- Accepting the submitted specification or documentation within fourteen calendar days,
- Rejecting the specification or documentation within fourteen calendar days, or
- Not responding to the Acceptance request within fourteen calendar days. Not responding to the Acceptance request within fourteen calendar days constitutes Customer's Acceptance of the specification or documentation.

If the specification or documentation does not conform to the Contract, Customer shall notify Provider using GL Portal specifying the specific contract exceptions which cause the specification or documentation to be unacceptable. All such deficiencies within the specification or documentation must be noted during Customer's initial review of the specification or documentation.

Provider shall correct the deficiencies and resubmit the specification or documentation within seven calendar days from the receipt of the rejection. Customer shall have fourteen calendar days to re-inspect, test and reevaluate the resubmitted specification or documentation to determine whether deficiencies initially noted are corrected. Additional cycles may be added until all deficiencies initially noted are corrected.

Acceptance of a specification or documentation constitutes Acceptance that Provider's configuration and implementation of the Software according to the specification or documentation satisfies Provider's performance obligations with respect to the corresponding contract requirement identified. Acceptance of a software deliverable constitutes Acceptance that the Software performs as specified.

Training. Provider shall provide end user training on how to use the configured Software as described in Accepted specifications. Customer shall require training attendance and participation by Software users. Customer shall provide one or more employees with responsibility for retraining users and providing personal direction to employees requiring additional assistance.

UAT. No later than 30 days prior to the planned commencement of User Acceptance Testing for the initial product usage of the Software, Customer and Provider shall adopt a UAT Plan, which describes the objective, measurable criteria for beginning and successfully exiting UAT. Successful performance of the UAT exit criteria constitutes Acceptance of setup services and customer's direction deliver the Software to the production environment. Customer shall conduct UAT testing of the configured Software exclusively by following process guides in the Software detailing each Customer business process.

Timeliness. Provider and Customer agree that timely and effective cooperation is essential to the provision of setup and support services in this contract. In the event Customer's cooperation is necessary for Provider's performance and Customer is responsible for a delay, Customer waives any requirement for Provider's timely performance; may cause delay in the production use of the software and subsequent delivery of support services. Notwithstanding the foregoing

paragraph, Customer's delay does not waive all of Provider's duties to perform on the Agreement, and, where possible, Provider shall mitigate the effects of any Customer delay by prioritizing tasks that can be completed unilaterally until the delay ends.

Acceptance. Any the following conditions constitute acceptance ("Acceptance") of a project document, specification, software, Software, sub-deliverable or deliverable by Customer, in the form delivered by Provider:

- Written acceptance by Customer;
- Production use of the Software in a live environment; or
- Failure to test, inspect, and report specific defects regarding the Software or any contract deliverable withing fourteen calendar days after delivery by Provider to Customer.

GL Simple Plan

GL Simple. GL Simple plans include the SaaS licensing and following the execution of setup services, certain support services. The annual cost of a GL Simple plan is based on the tier and number of named Customer employees with access to the Software whether or not such usage is concurrent as shown in the Pricing Addendum.

Tasks and Projects. Provider offers additional services to Customer in the form of Tasks or Projects.

- Projects – A project includes a request for a service with any of the following characteristics: 1) functionality requests that require coordination between Provider and a third-party; 2) functionality requests with three or more finite deliverables which must be delivered in a specific sequence to meet the Customer's business requirements; 3) functionality which may impact other aspects of the configured Software and therefore require a system test of an entire business process; or 4) service or functionality which requires the presence of a Provider employee onsite at Customer's place of business.
- Tasks – A task is a single request for a service except requests that are a project.
- At the Provider's sole discretion, Provider may establish and modify reasonable policies affecting the definition of services, the concurrency of item fulfillment, the definition of projects and tasks, and the request timing required to perform requests within a GL Simple plan.

GL Simple Plan Tiers. GL Simple plans are offered in three tiers: Standard, Professional and Enterprise. Provider shall provide "Tasks" and "Projects" specified for each tier as follows:

GL Simple Tier	Tasks for Services	Projects for Services
Standard	None included	None included
Professional	2 tasks/user/year or 24 tasks per year, whichever is greater; max 200	One concurrent project, no limit on total
Enterprise	4 tasks/user/year or 48 tasks per year, whichever is greater; max 400	Three concurrent projects, no limit on total

- GL Simple support fees apply to a maximum of 100 users. Additional users are licensed without charge.
- Customers purchasing the Standard tier must purchase GL Simple for a minimum of 25 named Customer employees or contractors with access to the Software.
- Customers purchasing the Professional tier must purchase GL Simple for a minimum of 8 named Customer employees or contractors with access to the Software.

- Customers purchasing the Enterprise tier must purchase GL Simple for a minimum of 3 named Customer employees or contractors with access to the Software.
- Customer may incrementally increase the number of Tasks or concurrent Projects in a GL Simple tier by paying an "Escalation Fee" in the amount applicable for each task or project pursuant to the Pricing Addendum.

Support Services. Provider offers GL Simple services as labeled in the first row in the GL Simple Service table below. The columns to the right of the service determine whether the service is offered to the GL Simple plan tier.

i. Services with a "$" mark are available to the tier through escalated Tasks and/or Projects only.

ii. Services with a check mark without the symbol "ŧ" are provided are provided without limitation.

iii. Services noted with the symbol "ŧ" utilize a Task or Project.

iv. Services without any mark for the tier are not available to that tier.

GL Simple Service	GL Simple Standard	GL Simple Professional	GL Simple Enterprise
Account Management			
Schedule Management	✓	✓	✓
Scope Management	✓	✓	✓
Risk Management	✓	✓	✓
Communication Management	✓	✓	✓
Client Engagement	✓	✓	✓
Project Initiation	✓	✓	✓
Change Management	✓	✓	✓
Critical Project Monitoring		✓	✓
Critical Task Prioritization		✓	✓
Technical Support			
Emergency Support (24 X 7 X 365)	✓ 3 hr response	✓ 1 hr response	✓ 15 min response
User Questions	✓	✓	✓
Design Review	✓	✓	✓
Developer Support	$	✓ ŧ	✓ ŧ
Hardware, Network and Security Support	$	✓ ŧ	✓ ŧ
Architecture and Best Practice Guidance		✓ ŧ	✓ ŧ

GL Simple Service	GL Simple Standard	GL Simple Professional	GL Simple Enterprise
Training and Documentation			
Design Training	✓	✓	✓
User Training	✓	✓	✓
Configuration and Developer Training Group Courses	$	✓ ŧ	✓ ŧ
Administrator Training	$	✓ ŧ	✓ ŧ
Administrator Documentation	✓	✓	✓
Software Patches and Releases for Core Software			
Software Releases	✓	✓	✓
Software Patches	✓	✓	✓
Software Release Installation	$	✓ ŧ	✓ ŧ
Software Patch Installation	✓	✓	✓
Warranty and Enhancements			
Lifetime Defect Correction	✓	✓	✓
Configuration and Customization	$	✓ ŧ	✓ ŧ
Security			
Compliance Audit (PCI, NIST, HIPAA)	✓ ŧ	✓ ŧ	✓ ŧ
Configuration Management (Tiered Environments: Dev, Sys, UAT and Prod)	✓	✓	✓
Security Assessment		✓ ŧ	✓ ŧ
Custom Network Isolation and Management		✓ ŧ	✓ ŧ
Multi-Factor Authentication			✓
Uptime Guarantee		98%	99.9%
Disaster Recovery			
Data Export Service	$	✓ ŧ	✓ ŧ
Automated Job and Interface Monitoring/Response			✓
Automated Site Monitoring/Response			✓
Backups	7 days	14 days	3 months
Disaster Recovery	within 14 days	within 3 days	within 1 hour
Mobile Inspections			
Mobile Inspection Service – per device	$	$	$

GL Simple Service	GL Simple Standard	GL Simple Professional	GL Simple Enterprise
Mobile Inspection Form Development		✓ ŧ	✓ ŧ
Mobile Inspection Dispatch Service		✓ ŧ	✓ ŧ
On-Premise Mobile Dispatch and Synchronization DB		✓ ŧ	✓ ŧ
Business Intelligence			
Power BI - Visual and interactive reports and dashboards for business analytics	$	✓ ŧ	✓ ŧ
Self-Service Administration (by Customer)			
User Security Administration	✓	✓	✓
Ticket and Project Tracking Portal	✓	✓	✓
Automated Task and Project Promotion Between Environments	✓	✓	✓
Business Rule Configuration	✓	✓	✓
Output Modification	✓	✓	✓
Access your data using alternative tools (e.g. SQL Server Management Studio)		✓ ŧ	✓ ŧ
Power BI Professional license for authoring and publishing			✓ ŧ

Service Level Agreement

Availability. The Software will be available to Customer twenty-four (24) hours a day, seven (7) days a week ("Uptime") less Excusable Downtime for at least the percentage of time indicated for the "Uptime Guarantee" corresponding to Customer's GL Simple plan tier in the GL Simple Service Table. Available means the software is generally accessible and usable, though certain functionalities may or may contain defects. Provider is not responsible for Customer's equipment or connectivity.

Downtime. For the purposes of this Contract, "Excusable Downtime" is defined as that period of time when the Licensed Services are not available to Customer due to scheduled network, hardware or service maintenance and/or upgrades. Except in cases of emergency, Customer shall be provided fourteen (14) business day advance notification of such maintenance and/or upgrade. In cases of emergency, Provider will use its best efforts to notify Customer of a planned Downtime as soon as practicable. Maintenance or upgrades shall not occur Monday through Friday, between the hours of 4:00 a.m. and 11:00 p.m. Eastern Time.

Penalties. Provider shall credit Customer applicable GL Simple charges in proportion of excess downtime in a month. For example, if the Uptime Guarantee is 98%, but the actual uptime was 95%, a credit equal to 3% of the GL Simple plan fees due for that month shall apply.

Warranty

Intellectual Warranties. Provider warrants that Provider has the full power and authority to grant the rights granted Customer hereunder with respect to the SaaS, and neither the license or use by Customer of the Software, as permitted under this License, will in any way constitute an infringement or other violation of any copyright, patent, trade secret, trademark or any other intellectual property right of any third party.

Government Mandates. In the event Software requires updating due to Federal, State statutory or regulatory requirements affecting Customer, the Provider's Software development department shall give its highest priority to the implementation of such updates, but Provider does not warrant that all such updates will be completed, or that any updates will be completed by a certain time. If Provider is unable to meet the deadline affecting the Customer, Customer and Provider will develop and agree to an implementation plan.

Setup and Services Warranty. During any GL Simple plan, Provider warrants that the Software configuration will perform in material conformity with Accepted specifications. Provider will cure all breaches of the foregoing warranty reported in GL Portal by Customer during a GL Simple plan.

Warranty and Remedy Limitations. EXCEPT AS EXPRESSLY SET FORTH IN THIS CONTRACT, PROVIDER MAKES NO OTHER WARRANTIES OF ANY KIND, AND EXPRESSLY DISCLAIMS ANY AND ALL OTHER WARRANTIES, EXPRESS AND IMPLIED, AS TO ANY MATTER WHATSOEVER, INCLUDING, WITHOUT LIMITATION, THE SUITABILITY OR THE CONDITION OF THE SOFTWARE, OR ITS FITNESS OR SAFETY FOR ANY PARTICULAR PURPOSE OR USE, OR AS TO ITS MERCHANTABILITY. PROVIDER MAKES NO WARRANTY REGARDING THE USABILITY OR CONVERTIBILITY OF ANY OF CUSTOMER'S DATA, THE SUITABILITY OF THE SOFTWARE FOR CUSTOMER'S NEEDS, OR ANY PERFORMANCE PROBLEM, OR OTHER MATTER ATTRIBUTABLE TO ANY USE OR MODIFICATION OF THE SOFTWARE, OR COMBINATION OF THE SOFTWARE WITH ANY OTHER SOFTWARE OR COMPUTER PROGRAM OR COMMUNICATIONS DEVICE, NOT EXPRESSLY AUTHORIZED BY PROVIDER IN WRITING. PROVIDER SHALL NOT BE LIABLE FOR INDIRECT, SPECIAL, INCIDENTAL OR CONSEQUENTIAL (INCLUDING LIABILITY IN TORT, STRICT OR OTHERWISE) DAMAGES ARISING DIRECTLY OR INDIRECTLY FROM THE SOFTWARE, THE USE, MISUSE, LOSS OF USE OR SALE THEREOF OR THE DELAY OR FAILURE OF DELIVERY OF THE SOFTWARE.

Miscellaneous

Amendments. This Contract may only be amended in a written agreement executed by authorized representatives of both parties hereto.

Assignments by Provider. Any and all rights and interests of Provider under this Contract may be assigned, either in whole or in part, without notice to Customer, and Customer agrees that its rights under this Contract are expressly subject and subordinate to any and all security interests which may now or hereafter be placed by Provider or its assigns upon the Software. All references in this subparagraph to assignment shall be deemed also to include any pledge, mortgage, transfer or other disposition. Subject always to the foregoing provisions of this section, this Contract shall inure to the benefit of, and shall be binding upon, the successors and assigns of the parties hereto and, where appropriate, their heirs, legatees and personal representatives. The Provider will provide Customer with no less than a ninety (90) calendar day notice of impending cessation of its business.

Notices. Any and all notices ("Notices") which either party hereto may desire to give to the other party hereunder shall be deemed to be duly given if and only if mailed by registered or certified mail, postage prepaid, addressed to the other party at its address as set forth below or at such other address as such party may designate to the other party in writing from time to time. Notification by any other means shall be considered a service request and a waiver of any related breach of contract dispute until such time as the party provides notice in accordance with this paragraph.

If to Provider: GL Suite, Inc.
PO Box 595
Kalispell, MT 59903

If to Customer: Mailing address identified by Customer
on Customer's public web site.

GL Suite, Inc.

By_____

Signature, Title *Date*

Customer

By_____

Signature, Title *Date*

SW1041 Software-Supplemental

Exhibit 1

Software Publishers		
Description	Maximum Cost + % Markup	% off List Price
GL Suite Software	3% year over year CPI increase	

Other Value Add Products and Services		
Description	Maximum Cost + % Markup	% off List Price
Third-Party Integrations		
All services and products are based on a value of one unit. E.g. per integration, per service, per application, etc.	$177.00 an hour	
3rd Party Authentication (OpenID, LDAP, Active Directory)	$3,540.00	
Docusign Integration	$3,540.00	
Board Meeting Management	$10,665.60 one-time	
Online Board Member	$3,540 one-time	
Online Complaint Management	$3,540 one-time	
Online Complainant	$3,540 one-time	
Online Respondent	$3,540 one-time	
Online Expert	$3,540 one-time	
3rd Party Integration (e.g., Online Retailer Portal for Background Checks)	$7,080.00	
Mobile & Field Services		
Mobile Inspections (DoForms)	$9,735 per inspection type	
Hosting		
Hybrid Hosting	$7,487.09 one-time	

Professional Services - Hourly Not-to-Exceed Rates		
Description	List Price	Discounted Hourly Rates
All services	$177.00	
Project Initiation (Includes Design Review/Acceptance)	$30,267 one-time	
Monthly Project Management Services	$61,950 per year	
Go-Live	$45,595 one-time	
Maintenance & Support		
Based on each licensed user and Tier	$2,651.43 per user per year for Standard	
	$5,137.05 per user per year for Professional	
	$8,948.19per user per year for Enterprise	

Testing & Training		
Testing		
System Testing	$2,655 per process	
User Acceptance Testing	$531.00 per process	
Test Scenario Creation	$1008.9 per business process	
Training		
Onsite Training	$7,080 / week	
Online Training	$2,832 / week	
Video Creation	$1,858.5 per video	
Training Validation	$2,124 per validation	
Configuration Training	$4,425 per training	
Hosting, Security, & Disaster Recovery		
Hosting (Setup)	$3,540 one-time	
Disaster Recovery (Setup)	$3,540 one-time	
Patches (Setup)	$3,540 one-time	
Security Assessment	$9,982.8 per assessment type	
Data Management & Integration		
Data Services		
Data Conversion	$26,550 per conversion	
Data Update Project/Cleanup	$11,505 / per project	
Data Exchange		
Data Interfaces (Flat File/Custom)	$10,620 per direction	
Reporting & Performance Management		
Key Performance Indicators	$3,540 per report	
Business Process Notifications/Alerts	$3,540 per report	
Staff Notifications/Alerts	$3,540 per report	
Staff Performance Reporting	$3,540 per report	
Business Performance Reporting	$3,540 per report	
Statistical Reports (Default to using KPIs)	$8,637.5 per report	
Complex Reports (Power BI, etc.)	$3,540 per report	
Communication & Document Management		
Online Communication Center (Portal)	$7,080 per portal	
Online Document Center (Notification/Collection)	$7,080 per process	
Scanner Integration	$4,425 per intergration	
Data Retention	$6,018 per process	
Online FOIA Management	$3,540 per process	
Core System Functionality		
User Portals & Dashboards		
Online Login and Dashboard - Individual	$7,664.1 per dashboard	
Online Dashboard [Other Entity]	$4,655.1 per dashboard	
Agency Management Dashboards	$8,850 per dashboard	

Business Process Dashboards	$8,850 per dashboard	
Staff Dashboards	$8,850 per dashboard	
Application & License Management		
Applications	$24,709.2 per application	
Renewals	$15,487.5 per renewal	
Name Change	$6,460.5 per change	
Address Change	$5,593.2 per change	
Change Process (Ownership, Service Modification)	$13,478.5 per process	
Background Checks	$7,965 per process	
Secure License/Wallet Cards (QR Codes)	$9,115.5 per report	
Digital License/Wallet Cards (Apple/Google Wallet)	$9,115.5 per license type	
Online Status Site (Status/Verification)	$7,080 per site	
Payments & Revenue Management		
Cash Receipts	$10,230.60	
Online Payments (Separated Payment Process)	$3,717 per process	
Compliance & Enforcement		
Inspections	$15,363.6 per process	
Complaints	$16,992 per process	
Compliance	$18,832.8 per process	
Investigations	$20,266.5 per process	
Corrective Action	$17,257.5 per process	
Continuing Education & Exams		
Continuing Education Auditing	$12,673.2 per process	
Continuing Education Hour Tracking	$11,115.6 per process	
Exams	$10,000.5 per process	

Attachment E-4: Offer of Value-Added Products and/or Services

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

As referenced in subsection 8.2.J, value-added products and/or services within scope of the Acquisition may be included in the Bid.

G.1. Bidder should provide information on value-add services that include but are not limited to product installation, maintenance and support, managed services, professional services and product training. Any Bidder offering product-related services must submit a description of those services and the related pricing in the Excel spreadsheet attached as Exhibit 1.

G.2. In addition to the Value Added services OMES directly associated with the sales of software, such as related maintenance and support agreements for new and previously purchased software, the Bidder would provide, at no additional cost, management services to include, but not be limited to, providing price quotes, tracking licenses (new and existing), management of licenses, monitoring volume levels and opportunities for cost savings, training, installation/de-installation/implementation support, and software advisement to OMES and/or OMES Customers.

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

Value-Added Products and Services

GL Solutions' implementation services are clearly defined in the Statement of Work (SOW), with all deliverables and functionalities itemized to ensure full transparency and no hidden costs. Our thorough requirements gathering process ensures the SOW encompasses all the agency's needs for a SaaS solution. If a service is not explicitly listed in the SOW, it is typically provided at no additional charge.

Our maintenance and support services are included in the expected yearly fee and cover:

- Customer service support
- User assistance and troubleshooting
- Free software upgrades and patches
- System usage guidance and optimization

To further control costs, GL Suite offers flexible licensing options, allowing agencies to cap active users at 150, even if there are 300 potential users, ensuring predictable maintenance and support costs.

Statement of Work (SOW)

AGENCY – GENERAL SCOPE

This Statement of Work (SOW) was prepared for the AGENCY (STATE) –by GL Suite, Inc. (dba GL Solutions), a Montana corporation (CONTRACTOR).

ACCEPTANCE PROCESS

CONTRACTOR and STATE agree to use GL Portal, an online, web-based project management system developed by CONTRACTOR to store project deliverables, communicate schedules, provide Acceptance of specifications and other deliverables, answer clarifications, report defects, and provide notifications. CONTRACTOR will issue STATE a unique login and access to GL Portal for each person authorized by STATE. STATE will authorize CONTRACTOR to grant GL Portal access only to STATE agents with authority to act on behalf of STATE. CONTRACTOR shall provide project management forms for acceptance, deliverable review reporting defects, etc. No other project management software or forms shall be used.

Any the following conditions constitute acceptance of a project document, specification, software, sub-deliverable or deliverable by STATE, in the form delivered by CONTRACTOR:

(a) Written acceptance by STATE;
(b) Production use of the Software in a live environment; or
(c) Failure to test, inspect and report specific defects regarding the Software or any contract deliverable within fourteen calendar days after delivery by CONTRACTOR to STATE.

SPECIFICATIONS

For each deliverable, CONTRACTOR shall create specifications and other documentation, such as project management documents, training, and software documentation, to support this sow. CONTRACTOR shall submit specifications and documentation to STATE for acceptance using GL Portal. CONTRACTOR shall specify which Deliverables requirements are met by the specification or documentation. STATE shall review the specification or documentation to determine whether

the document, if developed per the specification, fulfills the SOW requirement specified by CONTRACTOR. STATE shall respond to CONTRACTOR's request for approval by accepting the submitted specification or documentation; rejecting the specification or documentation, or; not responding to the acceptance request within fourteen calendar days. Not responding to the acceptance request constitutes STATE's acceptance of the specification or documentation.

If the specification or documentation does not conform to the SOW, STATE shall notify CONTRACTOR using GL Portal and forms provided by CONTRACTOR specifying the specific contract exceptions which cause the specification or documentation to be unacceptable. All such deficiencies within the specification or documentation must be noted during STATE's initial review of the specification or documentation. CONTRACTOR shall correct the deficiencies and resubmit the specification or documentation within seven calendar days from the receipt of the rejection. STATE shall have seven calendar days to re-inspect, test and reevaluate the resubmitted specification or documentation to determine whether deficiencies initially noted are corrected. Additional cycles may be added until all deficiencies initially noted are corrected. During any re-inspection by STATE, the STATE shall avoid reporting new deficiencies not reported during the initial rejection of the specification or documentation. Acceptance of a specification or documentation constitutes acceptance that CONTRACTOR's development and implementation of the software according to the specification or documentation satisfies CONTRACTOR's performance obligations with respect to the corresponding SOW contract requirement identified. Acceptance of a software deliverable constitutes acceptance that the Software performs as specified.

DELIVERABLES

PRICING

The cost for each deliverable is listed in Exhibit B – Payment Milestones. The STATE and CONTRACTOR shall agree to a start and finish dates in accordance with Deliverable 2: Project Management Plan.

DELIVERABLE 1: PROJECT KICKOFF MEETING

1. Description:

CONTRACTOR shall coordinate with STATE to schedule a Kickoff Meeting in person or via tele-conference with the core project team. CONTRACTOR shall lead the meeting. The Kickoff Meeting must facilitate the introduction of CONTRACTOR and STATE core project team members, and develop understanding and awareness of project objectives, scope, governance, schedule, and project risks and issues.

a. CONTRACTOR shall collaborate with STATE and provide agenda to attendees in advance of the meeting.
b. CONTRACTOR and STATE shall facilitate the meeting, and discuss and further define, at a minimum, the following:
    i. Effective project communication
    ii. Project vision, background, purpose, and objectives
    iii. Project governance structure, and project roles and responsibilities
    iv. Approach to creating the Project Management Plan
    v. Initial risk assessment

2. Expectations of STATE:

a. STATE shall coordinate the logistics and co-facilitate the Kickoff Meeting.
b. STATE's Project Sponsor and project team members shall participate in the Kickoff Meeting.

3. Completion Date:

CONTRACTOR shall start work with STATE within a mutually agreed upon timeframe after the signing of this Contract to schedule the Kickoff Meeting.

4. Acceptance Criteria:

For the acceptance of this deliverable to occur, the Kickoff Meeting results in:

a. Facilitation of Kickoff Meeting using a clearly defined agenda.
b. An introduction of CONTRACTOR and STATE resources assigned to the project.

c. Review of project purpose, business objectives, project governance structure, roles and responsibilities, and scope.
d. Discussion of communications approach and structure.
e. Discussion of known project risks and issues.

DELIVERABLE 2: PROJECT MANAGEMENT PLAN

1. Description:
   a. CONTRACTOR shall participate, contribute, and collaborate with STATE to develop a baseline Project Management Plan that provides, at a minimum, the following:
      i. Management plans to control cost, schedule, scope, and quality
      ii. Integrated change control process
      iii. A human resource management plan including:
         1. The project resources required for both STATE and CONTRACTOR
         2. Staff assigned and their location and schedule
         3. Resource allocation percentage by role
      iv. Communication management plan, including a plan for generation, documentation, storage, transmission, and disposal of project information
      v. Risk management plan to ensure risks are identified, planned for, analyzed, communicated, and acted upon effectively
      vi. Issue management plan
      vii. A procurement management plan.
   b. CONTRACTOR shall provide a Quality Management Plan to include the methodology for maintaining quality of the code and workmanship, and related subcontractor(s) activities where appropriate.
   c. CONTRACTOR shall develop, contribute, and collaborate with STATE on a detailed project schedule with fixed deadlines. The project schedule format will be mutually agreed-upon, and the project schedule will follow STATE best practices, including:
      i. A work breakdown structure
      ii. Schedule, including tasks, activities, activity duration, sequencing, and dependencies
      iii. Completion date of each task
      iv. Milestones, including entrance and exit criteria for specific milestones
      v. Both STATE and CONTRACTOR tasks are included
      vi. Project tasks are broken down into timeframes that can be reasonably managed – STATE encourages a maximum task length of approximately 80 hours/two (2) weeks
      vii. Project tasks have appropriate resources assigned with appropriate and reasonable allocation
      viii. Schedule has appropriate working times and incorporates STATE and CONTRACTOR holidays and nonworking times.
2. Expectations of STATE:
   a. The STATE's project manager will have primary responsibility for the management of the project.
3. Completion Date:

CONTRACTOR shall start work with STATE within a mutually agreed upon timeframe after the signing of this Contract to create the Project Management Plan.

4. Acceptance Criteria:

For the acceptance of this deliverable to occur, CONTRACTOR shall provide a Project Management Plan which adheres to the principles of the Project Management Body of Knowledge and includes the following:

a. A mutually agreed-upon detailed baseline scope and schedule for the project
b. Management plans to control scope, schedule, cost, and quality, including variance
c. The governance structure for the project
d. Quality assurance and quality control plans

e. Integrated change control process
f. Human resources management plan
g. Communication management plan
h. Risk management plan
i. Issue management plan

DELIVERABLE 3: GAP ANALYSIS

1. Description:
   CONTRACTOR to review, analyze, and confirm understanding of system functionality, business practices, interfaces, configurations, and customizations.
   a. CONTRACTOR shall lead the analysis effort.
   b. CONTRACTOR shall demonstrate how system's core functionality meets the requirements as defined in the Request for Proposal.
   c. CONTRACTOR shall identify and document gaps between the system's out-of-the-box functionality and STATE's requirements, and business processes and practices.
   d. CONTRACTOR shall identify any gaps that require system configuration or customization changes.
   e. CONTRACTOR shall identify any gaps that require system customization beyond the Request for Proposal response.
   f. CONTRACTOR shall collaborate with STATE to document agreed-upon changes to the system that may be needed as a result of the review and confirmed understanding.
2. Expectations of STATE:
   a. STATE staff shall actively participate in work and analysis sessions.
   b. STATE shall collaborate with CONTRACTOR to confirm requirements and gap analysis.
3. Acceptance Criteria:
   For the acceptance of this deliverable to occur, the following criteria must be met:
   a. Gap Analysis Matrix:
      i. To be presented in a traceability matrix that lists requirements and identifies which requirements can be met out-of-the-box, which need configuration, and which need customizations in accordance with CONTRACTOR's Request for Proposal response.
      ii. Specifies each applicable component (program and database changes), the core product components that are impacted for each component of customization/configuration, and what components shall be retested for deployment and ongoing maintenance.
      iii. Includes a descriptive statement on how CONTRACTOR will meet each requirement.
      iv. Includes which requirements that, through understanding and analysis, cannot be accomplished without additional efforts, including a recommended approach to resolve the gap and CONTRACTOR's level of effort.
      v. Includes detailed system interface requirements documented in sufficient detail for use as a basis for customization/configuration design activities.
   b. Documentation on operational workflows in sufficient detail for use as a basis for customization/configuration design activities.
   c. Architectural Design
      i. During the Analysis Phase, the contractor shall submit an Architectural Design for the proposed solution that conforms to the State's standards. The architectural analysis will be reviewed by the State's architects. The Architectural Analysis document must include:
         1. A narrative and graphical description of the following:
         2. Web Layer
         3. Middleware Layer
         4. Database Layer
         5. Storage
         6. Network Security

d. If applicable, a list and description of exceptions highlighting how the proposed solution does not adhere to the State's IT environment, and how the offeror plans to address the exceptions.
e. If applicable, a list and description of assumptions that were taken into consideration when producing the Architectural Design.
f. If applicable, Procurement and Acquisition Plan that must include:
    i. List and description of required hardware. The list should specify a minimum necessary configuration and a recommended configuration, including any usage assumption, load balancing factors, or performance metrics.
    ii. List and description of required software. The list should clearly indicate whether the software is to be provided by the STATE or contractor.

DELIVERABLE 4: SYSTEM CONFIGURATION – Licensing Design

1. Description:

CONTRACTOR shall design the system according to the requirements established during the Business Process Requirements gathering for applications, amendments, exceptions and renewals, and decisions made throughout the design effort.

a. CONTRACTOR shall lead the design effort.
b. CONTRACTOR shall confirm and reach design decisions in collaboration with STATE.
c. CONTRACTOR shall design components in alignment with requirements and decisions confirmed or identified in the Gap Analysis deliverable and demonstrate completed designs and reporting capabilities to STATE.

2. Expectations of STATE:
    a. STATE shall make necessary design decisions.
    b. STATE shall provide requested information and documentation as needed to design the system.
3. Acceptance Criteria:

For the acceptance of this deliverable to occur, the follow criteria must be met:

a. System designed according to the specifications and requirements documented in the Gap Analysis deliverable, and according to the information provided by STATE.
b. Successful demonstration of the design and approval of all design documents.

DELIVERABLE 5: SYSTEM CONFIGURATION – Licensing Configuration

1. Description:

CONTRACTOR shall configure the system according to the requirements established during the Business Process Design, and decisions made throughout the design effort.

a. CONTRACTOR shall lead the configuration effort.
b. CONTRACTOR shall confirm and reach configuration decisions in collaboration with STATE.
c. CONTRACTOR shall configure components in alignment with requirements and decisions confirmed or identified in the Gap Analysis deliverable and demonstrate completed configuration and reporting capabilities to STATE.

2. Expectations of STATE:
    a. STATE shall make necessary configuration decisions.
    b. STATE shall provide requested information and documentation as needed to configure the system.
3. Acceptance Criteria:

For the acceptance of this deliverable to occur, the follow criteria must be met:

a. System configured according to the specifications and requirements documented in the Gap Analysis deliverable, and according to the information provided by STATE.

DELIVERABLE 6: SYSTEM CONFIGURATION – Licensing Business Testing

1. Description:

CONTRACTOR shall test the system according to the requirements established during the Business Process Requirements gathering, and decisions made throughout the design effort.

a. CONTRACTOR shall lead the test effort.
b. CONTRACTOR shall test components in alignment with requirements and decisions confirmed or identified in the Gap Analysis deliverable and demonstrate completed tests scripts to STATE.

2. Expectations of STATE:
   a. STATE shall make necessary test decisions.
   b. STATE shall provide requested information and documentation as needed to test the system.
3. Acceptance Criteria:

For the acceptance of this deliverable to occur, the follow criteria must be met:

a. System tested according to the specifications and requirements documented in the Gap Analysis deliverable, and according to the information provided by STATE.
a.

1. Acceptance Criteria:

For the acceptance of this deliverable to occur, the follow criteria must be met:

a. System tested according to the specifications and requirements documented in the Gap Analysis deliverable, and according to the information provided by STATE.

DELIVERABLE 7: SYSTEM CONFIGURATION – Other Processes Design

1. Description:
   a. CONTRACTOR shall design the system according to the requirements established during the Business Process Requirements gathering, and decisions made throughout the design effort for the following business process areas:
      a. Surveys
      b. Financial Management
      c. Enforcement
      d. Background Checks
      e. Professional Development
      f. Provider Portal
      g. Public Compliance Data
   b. CONTRACTOR shall lead the design effort.
   c. CONTRACTOR shall confirm and reach design decisions in collaboration with STATE.
   d. CONTRACTOR shall design components in alignment with requirements and decisions confirmed or identified in the Gap Analysis deliverable and demonstrate completed designs and reporting capabilities to STATE.
2. Expectations of STATE:
   a. STATE shall make necessary design decisions.
   b. STATE shall provide requested information and documentation as needed to design the system.
3. Acceptance Criteria:

For the acceptance of this deliverable to occur, the follow criteria must be met:

a. System configured according to the specifications and requirements documented in the Gap Analysis deliverable, and according to the information provided by STATE.
b. Successful demonstration of the design and approval of all design documents.

DELIVERABLE 8: SYSTEM CONFIGURATION – Other Processes Configuration

1. Description:
   a. CONTRACTOR shall configure the system according to the requirements established during the Business Process Design, and decisions made throughout the design effort.
   b. CONTRACTOR shall lead the configuration effort.
   c. CONTRACTOR shall confirm and reach configuration decisions in collaboration with STATE.
   d. CONTRACTOR shall configure components in alignment with requirements and decisions confirmed or identified in the Gap Analysis deliverable and demonstrate completed configuration and reporting capabilities to STATE.
2. Expectations of STATE:
   a. STATE shall make necessary configuration decisions.
   b. STATE shall provide requested information and documentation as needed to configure the system.
3. Acceptance Criteria:

For the acceptance of this deliverable to occur, the follow criteria must be met:

a. System configured according to the specifications and requirements documented in the Gap Analysis deliverable, and according to the information provided by STATE.

DELIVERABLE 9: SYSTEM CONFIGURATION – Other Processes Business Testing

1. Description:
   a. CONTRACTOR shall test the system according to the requirements established during the Business Process Requirements gathering, and decisions made throughout the design effort.
   b. CONTRACTOR shall lead the test effort.
   c. CONTRACTOR shall test components in alignment with requirements and decisions confirmed or identified in the Gap Analysis deliverable and demonstrate completed tests scripts to STATE.
2. Expectations of STATE:
   a. STATE shall make necessary test decisions.
   b. STATE shall provide requested information and documentation as needed to test the system.
3. Acceptance Criteria:

For the acceptance of this deliverable to occur, the follow criteria must be met:

a. System tested according to the specifications and requirements documented in the Gap Analysis deliverable, and according to the information provided by STATE.

DELIVERABLE 10: TEST MANAGEMENT PLAN

1. Description:
   a. CONTRACTOR shall create a Test Management Plan with STATE support that outlines the overall testing approach for how the CONTRACTOR and the STATE shall verify the product meets the requirements.
   b. CONTRACTOR shall lead the test planning effort.
   c. CONTRACTOR shall conduct working session(s) with STATE to review and finalize the Test Management Plan prior to start of testing.
   d. CONTRACTOR shall coordinate with STATE to schedule all testing activities.

e. CONTRACTOR shall train STATE to conduct user acceptance tests and report results.
f. CONTRACTOR shall participate, contribute, and collaborate with STATE in development of user acceptance test cases.
g. CONTRACTOR shall perform all integrated system testing on the testing environment, while User Acceptance Testing will be performed on the staging environment (no testing will be conducted on the production environment)
h. CONTRACTOR shall repeat the test life cycle when a failure occurs at any stage of testing (e.g., a failure in User Acceptance Testing that necessitates a code change will require the component to go back through Unit Testing, Integration Testing, Security Testing, and Performance Testing)
i. CONTRACTOR shall refine the test documents, procedures, test scripts, and test cases throughout development and through full Acceptance Testing to reflect the as-built design and current requirements.

1. Expectations of STATE:

a. STATE shall actively participate in planning sessions.
b. STATE shall provide support and make any necessary decisions.
c. STATE shall review and provide feedback to CONTRACTOR.

2. Acceptance Criteria:

For the acceptance of this deliverable to occur, The Test Plan must, at a minimum, include the following areas:

a. Test philosophy including objectives, required levels or types of testing, and basic strategy for developing, testing and release of major subsystems/components.
b. Procedures and approach to test script and test case creation and review to ensure the testing will satisfy specific objectives and demonstrate that the requirements are met.
c. Detailed test plans for the following:
    i. Integration Testing
    ii. Security Testing
    iii. Performance Testing
    iv. User Acceptance Testing
a. Detailed description of each test required to ensure all system components and interfaces comply with requirements and specifications.
b. Test cases that include testing criteria and benchmarks for each requirement as defined in the requirements traceability matrix.
c. Automated test procedures and test scripts.
d. Agreed-upon high-level testing schedule in accordance with the project schedule, which has all testing completing prior to deployment.
e. Procedures and approach to ensure that each phase of the testing is complete, and how formal reports or debriefings will be conducted for each phase of testing including an overview of processes that will be used by the CONTRACTOR for releasing testing results.
f. Process and procedures for tracking and reporting results, variances, and defects.
g. Procedures and approach to defect resolution that describes the tracking and management of all problems discovered during any testing phase and in production.
h. Approach to define tested workload types (performance testing) and test data.
i. Overview of testing facilities, environment and specific testing tools to be used.
j. State resources required for testing during the development life cycle for each testing area, including testing assignments, responsibilities, and necessary skillsets.
k. Configuration management of the test environment, including instructions for modifying any desktop configuration settings.
l. Pilot site checklist, logistics, and approach.
m. Executive summary

DELIVERABLE 11: USER ACCEPTANCE TESTING

1. Description:
   a. CONTRACTOR shall support STATE testing efforts, make fixes, and remediate testing issues during STATE's user acceptance testing and performance testing efforts.
   b. CONTRACTOR shall demonstrate system functionality prior to commencement of acceptance testing by STATE.
   c. CONTRACTOR shall review and consult on STATE's test scripts to ensure scripts are accurate and thorough.
   d. CONTRACTOR shall provide template to document testing results.
   e. CONTRACTOR shall provide testing support to identify, troubleshoot, and resolve issues.
   f. CONTRACTOR shall provide technical assistance with testing, verification, and classification of issues.
   g. CONTRACTOR shall correct validated issues based on priorities and severities defined by STATE.
   h. CONTRACTOR shall work with STATE to ensure the development environment is correctly copied into the testing environment and all users have appropriate access.
2. Expectations of STATE:
   a. STATE shall ensure STATE testing occurs according to the project schedule, and test results and resolutions are documented.
   b. STATE shall create test scripts according to STATE-defined workflows and processes.
   c. STATE shall provide adequate and knowledgeable system users to participate in testing.
   d. STATE shall perform user acceptance testing.
   e. STATE shall perform application performance testing.
   f. STATE shall document any identified issues, assign priority and severity, and provide results to CONTRACTOR for troubleshooting.
3. Acceptance Criteria:

For the acceptance of this deliverable to occur, the following criteria must be met:

   a. Completion of system testing and system functionality demonstration by CONTRACTOR.
   b. Completion of user acceptance testing and performance testing support by CONTRACTOR.
   c. Testing issues are resolved.
   d. Testing approach and execution is in alignment with the Testing Management Plan.

DELIVERABLE 12: TRAINING MANAGEMENT PLAN

1. Description:

CONTRACTOR shall create a Training Management Plan. The plan will address training approaches, courses to be delivered, course instructors, overall objectives and competencies, training schedule, evaluation, and required resources.

   a. CONTRACTOR shall lead the training planning effort.
   b. CONTRACTOR shall create a Training Management Plan with STATE support.
   c. CONTRACTOR shall conduct working session(s) with STATE to review and finalize the Training Management Plan prior to start of training.
   d. CONTRACTOR shall coordinate with STATE to schedule all training activities.
   e. CONTRACTOR's strategy shall provide training early in the project to allow the training goals to be implemented throughout the project life cycle.
   f. CONTRACTOR shall include active participation of STATE to create the knowledge transfer plan during all phases of the application development life cycle, in the following roles: business analyst, technical analyst, architect, developer, user interface designer, and quality assurance.
2. Expectations of STATE:
   a. STATE shall actively participate in planning sessions.
   b. STATE shall provide support and make any necessary decisions.
   c. STATE shall review and provide feedback to CONTRACTOR.

d. STATE will define training effectiveness criteria.

3. Acceptance Criteria:

For the acceptance of this deliverable to occur, the Training Management Plan must include:

a. Description of training session(s).
b. Identification of roles and responsibilities, intended audience, training objectives, specific plan for training business and technical personnel, and evaluation methods.
c. Tasks and resources necessary to complete the training effort and identify tools and documentation that will be necessary to support proposed effort.
d. Types of training, the specific courses and course materials, the training approach for both business and technical personnel, and how training effectiveness will be measured and addressed.
e. Deliverables to support initial and ongoing training, including user manuals, system manuals, and online help and training materials for technical/non-technical personnel.
f. Knowledge transfer to enable state personnel to operate, maintain, configure, and modify the system; to include operation of the software development lifecycle processes and tools, supporting infrastructure, and security as agreed between STATE and CONTRACTOR
g. Metrics for tracking progress in achieving training and knowledge transfer objectives.
h. Method to report progress of training and knowledge transfer activities.
i. Approach to bring authorized user to appropriate level of understanding with the system.
j. Identification of agreed-upon high-level timing and approach for training.
k. Executive summary.

DELIVERABLE 13: TRAINING

1. Description:

CONTRACTOR to conduct end user and administrator system training to groups of staff based on roles and responsibilities. Groups identified to date are: STATE staff, and information technology staff. Training shall include a train-the-trainer approach for select users to ensure sustainability.

a. CONTRACTOR shall provide up-to-date and accurate process guides in Software, links to reference materials relevant to process steps, user manuals and any other training materials that can be given to training participants and future STATE staff.
b. CONTRACTOR shall provide a training syllabus to STATE for review and feedback in advance of the training.
c. CONTRACTOR shall provide qualified instructors.
d. CONTRACTOR shall conduct training sessions at a location and time mutually agreed-upon With STATE. This will likely include multiple locations.
e. CONTRACTOR shall collaborate with STATE to create training documentation for:
    i. STATE staff
    ii. System administration
    iii. System support and development (help desk) – trouble shooting and quick reference guides
f. CONTRACTOR shall collaborate with STATE to provide training modules (traditional and e-learning) that can be delivered to all end users specified by STATE.
g. CONTRACTOR shall train all end users with a combination of computer-based training/online training and train-the-trainer.

2. Expectations of STATE:

a. STATE shall review and provide feedback on the training syllabus to verify that desired areas are part of the training.
b. STATE shall make assigned trainees available for the scheduled training sessions.
c. STATE shall provide training facilities and equipment.
d. STATE shall develop and conduct survey of training participants to verify training was effective.

3. Acceptance Criteria:

For the acceptance of this deliverable to occur, the following criteria must be met:

a. Delivery of instructor and user manuals and training materials in electronic and paper formats.
b. Delivery of training in accordance with the syllabus.
c. STATE survey concludes that CONTRACTOR training was effective.
d. STATE has been prepared for system administration, version maintenance, and daily system application maintenance responsibilities.
e. Training approach and execution is in alignment with the Training Management Plan.

DELIVERABLE 14: IMPLEMENTATION AND TRANSITION PLAN

1. Description:
   a. CONTRACTOR shall collaborate with STATE to create an Implementation and Transition Plan to manage the implementation of the product and transition the product and work from the project structure to maintenance
   b. CONTRACTOR shall lead the planning effort.
   c. CONTRACTOR shall create an Implementation and Transition plan with STATE support.
   d. CONTRACTOR shall conduct working session(s) with STATE to review and finalize the Implementation and Transition Plan prior to any implementation or transition work.
   e. CONTRACTOR will collaborate with STATE during the first year after implementation for change and release management.
   f. CONTRACTOR will work with STATE to address warranty defect resolution.
2. Expectations of STATE:
   a. STATE shall actively participate in planning sessions.
   b. STATE shall provide support and make any necessary decisions.
   c. STATE shall review and provide feedback to CONTRACTOR.
3. Acceptance Criteria:

For acceptance of this deliverable to occur, the Implementation and Transition Plan must include:

   a. Implementation strategy
      i. The implementation strategy must deliver a System that includes a significant portion of the technical infrastructure early in the schedule without compromising the quality or inherent security of the System, along with validating the design and architecture
      ii. The implementation strategy must expose technically challenging area of the project as soon as possible.
      iii. The implementation strategy must deliver customized functionality to the State in incremental pieces that are in logical business application sequence.
   b. Learned and corrective actions from pilot test sites
   c. Implementation resources and tasks
   d. Implementation entry and exit criteria, and go/no go decision requirements
   e. Implementation contingency plan
   f. Information on technical challenges
   g. Capacity plan that includes:
      i. System workload assumptions
      ii. A description of how capacity and capacity requirements were calculated, including all formulas and calculations used in capacity planning for the State
      iii. A description of how capacity requirements will be met
      iv. A description of how capacity issues will be managed for all components of the State project
      v. A description of how capacity utilization will be monitored, and capacity thresholds will be established
      vi. A description of corrective and escalation processes that will be used in the event any capacity thresholds are reached
   h. Operational recovery plan that includes:
      i. Areas of the most susceptible to failure or disaster that would result in downtime

ii. Recommendations for System recovery processes, or steps to take in the event of a downtime event
iii. Recommendations for the State on how to comprehensively and effectively mitigate the risk of a downtime event
iv. Recommendations for securing System components during a period of emergency operation
v. Disaster Recovery requirements must include networking for disaster recovery datacenter access

i. Business migration strategy
j. Implementation go live checklist
k. Transition resources and tasks
l. Production release plan that includes:
i. CONTRACTOR processes for moving product into maintenance and ensuring ongoing support
ii. Transition resources and tasks
iii. Deployment schedule
m. Executive summary

DELIVERABLE 15: IMPLEMENTATION

1. Description:
   a. CONTRACTOR shall support implementation of the final system.
   b. CONTRACTOR shall participate, contribute, and collaborate with STATE for implementation preparations.
   c. CONTRACTOR shall make any fixes required in a timely manner to implement the system as approved in the Acceptance Testing deliverable
   d. CONTRACTOR shall provide technical support to STATE as needed for implementation efforts.
2. Expectations of STATE:
   a. STATE shall participate, contribute, and collaborate with CONTRACTOR for implementation preparations.
   b. STATE shall monitor the implementation and notify CONTRACTOR of any issues.
3. Acceptance Criteria:

For the acceptance of this deliverable to occur, the following criteria must be met:

a. CONTRACTOR support during implementation.
b. System go live.
c. All testing must be completed.

DELIVERABLE 16: POST-IMPLEMENTATION REPORT AND CLOSEOUT MEETING

1. Description:
   a. CONTRACTOR shall participate, contribute, and collaborate with STATE to develop a Post-Implementation Report that provides, at a minimum, the following:
      i. Key metrics related to schedule, cost, scope, and quality
      ii. Discussion of how well the business objectives were met
      iii. Lessons learned from the project
      iv. Success stories from the project
2. Expectations of STATE:
   a. STATE shall finalize agenda and send agenda to invitees.
   b. STATE shall lead the Closeout Meeting.
   c. STATE shall be responsible for the Post-Implementation Report.
3. Acceptance Criteria:

For the acceptance of this deliverable to occur, CONTRACTOR shall participate in the Closeout Meeting and provide content to STATE for the Post-Implementation Report:

a. Key project metrics related to schedule, cost, scope, and quality.
b. Comprehensive lessons learned valuable to future projects.
c. Success stories from the project.

DELIVERABLE 17: DATA CONVERSION PLAN

Description:

CONTRACTOR shall participate, contribute, and collaborate with STATE to create a Data Conversion Plan. The plan is intended to address the overall approach that will be followed for the data conversion effort and will be a subordinate plan to the Implementation Plan deliverable. The plan will define methodology, strategies, required competencies, tools, templates, quality standards, data cleansing, and data discrepancy resolution strategies.

a. CONTRACTOR shall lead the data conversion planning effort.
b. CONTRACTOR shall create a Data Conversion Plan that will outline the approach to convert the agreed-upon data by collaborating with and gathering input from STATE.
c. CONTRACTOR shall be responsible for the final product.

1. Expectations of STATE:
   a. STATE shall actively participate in planning sessions.
   b. STATE shall provide support and make any necessary decisions.
   c. STATE shall review and provide feedback to CONTRACTOR.
   d. STATE shall work with CONTRACTOR to develop approaches planned for STATE's data cleansing efforts.
2. Acceptance Criteria:

For the acceptance of this deliverable to occur, the Data Conversion Plan must include:

a. Data conversion methodologies and strategies to be used including a repeatable extract, transform, and load (ETL) process.
b. Details regarding the tools and templates to be used.
c. Outline of strategies and actions planned to resolve data discrepancies and mapping issues, which may include customizations and data cleansing.
d. Outline of the testing approach and methodology, including defined success criteria and quality standards.
e. Executive summary.

DELIVERABLE 18: DATA CONVERSION DESIGN

1. Description:

CONTRACTOR shall design the overall data conversion approach to convert data from the legacy system.

a. CONTRACTOR shall lead the data conversion design effort.
b. CONTRACTOR shall provide all necessary data conversion documentation to STATE.
c. CONTRACTOR shall provide example conversion files to STATE to assist STATE in generating successful data conversion files.

2. Expectations of STATE:
   a. STATE shall assist CONTRACTOR's review and design of data elements applicable to data conversion.
   b. STATE shall provide necessary and relevant resources to make design decisions.
3. Acceptance Criteria:

For the acceptance of this deliverable to occur, the Data Conversion Design must include:

a. Proposed system context and workflow to be accomplished with the customizations.
b. Documentation of development and how the development meets the requirements outlined in the Gap Analysis deliverable.

DELIVERABLE 19: DATA CONVERSION VALIDATION

1. Description:
   a. CONTRACTOR and STATE shall validate the data conversion effort by reviewing the data loaded into the user acceptance testing environment and making any fixes to the system or data conversion process to ensure data transfers accurately and completely.

b. CONTRACTOR shall initially validate the data conversion into the user acceptance testing environment and resolve any issues prior to STATE data conversion validation efforts.
c. CONTRACTOR shall support STATE's effort to identify and resolve any issues with the data conversion prior to Go Live.

2. Expectations of STATE:
   a. STATE shall test the data conversion into the user acceptance testing environment.
   b. STATE shall identify, document, trouble-shoot, and work with CONTRACTOR to resolve any data conversion issues.
3. Acceptance Criteria:

For the acceptance of this deliverable to occur, the following criteria must be met:

a. Successful upload of accurate and complete data extract from the legacy system to the user acceptance testing environment.
b. CONTRACTOR review of STATE-documented user acceptance testing issues and recommendations for file extract changes to remediate issues.
c. Subsequent load(s) of STATE-provided revised data extracts to confirm resolution of issues, or documented alternatives to resolution.

DELIVERABLE 20: INTERFACE DESIGN

1. Description:

CONTRACTOR shall design the interface from the system to or from the following systems:

1. GIS Realtime geocoding) (bidirectional)
2. KBI (bidirectional)
3. Child Abuse Registry (bidirectional)
4. Interface is a web service, real time. (bidirectional)
5. Online payments (bidirectional)
6. Workforce Registry (bidirectional)

, including any configurations or customizations required to support the integration of the interface with the system.

a. CONTRACTOR shall lead the interface design effort.
b. CONTRACTOR shall develop a high-level conceptual design for the interface.
c. CONTRACTOR shall collaborate with STATE to finalize design.

2. Expectations of STATE:
   a. STATE shall review conceptual designs and provide feedback and clarification as requested.
   b. STATE shall provide technical resources and subject matter experts who will assist and collaborate with CONTRACTOR during the design process.
3. Acceptance Criteria:

For the acceptance of this deliverable to occur, the Interface Design must include:

a. Design documentation for the interface.
b. Document detailing any customizations to support the integration between the systems.

DELIVERABLE 21: INTERFACE DEVELOPMENT AND RELEASE

1. Description:
   a. CONTRACTOR shall build and release the interface per the requirements defined during analysis and the Interface Design deliverable.
   b. CONTRACTOR shall complete development of the interface.
   c. CONTRACTOR shall conduct thorough technical testing of the interface as identified in the Testing Management Plan.
   d. CONTRACTOR shall resolve issues identified with the interface.
   e. CONTRACTOR shall install and validate the interface in preparation for user acceptance testing.
2. Expectations of STATE:

a. STATE shall provide technical resources and an environment for testing of the interface.
b. STATE shall collaborate with CONTRACTOR to validate CONTRACTOR installed interface correctly.
c. STATE shall validate interface is ready for user acceptance testing.

3. Acceptance Criteria:

For the acceptance of this deliverable to occur, the following criteria must be met:

a. Release of the interface to STATE's user acceptance testing environment.
b. Completion of CONTRACTOR's testing effort and remediation of any deficiencies.

DELIVERABLE 22: MOBILE FORM DESIGN

1. Description:

CONTRACTOR shall design all interfaces from the system to identified third parties including any configurations or customizations required to support the integration of the mobile inspections with the system.

a. CONTRACTOR shall lead the mobile form design effort.
b. CONTRACTOR shall develop a high-level conceptual design for the mobile forms
c. CONTRACTOR shall collaborate with STATE to finalize design.

2. Expectations of STATE:

a. STATE shall review conceptual designs and provide feedback and clarification as requested.
b. STATE shall provide technical resources and subject matter experts who will assist and collaborate with CONTRACTOR during the design process.

3. Acceptance Criteria:

For the acceptance of this deliverable to occur, the Mobile Form Design must include:

a. Design documentation for the mobile forms
b. Document detailing any customizations to support the integration between the systems.

DELIVERABLE 23: MOBILE FORM DEVELOPMENT AND RELEASE

1. Description:

a. CONTRACTOR shall build and release design all interfaces from the system to identified third parties including any configurations or customizations required to support the integration of the mobile inspections with the system, per the requirements defined during analysis and the Mobile Form Design deliverable.
b. CONTRACTOR shall complete development of the mobile forms.
c. CONTRACTOR shall conduct thorough technical testing of the mobile forms as identified in the Testing Management Plan.
d. CONTRACTOR shall resolve issues identified with the mobile forms.
e. CONTRACTOR shall install and validate the mobile forms in preparation for user acceptance testing.

2. Expectations of STATE:

a. STATE shall provide technical resources and an environment for testing of the mobile forms.
b. STATE shall collaborate with CONTRACTOR to validate CONTRACTOR installed mobile forms correctly.
c. STATE shall validate mobile forms is ready for user acceptance testing.

3. Acceptance Criteria:

For the acceptance of this deliverable to occur, the following criteria must be met:

a. Release of the mobile forms to STATE's user acceptance testing environment.
b. Completion of CONTRACTOR's testing effort and remediation of any deficiencies.

DELIVERABLE 24: System Acceptance

1. Description:

a. CONTRACTOR shall resolve agency reported defects following system go live.
b. CONTRACTOR shall participate, contribute, and collaborate with STATE to plan, prioritize and address issues.
c. CONTRACTOR shall make any fixes required in a timely manner to support the system as approved in the Acceptance Testing deliverable

2. Expectations of STATE:
   a. STATE shall plan, prioritize and clarify system issues.
   b. STATE shall report, test and reject or accept CONTRACTOR corrections.
3. Acceptance Criteria:

For the acceptance of this deliverable to occur, the following criteria must be met:

   a. CONTRACTOR correction of all reported defects that cause a significant loss of functionality or performance resulting in some users being unable to perform normal functions without a convenient workaround (e.g., severity 1 and 2 defects).

DELIVERABLE 25: GL Simple Standard Hosting, Support and Warranty

1. Description:
   a. CONTRACTOR shall provide ongoing services as defined in end-user license agreement as GL Simple-Standard SLA for the period beginning from the first production usage of the system for a period of 1 year. In the event of a multi-phased go-live, the deliverable shall not be invoiced until completion of the final go-live, even though the support plan commenced as of the first production usages of the system.
2. Expectations of STATE:
   a. See end user license agreement.
3. Acceptance Criteria:

   a. Production usage of the software.

PROJECT DELIVERABLE PAYMENT SCHEUDLE

The following table defines all payment points. After completion of the Project Management Plan, this table will be amended with all dates filled in.

Deliverable	Part #	Description	GLS Price
1	GLS-SaaSInstall-23	Project Kickoff Meeting	[redacted]
2	GLS-SaaSInstall-23	Project Management Plan	[redacted]
3	GLS-SaaSInstall-23	Gap Analysis	[redacted]
4	GLS-SaaSInstall-23	System Configuration - Licensing Design	[redacted]
5	GLS-SaaSInstall-23	System Configuration - Licensing Configuration	[redacted]
6	GLS-SaaSInstall-23	System Configuration - Licensing Process Testing	[redacted]
7	GLS-SaaSInstall-23	System Configuration - Other Processes Design	[redacted]
8	GLS-SaaSInstall-23	System Configuration - Other Processes Configuration	[redacted]
9	GLS-SaaSInstall-23	System Configuration - Other Processes Process Testing	[redacted]
10	GLS-SaaSInstall-23	Test Management Plan	[redacted]
11	GLS-SaaSInstall-23	User Acceptance Testing	[redacted]
12	GLS-SaaSInstall-23	Training Management Plan	[redacted]
13	GLS-SaaSInstall-23	Training	[redacted]
14	GLS-SaaSInstall-23	Implementation and Transition Plan	[redacted]
15	GLS-SaaSInstall-23	Implementation	[redacted]
16	GLS-SaaSInstall-23	Post Implementation Report	[redacted]
17	GLS-SaaSInstall-23	Data Conversion Plan	[redacted]
18	GLS-SaaSInstall-23	Data Conversion Design	[redacted]
19	GLS-SaaSInstall-23	Data Conversion Validation	[redacted]
20	GLS-SaaSInstall-23	Interface Design	[redacted]
21	GLS-SaaSInstall-23	Interface Development and Release	[redacted]
22	GLS-SaaSInstall-23	Mobile Form Design	[redacted]

23	GLS-SaaSInstall-23	Mobile Form Development and Release	[redacted]
24	GLS-SaaSInstall-23	System Acceptance	[redacted]
25	GLS-SaaSInstall-23	GL Simple Standard Hosting, Support and Warranty	[redacted]
		TOTAL CONTRACT PRICE	[redacted]