



**STATE OF OKLAHOMA STATEWIDE CONTRACT WITH INTEGRATED HEALTH
RESOURCES DBA BEHAVIORAL HEALTH LINK**

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 Integrated Health Resources dba Behavioral Health Link (“Supplier”) and is effective as of the date of last signature to this Contract. The initial term of the Contract shall be for 1 year with four (4) one-year options to renew.

Purpose

The State is awarding this Contract to Supplier for the provision of software, training, pre-sales assistance, documentation, installation, maintenance, support, configuration, customization, and license agreement administration and services, as a SaaS, either cloud-based or on premises, to support State agencies and other eligible Oklahoma Interlocal Entities, as is more particularly described in certain Contract Documents. Supplier submitted a proposal containing exceptions to the Solicitation, 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 with Exhibits, Attachment A;
 - 2.2. General Terms, Attachment B;
 - 2.3. Statewide Contract Terms, Attachment C;
 - 2.4. Information Technology Terms, Attachment D;
 - 2.5. Additional Terms, Attachment E1;
 - 2.6. Master Terms, Attachment E2;
 - 2.7. Pricing, Attachment E3;
 - 2.8. Value Add Offerings, Attachment E4;
 - 2.9. Third-Party Terms, Attachment E5;
 - 2.10. Service Level Agreement, Attachment E6; and

- 2.11. Statement of Work, Attachment E7.
3. The parties additionally agree:
- 3.1. Except for the portions agreed by the State and Supplier to be held confidential and 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. All representations made by Supplier in response to the Solicitation regarding specifications and requirements are incorporated herein by reference into this Contract.
- 3.3. Regarding the requirement for the Supplier to have security and privacy liability insurance in the amount of \$5,000,000 per occurrence under Section 8 of Attachment B, Supplier agrees to increase coverage limits to \$5,000,000 per occurrence upon execution of an order form and prior to commencing work under such order form. Supplier shall provide proof of increased coverage to Customer and any applicable state authorities before work commencement.
- 3.4. To the extent any term or condition in any Contract Document, including via a hyperlink or uniform resource locator, conflicts with an applicable Oklahoma and/or United States law or regulation, such term or condition is void and unenforceable. By executing any Contract Document which contains a conflicting term or condition, the State or Customer makes no representation or warranty regarding the enforceability of such term or condition and the State or Customer does not waive the applicable Oklahoma and/or United States law or regulation which conflicts with the term or condition.
4. 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:**

**INTEGRATED HEALTH RESOURCES
DBA BEHAVIORAL HEALTH LINK**

By:  Dan Cronin (Sep 22, 2025 08:28:35 CDT)

By:  Charles Browning (Sep 19, 2025 17:01:12 EDT)

Name: Dan Cronin

Name: Charles Browning

Title: Chief Information Officer/Chief Transformation Officer

Title: CEO

Date: Sep 22, 2025

Date: Sep 19, 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.**

Exhibit #2 Requirements
SW1041 Software Value Added Reseller
EVENT NO. 00000640

The Office of Management and Enterprise Services (OMES), Central Purchasing on behalf of Information Services is soliciting proposals from qualified Suppliers for software and services to support State agencies and other eligible Oklahoma Interlocal Entities.

The State of Oklahoma’s objectives are to reduce current expenses with price protected offers while optimizing services to participating agencies and Interlocal Entities. In addition, the State is seeking the highest level of customer service.

The State of Oklahoma seeks Supplier(s) able to 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.

OMES wishes to encourage Bidders to submit for all categories of software including business specific, law enforcement, emergency preparedness, productivity, and security products. This list is not exhaustive of all software that Oklahoma may have interest in.

Services will be obtained on a time and materials basis.

Excluded Software

This listing is subject to change during the life of the contract.

Oklahoma List of EXCLUDED SOFTWARE *			
Oracle	Microsoft	IBM	Hyland

*Software is excluded if it is available at the same or better pricing from a current Statewide Contract with the software publisher.

Number of Awards

Oklahoma will determine whether it will award Contracts to one or more of the selected Bidders based on a Best Value determination and reasonably expects to award to multiple Suppliers.

Adding Contractors After Initial Statewide Contract Award

If, over the life of the Contract, Oklahoma determines that additional Suppliers over and above those initially selected should be added, these may first be drawn from companies that responded to this Solicitation but were not among those initially selected. If necessary to meet the requirements of Oklahoma, the Solicitation may be reopened to obtain additional bids.

Contract Duration

The initial term of this Contract will one year with 4 options to renew.

Estimated Value of the Contract (Including All Options to Renew)

Oklahoma makes no guarantee that any goods or services will be purchased from any Contract resulting from this Solicitation. Any estimates or past procurement volumes referenced in this Solicitation are included only for the convenience of Bidders and are not to be relied upon as any indication of future purchase levels.

The historical annual sales under the contract to be awarded as a result of this RFP are:

Oklahoma FY21	\$22,196,972.00
Oklahoma FY22	\$19,028,378.00

Estimated 5-year contract value	\$103,063,375.00
---------------------------------	------------------

Minimum Requirements

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.

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.

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.

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.
- Billing Information outlines what information is provided in billing and how it is delivered.
- Documentation outlines how detailed documents of services that are provided to entities on an on-going basis to include services by location and account information can be obtained.
- 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.
- Account Team and Support Provisions outline the Suppliers capabilities of providing world class support and account service.
- Statement of Work Template provides an outline of the how the Supplier will provide and execute project-based requirements.

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.

References

Provide a total of three (3) references from government and/or private companies of comparable size and spend.

References provided shall contain a contact person with full contact information (i.e., current employer, telephone number, mailing address, and e-mail address). OMES is not responsible for references that do not respond.

Value-Added Services

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

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.

Pricing

Pricing should be provided in Excel format using Exhibit 1 for each software publisher you are proposing to provide under this contract.

Pricing should be provided as a discount off-list price, or a cost-plus mark-up model.

Professional Services categories should be identified by types and should be provided as an hourly not-to-exceed cost.

Price increases, as subject to review at annual renewal, shall be capped at 3% per year.

Deliverables

- Point by point response to bid requirements
- References
- Documentation
- Pricing response
- Security Assessment, if chosen for award

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 debaring 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 OAC** means the Oklahoma Administrative Code.
- 4.14 OMES** means the Office of Management and Enterprise Services.

- 4.15 Solicitation** means the document inviting Bids for the Acquisition referenced in the Contract and any amendments thereto.
- 4.16 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.
- 4.17 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.
- 4.18 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.
- 4.19 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.

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 \$2,000,000 per occurrence;
- C.** Automobile Liability Insurance with limits of liability of not less than \$2,000,000 combined single limit each accident;
- D.** [Omitted];
- 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, and Americans with Disabilities Act of 1990;
 - 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 or, for services cease all use of the services upon written request, in exchange for a refund of the price paid for such returned goods or in the case of services, a pro rata refund of amounts paid in advance for use of services, including Supplier's SaaS services, after the termination date (provided, that for any custom Work Product, Supplier will refund all fees paid to develop the custom Work Product, including but not limited to any prepaid or advance amounts and any fees paid toward the customization of the Work Product up to the point of the termination date, as set forth in the applicable SOW), 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 \(oklahoma.gov\)](https://oklahoma.gov/content/dam/ok/en/omes/documents/InfoSecPPG.pdf). 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. Notwithstanding the foregoing, enhancements, modifications, updates, or additions to Supplier's existing Software-as-a-Service (SaaS) platform or proprietary software solutions that are developed to serve multiple customers or that become part of Supplier's core platform functionality shall remain the exclusive property of Supplier, regardless of whether such enhancements were requested by the State. The State shall receive the benefit of such enhancements through its licensed use of the platform but shall not obtain ownership rights therein. 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.

For the avoidance of doubt, "customization" as used in this section refers to bespoke software development created exclusively for the State's use and does not include enhancements, updates, or modifications to Supplier's existing multi-tenant SaaS platform, proprietary software products,

or core platform functionality, which shall remain the property of Supplier even if requested by the State.

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 are 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 that constitutes bespoke custom development exclusively for Customer 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. This provision shall not apply to Supplier's existing SaaS platform, proprietary software, or enhancements thereto as defined in Section 11. 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 bespoke custom 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 bespoke custom Work Product.

- 12.3** Supplier hereby irrevocably and forever waives, and agrees never to assert, any Moral Rights in or to the bespoke custom Work Product developed exclusively for Customer 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. This waiver does not apply to Supplier's existing SaaS platform, proprietary software, or enhancements thereto.
- 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 bespoke custom Work Product developed exclusively for Customer, generated or developed by Supplier or furnished by Customer to Supplier, including all materials embodying the bespoke custom Work Product, any Customer confidential information and Intellectual Property Rights in such bespoke custom Work Product, regardless of whether complete or incomplete. This provision shall not apply to Supplier's proprietary SaaS platform, related documentation, or any materials that are part of Supplier's standard service offerings. 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 bespoke custom Work Product.

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.

- 12.7** To the extent that any Third Party Intellectual Property is embodied or reflected in the Work Product or is necessary to provide services, Supplier shall obtain from the applicable third party for the Customer's benefit, an irrevocable, perpetual, non-exclusive, worldwide, royalty-free license, solely for Customer's internal business purposes; likewise, with respect to any Supplier Intellectual Property embodied or reflected in the Work Product or necessary to provide services, Supplier grants to Customer an irrevocable, perpetual, non-exclusive, worldwide, royalty-free license, solely for the Customer's internal business purposes. Each such license shall allow the applicable Customer to (i) use, copy, modify, display, perform (by any means), transmit and prepare derivative works of any Third Party Intellectual Property or Supplier Intellectual Property embodied in or delivered to Customer in conjunction with the Work Product and (ii) authorize others to do any or all of the foregoing. Supplier agrees to notify Customer on delivery of the Work Product or services if such materials include any Third Party Intellectual Property. The foregoing license includes the right to sublicense third parties, solely for the purpose of engaging such third parties to assist or carry out Customer's internal business use of the Work Product. Except for the preceding license, all rights in Supplier Intellectual Property remain in Supplier. On request, Supplier shall provide Customer with documentation indicating a third party's written approval for Supplier to use any Third Party Intellectual Property that may be embodied or reflected in the Work Product.
- 12.8** 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.
- 12.9** To the extent not inconsistent with Customer's rights in the bespoke custom 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 bespoke custom Work Product is utilized, and no Intellectual Property Rights of Customer therein are infringed by such competitive materials. For the avoidance of doubt, this provision shall not restrict Supplier's right to enhance, modify, or develop its existing SaaS platform or proprietary software solutions for any customers, including competitors of Customer. To the extent that Supplier wishes to use the bespoke custom 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.
- 12.10** 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.
- 12.11 SaaS Platform Clarification** Notwithstanding any other provision in this Section 12, all references to "Work Product" in this section shall be interpreted to mean only bespoke custom development created exclusively for Customer and shall not include: (a) Supplier's existing SaaS platform or proprietary software; (b) enhancements, modifications, or updates to such platform or software; (c) any functionality that serves

or could serve multiple customers; or (d) any intellectual property that forms part of Supplier's core business offerings. Customer acknowledges that Supplier's SaaS platform and related enhancements remain Supplier's intellectual property as set forth in Section 11.

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 through the Hosting environment any material that contains software viruses, malware or other surreptitious code designed to interrupt, destroy or limit the functionality of any computer software or hardware or telecommunications equipment or circumvent any “copy-protected” devices, or any other harmful or disruptive program.

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 access 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 E1 - Additional Bidders Terms

MASTER SOFTWARE AS A SERVICE AGREEMENT

This **MASTER SOFTWARE AS A SERVICE AGREEMENT** (“Agreement”) is effective as [REDACTED], 2025 (“Effective Date”) and is by and between **INTEGRATED HEALTH RESOURCES, LLC d/b/a Behavioral Health Link**, a Georgia limited liability company (“BHL”), and [REDACTED] (“Customer”). This Agreement consists of the terms and conditions set forth herein; the initial Order Form attached hereto as Attachment E7 (Statement of Work) and any subsequent Order Forms that reference this Agreement; the Service Level Agreement attached as Attachment E6 and the Business Associate Agreement and breach notification form attached as Exhibit A and Exhibit A-1 respectively. In consideration of the promises and the mutual obligations of the parties set forth herein, and for other good and valuable consideration, the adequacy and sufficiency of which are hereby acknowledged, the parties agree as follows:

- 1. License to Use Application and Receive Maintenance and Other Services.** During the Term set forth on Attachment E7, Customer hereby subscribes for the use of the Application(s) identified on the applicable Order Form (the initial Order Form is attached hereto as Attachment E7) (“Application(s)”) for the authorized scope of use set forth on the applicable Order Form, which includes ongoing maintenance, and support services (“Maintenance Services”). BHL will also provide professional services (which may include training, implementation, or customization) (“Professional Services”) as set forth in a Statement of Work (“SOW”) signed by both parties. During the Term, BHL hereby grants to Customer a non- exclusive, non-transferable, non-assignable, term license to access and use the Application(s) for the authorized scope of use set forth on the applicable Order solely in connection with Customer's support of its own mental health call center and/or mobile crisis operations, all in accordance with the terms set forth herein. Upon the Customer's written request and at no additional cost, BHL will provide Customer with access to export Customer's data via a mutually agreed format for up to 30 days after the effective date of termination, if the termination is termination by convenience. If the termination is termination for cause, then BHL will provide Customer with access to export Customer's data via a mutually agreed format for up to 60 days. The export will be in .csv format or another mutually agreed format. At the end of the 60-day period, BHL will permanently delete or permanently remove the Customer's data from BHL's platform.
- 2. Reservation of Rights.** Customer acknowledges that BHL's grant of a term subscription to use the Application(s) within the limited scope of use set forth in Section 1 above is only a limited license to access and use the Application(s) and is not a sale or other transfer of rights in the Application(s). BHL reserves all rights not expressly granted to Customer by this Agreement. Customer may not, except as permitted in this Section 2, copy, modify, adapt, publicly display, publicly perform, or create derivative works of the Application(s) or Services or any portion thereof or associated documentation, or remove any copyright or other proprietary rights notices thereon. Customer shall not itself, and shall not permit its Users (as defined herein) or any other party to, directly or indirectly, in whole or in part, sell, re-sell, assign, sublicense, distribute, lease, make available as a service bureau, disclose, divulge or otherwise transfer, make available or allow any third parties any right or access to the Application(s); disassemble, decompile, decrypt, or reverse engineer, or otherwise attempt to discover or replicate source code or database architecture/configuration for the Application(s); or alter, modify, or prepare derivative works based on the Application(s) or the results of the Professional Services. Notwithstanding the foregoing, BHL acknowledges and agrees that that Customer may transfer licenses to a successor agency or other subdivision of the state resulting from a reorganization imposed by the state legislature. Customer



acknowledges and agrees that BHL owns and retains all rights existing from time to time in any jurisdiction under copyright law, patent law, moral rights law, trade secret law, confidential information law, trademark law, unfair competition law or other similar rights (“Proprietary Rights”) in the Application(s), Services, and documentation, any training materials and any copies, modifications, adaptations, derivative works, and enhancements thereof, by whomever produced. Notwithstanding the foregoing, if a statement of work expressly identifies specific Work product as prepared specifically for Customer on a “work for hire” basis, Customer will own the Proprietary Rights in such custom Work Product as set forth in the applicable statement of work.

Application User(s) include employees of the Customer, independent contractors engaged by the Customer, or entities contracting with the Customer for services specified in the applicable order form. Application User(s) also include customers, suppliers, members of the general public, and other entities with whom the Customer may find it necessary or desirable to process or communicate electronically in pursuit of its business content.

Authorized Scope of Use of the Application(s). Customer may only access and use the Application(s) for the scope of use authorized on the applicable Order Form(s). The Application(s) (including any changes thereto made by or on behalf of Customer) may be used only for, by or on behalf of the Customer and only to process its own data and the data of its affiliates and agency controlled entities. There shall be no other use of the Application(s) without prior written consent of BHL. If the actual usage of the services or resources exceeds the amounts or limits contemplated under this Agreement, such excess usage may be used solely as a basis for discussion and negotiation of any renewal or extension of this Agreement, including the potential adjustment of usage limits. However, no additional charges related to such excess usage shall be automatically applied under this Agreement. Any charges or fees related to usage beyond the agreed scope must be discussed in good faith and mutually agreed to in writing by both parties prior to being invoiced or becoming payable. In the absence of such prior written agreement, no additional usage charges shall be deemed due or enforceable.

Each employee, contractor or other representative of Customer that will access and/or use the Application(s) (hereinafter, a “User”) must have his or her own login credentials as a User (“Login Information”). Customer will designate an administrator (“Account Administrator”) who will grant and manage access to individual employees or other end users. The Account Administrator will have access to the settings for its end users’ accounts and will have the option to create roles with specific permissions and assign those roles to users as the customer sees fit. Upon account creation by the Account Administrator, end users will be able to use the provided user account and may change account settings or profile information by logging into their accounts through BHL Platform’s website. BHL may make changes to account settings upon Customer request. Customer will be solely responsible for all actions of any individual who accesses the Application(s) using the Login Information. Customer shall

(i) require Users to utilize strong form, alpha numeric Login Information and change such Login Information not less frequently than every sixty (60) days, (ii) protect the confidentiality of all Login Information, (iii) notify BHL of any breach of the confidentiality of any Login Information, and (iv) notify BHL if any individual who knows the Login Information leaves the employment of Customer, is no longer authorized to use the Login Information or misuses the Login Information.

[Omitted]

- 3. Third-Party Services.** Certain of the Services allow Customer to connect to various third-party services via API or other integrations (“Linked Services”) and may contain links to other third-party websites and services. BHL is providing these connections to Customer only as a convenience, and the inclusion of any connection or link does not imply endorsement by BHL of the Linked Services, website or policies, or any association with its operators. Customer acknowledges that access to and use of such Linked Services is subject to the independent terms and conditions of such Linked Services. BHL is not responsible or liable for the contents or behavior of any Linked Services, including without limitation, any link contained in a Linked Service (or the policies or procedures of that Linked Service), or any changes or updates to a Linked Service (or the policies or procedures of that Linked Service). To the extent that Customer elects, at its discretion, to use Linked Services in connection with the Services, Customer agrees that it shall be responsible for such use. BHL shall not access or transmit Customer data to any Linked Services except to the extent a) necessary to enable the integration as expressly initiated or configured by Customer; b) subject to prior written agreement or informed consent by Customer; or, c) as otherwise required by law. BHL shall use commercially reasonable efforts to ensure that any integration with Linked Services includes appropriate data protection and security measures and shall promptly notify Customer of any known material issue affecting the confidentiality, integrity, or availability of Customer data transmitted to or received from a Linked Service. Customer agrees that BHL shall not be liable for any damages, losses or claims arising from the acts or omissions of Linked Services; provided, however, that BHL shall remain liable for any breach of its obligations under this Agreement, including any unauthorized disclosure of Customer data caused by BHL’s gross negligence or willful misconduct. Nothing in this Section shall be construed as a waiver of Customer’s rights under data protection laws or any applicable law governing the protection of confidential or proprietary information.
- 4. Technical Support Services.** Customer will respond to questions and complaints from its end users or third parties relating to use of the Services. If Customer is unable to resolve such support issue, then Customer may escalate such issue to BHL’s Customer Support Department (customersupport@ihrcorp.com). Customer agrees that it will have no more than three (3) employees who will be authorized to contact BHL and its help desk for support.
- 5. Fees and Payment.**

a. *General.* The annual subscription fee for use of the Application(s) is due in advance on or before the first day of each year of the Initial Term (“Subscription Fees”). Customer will pay BHL for Professional Services billed in accordance with the terms of the applicable SOW. Payment of BHL’s invoices is due within thirty (30) days of Customer’s receipt of the invoice but shall not be deemed late or accrue interest until after Net 45 days. If BHL fails to receive timely payment of any fees, it may, in its sole discretion, suspend or terminate Customer’s account.

Disputes for any charges for the Services must be made in writing to BHL within thirty (30) days of the date of the invoice by BHL or date of charge, as applicable. Failure to provide a written statement explaining in reasonable detail the reasons for disputing the charge(s) within such time period irrevocably waives any objection and further recourse regarding such charges. Written statements disputing charges must be emailed to BHL’s Customer Support Department at accounts-payable@ihrcorp.com.

b. *Changes to Fees.* Upon expiration of the Initial Term or any Renewal Term (each as defined in Section 9 below), BHL may change the Subscription Fees and set forth in the Order Form upon written notice of such change and approval by Customer with a signed Change Order not later than forty-five (45) days prior to the end of the Initial Term or annual renewal term.

c. *[Omitted].*

d. *[Omitted].*

6. Representations, Warranties, Covenants, and Disclaimer

a. **Mutual.** Each party represents and warrants to the other party that: (i) it has the power, authority and legal right to make, deliver and perform the obligations set forth herein and to its knowledge, no other agreement conflicts with the terms set forth herein; and (ii) the execution of this Agreement has been duly authorized and executed and is, or upon delivery will be, a legal, valid and binding obligation enforceable in accordance with its terms. Furthermore, BHL warrants that its provision of, and Customer warrants that its use of, the Application(s) and Services is in compliance with applicable law and regulations, including federal, state and local statutes, ordinances and regulations, including tax and license fees of federal, state and local governmental agencies or bodies.

b. **BHL.** BHL will use commercially reasonable efforts to maintain the Application(s) in a manner which minimizes errors and interruptions in the Services.

c. **Customer.** Customer will maintain sufficient Internet access, network connectivity, and power to enable use of the Services. Customer represents to BHL that it owns or has right to use Customer Data as contemplated herein; and will use the Application(s) and Services in compliance with applicable law.

7. **Indemnification.** BHL shall indemnify and hold harmless Customer from any claims made or any suits or proceedings brought against Customer arising out of an allegation that any or all of the Application(s) or results of the Professional Services furnished hereunder infringe a patent, trademark, and/or copyright of the United States, if BHL is notified promptly by Customer in writing and given information, assistance at BHL's expense, and BHL shall pay all damages and costs finally awarded therein against Customer. In the event the Application(s) in such a suit is held to infringe and the use of the Application(s) or results of the Professional Services is enjoined, or in the case of a settlement as referred to above, BHL shall have the option, at its own expense, to procure for Customer the right to continue using the Application(s); or to replace same with a non-infringing comparable product; or to modify same so it becomes non-infringing; or to terminate this Agreement and refund to Customer the amounts paid in advance for the remaining subscription period after the termination date. BHL shall not be liable to Customer if any infringement claim is based upon use of the Application(s) in any manner which does not comply with the terms of this Agreement.

8. **Term.** This Agreement shall be effective as of the Effective Date and shall remain in effect for initial term set forth on Exhibit A (the "Initial Term"), unless earlier terminated by either party as described herein. This Agreement will automatically renew for successive terms of the same length as the initial term (each a "Renewal Term") (the Initial Term and all Renewal Terms are the "Term") at BHL's standard rates in effect at the time of such renewal, unless either party delivers the other written notice of non-renewal at least sixty (60) prior to expiration of the then-current term at the rates in effect in the immediately preceding year of the Term, subject to BHL's right to increase its rates pursuant to Section



6(b) hereof.

9. **Protected Health Information: Compliance with Laws.** The parties acknowledge and agree that the Application(s) will process Customer's "Protected Health Information," as defined in the Health Insurance Portability and Accountability Act of 1996, as amended and supplemented ("HIPAA"), and the substance abuse, diagnosis, treatment, or referral records protected by 42 C.F.R. Part 2 ("Part

2”), and the data processed by the Application(s) may be subject to regulation or protection under other state and federal laws and regulations. **BHL agrees that its access to and the processing and use of all Customer Protected Health Information will be solely for purposes of fulfilling its obligations under this Agreement, and such access and use will be subject to the terms and conditions of the Business Associate Agreement attached hereto as Exhibit C, and otherwise in compliance with all applicable laws.** BHL shall not cause or permit any Individually Identifiable Health Information to be processed in any manner or for any purpose other than the performance of its obligations hereunder and in compliance with the restrictions set forth in this Agreement and all applicable laws, including but not limited to HIPAA, Part 2 and the HITECH Act. As between Customer and BHL, Customer is and shall remain the sole and exclusive owner of all right, title and interest in and to all Personal Health Information included therein. The parties shall also comply with all laws that apply to the parties’ performance of their obligations under this Agreement. In the event either party reasonably determines that any provision of this Agreement may be inconsistent with any applicable law or regulation, the parties agree to negotiate in good faith to modify such provision.

10. General.

a. *Relationship of Parties.* The relationship of the parties is that of independent contractors, and this Agreement shall not be construed to create any employment relationship, partnership, joint venture, or agency relationship or to authorize any party to enter into any commitment or agreement binding on the other party.

b. *Publicity.* Upon the written approval of Customer, BHL may have a royalty-free, limited, nontransferable (except in connection with an assignment of this Agreement), nonexclusive license during the term of this Agreement to use and display Customer’s name and publicly available branding in customer lists, advertising materials, trade show materials and other literature identifying BHL’s customers. Such approval terminates upon the termination of this Agreement and may be terminated immediately upon Customer giving BHL written notice of the termination of such approval. Upon such termination, BHL will promptly cease using and remove Customer’s name and publicly available branding in customer lists, advertising materials, trade show materials and other literature identifying BHL’s customers.

c. *Equitable Remedies.* Customer agrees that any threatened or actual breach of BHL's Proprietary Rights by Customer shall constitute immediate, irreparable harm to BHL for which monetary damages is an inadequate remedy and for which equitable remedies may be awarded by a court of competent jurisdiction. Nothing contained herein shall limit either party's right to any remedies at law, including the recovery of damages for breach of this Agreement.

- d. *Assignment.* Customer's rights under this Agreement may not be assigned, sublicensed, or otherwise transferred voluntarily whether by operation of law (e.g., in connection with a merger) or otherwise, without BHL's prior written consent.
- e. *Binding Effect.* This Agreement shall be binding upon, and inure to the benefit of the parties, their legal representatives, successors, and assigns as permitted by this Agreement.
- f. *Force Majeure.* Except for any payment obligations hereunder, neither party shall be liable for failure to perform any of its respective obligations hereunder if such failure is caused by an event outside its reasonable control, including but not limited to, an act of God, war, or natural disaster.
- g. *No Waiver.* No delay or failure in exercising any right hereunder and no partial or single exercise thereof shall be deemed to constitute a waiver of such right or any other rights hereunder. No consent to a breach of any express or implied term of this Agreement shall constitute a consent to any prior or subsequent breach.
- h. *Amendments.* No modifications, waivers, additions, or amendments to this Agreement shall be effective unless made in writing as an addendum to this Agreement and signed by handwritten or certified electronic signature by duly authorized representatives of the parties.
- i. *Counterparts.* This Agreement may be executed in one or more counterparts, each of which shall for all purposes be deemed to be an original and all of which shall constitute the same instrument.
- j. *Severability.* If any provision hereof is declared invalid by a court of competent jurisdiction, such provision shall be ineffective only to the extent of such invalidity, so that the remainder of that provision and all remaining provisions of this Agreement shall be valid and enforceable to the fullest extent permitted by applicable law.
- k. *Construction.* Should any provision of this Agreement require judicial interpretation, the parties agree that the court interpreting or construing the same shall not apply a presumption that this Agreement shall be more strictly construed against one party than the other.
- l. *Notices.* All notices required to be given hereunder shall be given in writing and shall be delivered either by hand, by certified mail with proper postage affixed thereto, or by facsimile (with confirmation copy sent by certified mail) addressed to the signatory at the address set forth on the first page, or such other person and address as may be designated from time to time in writing. All such communications shall be deemed received by the other party upon the earlier of actual receipt or actual delivery.
- m. *Governing Law; Venue.* This Agreement shall be governed by and construed in accordance with the laws of the State of Oklahoma, without regard to its rules regarding conflict of laws. The parties agree that this Agreement does not involve the sale of goods and that neither the Uniform Commercial Code as enacted in Oklahoma, nor any similar statutes concerning the sale of goods, nor the United Nations Convention on the International Sale of Goods shall apply to this Agreement.

(SIGNATURE PAGE FOLLOWS)

IN WITNESS WHEREOF, the parties have caused their authorized representatives to execute this Agreement effective as of the Effective Date.

Integrated Health Resources, LLC
d/b/a Behavioral Health Link:

[Customer]

By: _____

By: _____

Name: _____

Name: _____

Title: _____

Title: _____

Date: _____

Date: _____

Customer Billing Information:

Customer Contact: _____

Title: _____

Phone Number: _____

E-mail: _____

Billing Address: _____

Exhibit A

BUSINESS ASSOCIATE AGREEMENT

THIS BUSINESS ASSOCIATE AGREEMENT (this “Agreement”) is entered into this [REDACTED] by and between, whose address [REDACTED] (hereinafter referred to as “Covered Entity”) and **INTEGRATED HEALTH RESOURCES, LLC** whose address is 1201 Peachtree Street NE, Build 400, Suite 1215, Atlanta, GA 30303 (hereinafter referred to as “Business Associate”).

RECITALS

A. Covered Entity and Business Associate have entered or may enter into a separate contract(s) (the “Contract”) pursuant to which Business Associate provides or will be providing certain services to Covered Entity;

B. In the course of performing services under the Contract, Business Associate may be provided with access to Protected Health Information (as defined in Section III. of this Agreement), which may include Patient Identifying Information, as defined under 42 CFR Part 2); and

C. Covered Entity and Business Associate desire to enter into this Agreement to ensure compliance with all applicable federal and state laws, including but not limited to the Health Insurance Portability and Accountability Act of 1996 and its implementing regulations (45 CFR Part 160 and Part 164) as amended by the Health Information Technology for Economic and Clinical Health Act (the “HITECH Act”) (collectively, “HIPAA”); the Drug Abuse Prevention, Treatment and Rehabilitation Act, as amended and its implementing regulations (42 CFR Part 2).

NOW THEREFORE, in consideration of granting Business Associate access to Protected Health Information and continuing the business relationship pursuant to the Contract, and for other good and valuable consideration, the receipt and sufficiency of which is hereby acknowledged, the parties hereby agree as follows:

I. RECITALS.

The Recitals set forth above are incorporated by reference herein and made a part hereof.

II. PRIOR AGREEMENTS.

This Agreement supersedes and replaces any and all business associate agreements Covered Entity and Business Associates may have entered into prior to the date hereof.

III. **DEFINITIONS.**

- A. **Breach.** “Breach” shall have the same meaning as the term “breach” in 45 CFR 164.402.
- B. **Designated Record Set.** “Designated Record Set” shall have the same meaning as the term “designated record set” in 45 CFR 164.501.
- C. **Electronic PHI.** “Electronic PHI” shall have the same meaning as the term “Electronic Protected Health Information” in 45 CFR 160.103.
- D. **Individual.** “Individual” shall have the same meaning as the term “individual” in 45 CFR 160.103 and shall include a person who qualifies as a personal representative in accordance with 45 CFR 164.502(g).
- E. **Privacy Rule.** “Privacy Rule” shall mean the Standards for Privacy of Individually Identifiable Health Information at 45 CFR Part 160 and Part 164, Subparts A and E.
- F. **Protected Health Information.** “Protected Health Information” or “PHI” shall have the same meaning as the term “Protected Health Information” in 45 CFR 160.103, limited to the information created or received by Business Associate from or on behalf of Covered Entity.
- G. **Required by Law.** “Required By Law” shall have the same meaning as the term “required by law” in 45 CFR 164.103.
- H. **Secretary.** “Secretary” shall mean the Secretary of the Department of Health and Human Services or his/her designee.
- I. **Security Incident.** “Security Incident” shall have the same meaning as the term “security incident” in 45 CFR 164.304.
- J. **Security Rule.** “Security Rule” shall mean 45 CFR Part 160 and Subparts A and C of Part 164.
- K. **Substance Abuse Records Rule.** “Substance Abuse Records Rule” shall mean 42 CFR Part 2.
- L. **Unsecured Protected Health Information.** “Unsecured Protected Health Information” or “Unsecured PHI” shall mean Protected Health Information that is not secured through the use of a technology or methodology specified by the Secretary in guidance or as otherwise defined in the §13402(h) of the HITECH Act.

Terms used, but not otherwise defined in this Agreement, shall have the same meaning as those terms in the Privacy Rule, Security Rule and the HITECH Act as they may be amended from time to time.

IV. **PERMITTED USES AND DISCLOSURE BY BUSINESS ASSOCIATE OF PROTECTED HEALTH INFORMATION.**

A. Except as otherwise limited in this Agreement, Business Associate may use or disclose Protected Health Information to perform functions, activities, or services for, or on behalf of, Covered Entity as specified in the Contract, this Agreement, provided that such use or disclosure shall not violate the Privacy Rule, the Substance Abuse Records Rule and/or Security Rule.

B. Except as otherwise limited in this Agreement, Business Associate may use and disclose Protected Health Information as Required by Law.

C. Except as otherwise specifically provided in the Contract or this Agreement, Covered Entity will not request Business Associate to use or disclose Protected Health Information in any manner that would not be permissible under the Privacy Rule if done by Covered Entity. Without limiting the generality of the foregoing, Covered Entity will provide, and Business Associate agrees to request, no more than, the minimum necessary amount of Protected Health Information required for the performance of Business Associate's services under the Contract. Business Associate and Covered Entity will comply with the guidance on minimum necessary to be issued by the Secretary as to the minimum necessary as specified by Covered Entity.

D. Business Associate may not use or disclose Protected Health Information for its own management in a manner that would violate Subpart E of 45 CFR Part 164 if done by Covered Entity. Furthermore, Business Associate may not use Protected Health Information to de-identify the information in accordance with 45 CFR 164.514(a)-(c).

V. BUSINESS ASSOCIATE RESPONSIBILITY.

Business Associate shall be directly responsible for full compliance with the relevant requirements of HIPAA (including the Privacy Rule) to the same extent as Covered Entity. Business Associate shall establish safeguards that are reasonable and appropriate to prevent any use or disclosure of Protected Health Information not expressly authorized by this Agreement.

VI. OBLIGATIONS AND ACTIVITIES OF BUSINESS ASSOCIATE.

A. Business Associate shall not use or disclose Protected Health Information other than as permitted or required by this Agreement, the Substance Abuse Records Rule, Security Rule or Required by Law.

Business Associate acknowledges that in receiving, storing, processing, or otherwise dealing with any records from Covered Entity, it is fully bound by 42 CFR 2. Notwithstanding anything to the contrary in this Section or in this Agreement, to the extent Business Associates receives a request to compel production from a judicial forum, government agency or otherwise, it shall immediately report such to Covered Entity and Business Associate shall take all measures reasonably necessary to prevent access or disclosure of the PHI subject to the Substance Abuse Records Rule, which may include obtaining a protective order, and shall not disclose any such information if, in the reasonable opinion of the Covered Entity, such would violate the Substance Abuse Records Rule.

B. Business Associate shall use appropriate safeguards, and comply with Subpart C of 45 CFR Part 164 with respect to Electronic PHI, to prevent use or disclosure of the Protected Health Information other than as provided for by this Agreement.

C. Business Associate shall mitigate, to the extent practicable, any harmful effect that is known to Business Associate of a use or disclosure of Protected Health Information by Business Associate in violation of the requirements of this Agreement.

D. Business Associate shall immediately report in writing to Covered Entity any use or disclosure of the Protected Health Information not provided for by this Agreement of which it becomes aware, including breaches of Unsecured Protected Health Information as required at 45 CFR 164.410, and any Security Incident of which it becomes aware. The parties agree that this Section satisfies any notices necessary by Business Associate to Covered Entity of the ongoing existence and occurrence of unsuccessful Security Incidents for which no additional notice to Covered Entity shall be required, except on request as stated below. For purposes of this Agreement, such unsuccessful Security Incidents include, without limitation, activity such as pings and other broadcast attacks on Business Associate's firewall, port scans, unsuccessful log-on attempts, denial of service, and any combination of the above, so long as no such unsuccessful Security Incident results in unauthorized access, use, disclosure, modification, or destruction of Electronic PHI or interference with information system operations related to the Electronic PHI, and provided that, upon written request from Covered Entity, Business Associate will provide a log or similar

documentation of unsuccessful Security Incidents for the period of time reasonably specified in Covered Entity's request. Successful Security Incidents will be reported to Covered Entity in writing within three (3) business days of the date the successful Security Incident is, or in the exercise of reasonable efforts should have been known, to Business Associate. If the successful Security Incident constitutes a Breach, the parties will proceed as required under this Agreement as to a Breach.

E. In accordance with 45 CFR 164.502(e)(1)(ii), if applicable, Business Associate shall ensure that any agent, including a subcontractor, that creates, receives, maintains, or transmits Protected Health Information on behalf of Business Associate agrees to the same restrictions, conditions, and requirements that apply to the Business Associate with respect to such information. Business Associate shall be responsible for any violation of this Section VI.E. by any agent and/or subcontractor and shall indemnify and hold Covered Entity harmless from any and all claims related to any such violation of this Section VI.E.

F. Business Associate shall provide access, at the request of Covered Entity, in the time and manner requested by Covered Entity, to Protected Health Information in a Designated Record Set, to Covered Entity or, as directed by Covered Entity, to an Individual in order to meet the requirements under 45 CFR 164.524. Business Associate will notify Covered Entity within three (3) days of any requests for access received directly from an Individual.

G. Business Associate shall, as directed by Covered Entity, provide Individual(s) with access to their Protected Health Information in an electronic format and transmit such information in electronic format directly to an entity specified by the Individual, to the extent the Individual's Protected Health Information is Covered Entity's Protected Health Information and is held or controlled by Business Associate, in accordance with HIPAA.

H. Business Associate shall make any amendment(s) to Protected Health Information in a Designated Record Set that the Covered Entity directs or agrees to pursuant to 45 CFR 164.526 at the request of Covered Entity or an Individual, or take other measures as necessary to satisfy Covered Entity's obligations under 45 CFR 164.526. Business Associate will notify Covered Entity within three (3) days of any requests for amendments received directly from an Individual.

I. Business Associate shall make internal practices, books, and records, including policies and procedures and Protected Health Information, relating to the use and disclosure of Protected Health Information received from, or created or received by Business Associate on behalf of, Covered Entity available to the Covered Entity, and/or to the Secretary, for purposes of the Covered Entity and/or Secretary determining compliance with HIPAA (including Privacy Rule).

J. Business Associate shall document such disclosures of Protected Health Information and information related to such disclosures as would be required for Covered Entity to respond to a request by an Individual for an accounting of disclosures of Protected Health Information in accordance with 45 CFR 164.528. Business Associate agrees to provide to Covered Entity or an Individual, in timely manner, information collected in accordance with this Section VI.J., to permit Covered Entity to respond to a request by an Individual for an accounting of disclosures of Protected Health Information in accordance with 45 CFR 164.528. Business Associate shall maintain, and upon request with reasonable notice and at no cost to Covered Entity, provide Covered Entity with an accounting of uses and disclosures of Protected Health Information as necessary to satisfy Covered Entity's obligations under 45 CFR 164.528.

K. To the extent Business Associate is to carry out one or more of Covered Entity's obligations under Subpart E of 45 CFR Part 164, Business Associate shall comply with the requirements of Subpart E that apply to the Covered Entity in the performance of such obligations.

L. Business Associate agrees to use appropriate safeguards to prevent use or disclosure of Protected Health Information, other than as provided for by the Contract or this Agreement, in accordance with all requirements at 45 C.F.R. Sections 164.301 through 164.314. If and to the extent Business Associate, creates, receives, maintains, transmits or otherwise controls Electronic PHI of Covered Entity, Business Associate shall comply with the applicable provisions of the Security Standards, by providing Administrative, Physical, and Technical Safeguards for all Electronic PHI and by developing Policies and Procedures implementing those Safeguards.

M. Business Associate agrees to ensure that any agent, including a subcontractor, to whom it provides Protected Health Information received from, or created, received, maintained, or transmitted by Business Associate on behalf of Covered Entity, provides satisfactory written assurances, in a form meeting all requirements of 45 CFR 164.314 (i.e., a business associate agreement), to the same restrictions and conditions that apply through this Agreement to Business Associate, including requirements to terminate the relationship in certain circumstances, provide adequate Administrative, Physical, and Technical Safeguards for Electronic PHI, and implement appropriate policies and procedures, with respect to such information.

N. Upon Business Associate's knowledge of a pattern of activity or practice of a subcontractor in violation of assurances provided by a subcontractor pursuant to Section M. herein, Business Associate may provide an opportunity for that subcontractor to end the violation. Business Associate shall terminate the agreement with that subcontractor if the subcontractor does not end the violation within the time specified by the Business Associate.

O. Subject to receiving notice as described in Section VIII herein, Business Associate agrees to abide by any restriction on the use or disclosure of Protected Health Information agreed to by Covered Entity including, without limitation, agreements required by HIPAA not to disclose an item or service paid for entirely out-of-pocket by an individual to a Health Plan for payment or health care operations purposes, unless such disclosure is Required by Law.

P. Business Associate agrees to mitigate at its sole expense, and to the fullest extent possible, any harmful effect, resulting from a use or disclosure of Protected Health Information by Business Associate in violation of HIPAA, this Agreement, or the Contract including, without limitation, a Breach of Unsecured PHI as set forth in Section VII herein (collectively "Harmful Effect"), and to coordinate such mitigation efforts with Covered Entity. Notwithstanding the foregoing or anything to the contrary in the Contract, Business Associate agrees to pay costs and expenses incurred by Covered Entity (including reasonable attorneys' fees) to address, investigate, notify, cure or pay any fines or penalties associated with any Harmful Effect such as Breach of Unsecured PHI.

VII. BREACH OF UNSECURED PROTECTED HEALTH INFORMATION.

Business Associate shall document and notify Covered Entity of a Breach of Unsecured Protected Health Information. Business Associate's notification to Covered Entity hereunder shall:

A. Be made to Covered Entity without unreasonable delay and in no case later than three (3) calendar days after the incident constituting the Breach is first known, except where a law enforcement official determines that a notification would impede a criminal investigation or cause damage to national security. For purposes of clarity for this Section VII.A., Business Associate must notify Covered Entity of an incident involving the acquisition, access, use or disclosure of Protected Health Information in a manner not permitted under 45 CFR 'E within three (3) calendar days after an incident even if Business Associate has not conclusively determined within that time that the incident constitutes a Breach as defined by HIPAA;

B. Include the names of the Individuals whose Unsecured Protected Health Information has been, or is reasonably believed to have been, the subject of a Breach;

C. Be in substantially the same form as Exhibit A hereto; and

D. Include a draft letter for the Covered Entity to utilize in Covered Entity's discretion to notify the Individuals that their Unsecured Protected Health Information has been, or is reasonably believed to have been, the subject of a Breach that includes, to the extent possible:

- (1) A brief description of what happened, including the date of the Breach and the date of the discovery of the Breach, if known;

- (2) A description of the types of Unsecured Protected Health Information that were involved in the Breach (such as full name, Social Security number, date of birth, home address, account number, disability code, or other types of information that were involved);
- (3) Any steps the Individuals should take to protect themselves from potential harm resulting from the Breach;
- (4) A brief description of what the Covered Entity and the Business Associate are doing to investigate the Breach, to mitigate losses, and to protect against any further Breaches; and
- (5) Contact procedures for Individuals to ask questions or learn additional information, which shall include a toll-free telephone number, an e-mail address, Web site, or postal address.

(E) Provide other information relating to the Breach as discovered or as requested by Covered Entity, and shall cooperate with Covered Entity with regard to the provision of required notices to individuals and, if applicable, government agencies, to the extent such notices are determined necessary by Covered Entity.

VIII. OBLIGATIONS OF COVERED ENTITY TO INFORM BUSINESS ASSOCIATE OF INDIVIDUAL RESTRICTIONS.

A. Covered Entity will notify Business Associate of any restriction on the use or disclosure of Protected Health Information to which Covered Entity has agreed in accordance with the Privacy Rule, to the extent that such restriction may affect Business Associate's use or disclosure of Protected Health Information, at least ten (10) days in advance of the date on which compliance by the Business Associate is required, including agreements required by HIPAA not to disclose an item or service paid for entirely out-of-pocket by an Individual to a Health Plan for payment or health care operations purposes, unless such disclosure is required by law.

IX. TERM: TERMINATION AND EFFECT OF TERMINATION.

A. Term. This Agreement shall terminate when all of the Protected Health Information provided by Covered Entity to Business Associate, or created or received by Business Associate on behalf of Covered Entity, is destroyed or returned to Covered Entity, or, if it is infeasible to return or destroy Protected Health Information, protections are extended to such information, in accordance with the termination provisions in this Section IX.

B. Termination for Cause. Upon Covered Entity's knowledge of a material breach of this Agreement by Business Associate, Covered Entity shall at its option:

- (1) Provide an opportunity for Business Associate to cure the breach or end the violation and, if Business Associate does not cure the breach or end the violation within the time specified by Covered Entity, terminate this Agreement;
- (2) Immediately terminate this Agreement if Business Associate has breached a material term of this Agreement and cure is not possible;
- (3) If neither termination nor cure is feasible, report the violation to the Secretary; and/or
- (4) Immediately terminate the Contract.

C. Effect of Termination.

- (1) Except as provided in Paragraph (3) of this Section IX.C., upon termination of this Agreement and/or the Contract, for any reason, Business Associate shall, at the election of the Covered Entity, return or destroy all Protected Health Information received from Covered Entity, or created or received by Business Associate on behalf of Covered Entity. This provision shall apply to Protected Health Information that is in the possession of subcontractors and/or agents of Business Associate. Business Associate shall not retain any copies of the Protected Health Information. Business Associate shall provide a written certification that all such Protected Health Information has been returned or destroyed.
- (2) In the event that Business Associate determines that returning or destroying the Protected Health Information is infeasible, Business Associate shall provide to Covered Entity written certification of the conditions that make return or destruction infeasible. If Covered Entity agrees that the conditions described by Business Associate make return or destruction infeasible, which agreement will not be unreasonably withheld, it will notify Business Associate in writing, and in lieu of return or destruction, Business Associate shall extend the protections of this Agreement to such Protected Health Information and limit further uses and disclosures of such Protected Health Information to those purposes that make the return or destruction infeasible, for so long as Business Associate maintains such Protected Health Information.
- (3) Should Business Associate make an intentional or grossly negligent Breach of Protected Health Information in violation of this Agreement or HIPAA or an intentional or grossly negligent disclosure of information protected by the MCMRA, Covered Entity shall have the right to immediately terminate any contract, other than this Agreement, then in force between the parties, including the Contract.
- (4) Upon termination of this Agreement and/or the Contract for any reason, Business Associate shall ensure the compliance with this Section IX. by all agents and subcontractors of Business Associate.

X. **REMEDIES IN EVENT OF BREACH.**

Business Associate hereby recognizes that irreparable harm will result to Covered Entity, and to the business of Covered Entity, in the event of breach by Business Associate of any of the covenants and assurances contained in this Agreement. In the event of breach of any of the covenants and assurances contained in this Agreement, Covered Entity shall be entitled to enjoin and restrain Business Associate from any continued violation of this Agreement. The remedies contained in this Section shall be in addition to (and not supersede) any action for damages and/or any other remedy Covered Entity may have for breach of any part of this Agreement.

XI. **OTHER LAWS.**

Business Associate hereby agrees to comply with the Substance Abuse Records Rule. In the event of a conflict among the Substance Abuse Records Rule and the HIPAA Privacy and Security Rules, the Business Associate shall comply with the more restrictive protection requirement.

XII. **INDEMNIFICATION.**

Business Associate hereby agrees to defend (at the option of Covered Entity), indemnify and hold harmless Covered Entity and its agents, shareholders, employees, officers, funders and directors against any and all claims, demands, causes of action, losses, damages, liabilities, judgments, costs and expenses

(including reasonable attorney's fees) asserted against or incurred by Covered Entity or its agents, shareholders, employees, officers, funders and directors as a result of, or failure to comply with or in any way related to, the provisions of this Agreement and/or HIPAA by Business Associate, its subcontractors and/or its agents. In the event of a claim under this Agreement (a "Claim"), Covered Entity shall promptly notify Business Associate and Covered Entity shall engage qualified legal counsel reasonably acceptable to Business Associate to represent Covered Entity as to the Claim, at Business Associate's sole expense. Covered Entity will not settle any Claim without the consent of Business Associate, which consent will not be unreasonably withheld or conditioned. This indemnity obligation will expressly survive the termination of this Agreement for any reason.

XIII. MISCELLANEOUS.

A. Regulatory References. A reference in this Agreement to a section in the Privacy Rule, Security Rule, or HIPAA means the section as in effect or as amended.

B. Amendment. The parties agree to take such action as is necessary to amend this Agreement from time to time as is necessary for Covered Entity to comply with the requirements of the Privacy Rule, Security Rule, or HIPAA and any other applicable law. This Agreement can only be modified in writing signed by both parties.

C. Survival. The respective obligations of Business Associate pursuant to this Agreement shall survive the termination of this Agreement.

D. Interpretation. Any ambiguity in this Agreement shall be resolved in favor of a meaning that permits Covered Entity to comply with HIPAA and other applicable laws. In the event of a conflict between this Agreement and any other agreement between the parties, the terms of this Agreement shall govern unless the parties specifically state otherwise.

E. Notices. All notices pursuant to this Agreement shall be given in writing to the address listed above in this Agreement.

F. Full Force and Effect. Except as explicitly modified herein, the Contract shall remain in full force and effect.

G. Consideration. Business Associate recognizes that the promises it has made in this Agreement shall, henceforth, be detrimentally relied upon by Covered Entity in choosing to continue or commence a business relationship with Business Associate.

H. Subpoenas, Court Orders, and Governmental Requests. If Business Associate receives a court order, subpoena, or governmental request for documents or other information containing Protected Health Information, Business Associate will use its best efforts to notify Covered Entity of the receipt of the request, as permitted by law, within two (2) business days and provide Covered Entity an opportunity to respond. Business Associate may comply with such an order, subpoena, or request as required by Law.

I. Construction and Jurisdiction. This Agreement shall be governed by and construed in accordance with the laws of the State of Oklahoma (excepting any conflict of laws provisions which would serve to defeat application of Oklahoma substantive law). Each of the parties hereto submits to the exclusive jurisdiction of the state and/or federal courts located within the State of Oklahoma for any suit, hearing or other legal proceeding of every nature, kind and description whatsoever in the event of any dispute or controversy arising hereunder or relating hereto, or in the event any ruling, finding or other legal determination is required or desired hereunder.

J. Independent Contractor, Not Agent. For purposes of this Agreement, the Contract, and HIPAA, Business Associate, at all times, shall be considered and deemed to be an independent contractor, and not an Agent, of Covered Entity.

IN WITNESS WHEREOF, the parties have hereunto set their hands and seals the day and year first above written.

COVERED ENTITY:

[Customer]

By: _____

Name: _____

Title: _____

Date: _____

BUSINESS ASSOCIATE:

INTEGRATED HEALTH RESOURCES, LLC

By: _____

Name: _____

Title: _____

Date: _____

Exhibit A-1**NOTIFICATION OF BREACH OF UNSECURED PROTECTED HEALTH INFORMATION**

This notification is made pursuant to Section VII.C of the Business Associate Agreement between:

- <Organization Name> (Covered Entity), and
- _____ (Business Associate).

Business Associate hereby notifies Covered Entity that there has been a breach of unsecured (e.g., unencrypted) protected health information (PHI) that Business Associate has used or has had access to under the terms of the Business Associate Agreement.

Description of the breach: _____

Date of the breach: _____

Date of discovery of the breach by Business Associate: _____

Does the breach involve 500 or more individuals?

Yes/N

o If yes, do the people live in multiple states?

Yes/No

Number of individuals affected by the breach: _____

Names and identifying information of individuals affected by the breach: _____

The types of unsecured PHI that were involved in the breach (such as full name, Social Security number, date of birth, home address, account number, or disability code): _____

Description of what Business Associate is doing to investigate the breach, to mitigate losses, and to protect against any further breaches: _____

Contact information for an individual at Business Associate's office to ask questions or learn additional information regarding the breach:

Name/Title: _____

Address: _____

Email Address: _____

Phone Number: _____

ATTACHMENT E2

MASTER TERMS

Intentionally left blank.

ATTACHMENT E3 PRICING

SW1041 Software-Supplemental

Software Publishers		
Description	Maximum Cost + % Markup	% off List Price
<p>Comprehensive Call Center Hub for Government: Industry-standard platform with Lifeline-required data elements, embedded suicide risk assessments, and 988-ready streamlined call flow. Guides agents to appropriate care levels while ensuring compliance with national standards. Includes priority 24/7 technical support.</p> <p>List price: \$300 per user per month with 25 minimum users Module bundles and high user count may qualify for additional discounts</p>		10
<p>Advanced GPS-enabled Mobile Crisis Dispatch for Government: Real-time location-based dispatch system for crisis teams with integrated face-to-face, telehealth and transport workflows. Features electronic staff check-ins and configurable silent urgent escalation for enhanced field safety. Includes priority 24/7 technical support.</p> <p>List price: \$300 per user per month with 25 minimum users Module bundles and high user count may qualify for additional discounts</p>		10
<p>Comprehensive Follow-up Module for Government: Complete post-crisis management system with automated scheduling, embedded clinical assessments, and care collaboration tools. Ensures clinical stability and seamless linkage to ongoing care services. Includes priority 24/7 technical support.</p> <p>Flat fee module list price: \$10,000 Module bundles and high user count may qualify for additional discounts.</p>		10
<p>Dynamic Real-time Bed Registry for Government: Statewide bed capacity management system with secure provider referral capabilities. Eliminates outdated communication methods and streamlines placement workflows. Includes priority 24/7 technical support.</p> <p>List price: \$300 per user per month with 25 minimum users Module bundles and high user count may qualify for additional discounts</p>		10
<p>Sample Bundle Option 1: Seamless combination of Call Center Hub and Mobile Crisis Dispatch for Government. Creates uninterrupted workflow from initial contact through field intervention with complete data continuity across crisis episodes.</p>	-	-
<p>Sample Bundle Option 2: Complete Crisis Management Solution for Government: All-inclusive platform integrating call center, mobile crisis, follow-up, and bed registry capabilities. Provides end-to-end crisis management with unified reporting and analytics for comprehensive program oversight.</p>	-	-
<p>Platform Implementation Services for Government: Expert-led implementation including workflow analysis, configuration of 988-compliant protocols, and comprehensive staff training. Fixed percentage of subscription ensures predictable implementation costs.</p> <p>Fixed List % off price: 35% of platform annual subscription cost Module bundles and training effort may qualify for additional discounts.</p>		10

Other Value Add Products and Services		
Description	Maximum Cost + % Markup	% off List Price
<p>Platform Customization beyond out of the box functionality.</p> <p>List price: \$300 per hour. Note: after discovery, additional bundle discounts may apply</p>		10
<p>Integration services to streamline data flow with other software and other platforms.</p> <p>List price: \$350 per hour Note: after discovery, additional bundle discounts may apply</p>		10
<p>Reporting as a Service for customizations beyond the standard reporting that is included with the platform.</p> <p>List price is \$300 per hour Note: after discovery, additional bundle discounts may apply</p>		10
<p>Program Evaluation Services.</p> <p>List price is \$500 per hour Final hourly rate is based on the subject matter expertise required</p>		15%

Professional Services - Hourly Not-to-Exceed Rates		
Description	List Price	Discounted Hourly Rates
<p>Behavioral Health Crisis Continuum Consultation</p> <p>Final hourly rate is based on the subject matter expertise required</p>	500	10% off

ATTACHMENT E4

Offer of Value-Added products and/or Services

Value-Added Platform Customization Services

List price: \$300 per hour. Note: after discovery, additional bundle discounts may apply.

Beyond our standard implementation, we provide specialized platform customization services that extend the core functionality of software solutions deployed for Customers. We recognize that organizations often require tailored experiences that align precisely with their unique workflows and business requirements.

Our Platform Customization as a Service offering provides access to our expert development team who will work collaboratively with stakeholders to design, develop, and deploy customizations that enhance the platform's value. This specialized team delivers several key advantages at no additional cost:

- Business Process Alignment: Our specialists work directly with your teams to understand specific operational needs and develop customizations that streamline processes
- User Experience Enhancement: Custom interfaces and workflows designed specifically for Oklahoma's unique requirements improve adoption and productivity
- Regulatory Compliance: Tailored functionality ensures platforms meet Oklahoma's specific regulatory and policy requirements
- Future-Proof Development: All customizations are built using best practices to ensure longevity and compatibility with future platform updates

This collaborative approach to platform customization ensures that software investments deliver maximum value by adapting to your specific needs rather than forcing adaptation of processes to solution limitations.

Value-Added Integration Services

List price: \$350 per hour. Note: after discovery, additional bundle discounts may apply.

In today's behavioral health complex technology ecosystem, the true value of any software platform is determined not only by its standalone capabilities but by how effectively it connects with other systems across the organization. Our Integration Services offering addresses this critical need by providing specialized expertise to create seamless data flows between platforms.

Our Integration as a Service offering provides Customers with access to integration architects and developers who specialize in building reliable, secure, and efficient connections between systems. This specialized team delivers several key advantages at no additional cost:

- Ecosystem Optimization: Our specialists map the entire technology landscape to identify integration opportunities that maximize value across platforms
- Data Synchronization: Automated, bidirectional data flows ensure consistency across systems without manual intervention

- Security-First Design: All integrations are built with data protection as a foundational principle, ensuring sensitive information remains secure during transit
- Performance Monitoring: Ongoing oversight of integration performance ensures data flows remain reliable and efficient

Our goal is to support smooth system integrations that eliminates data silos and manual processes while creating a cohesive technology ecosystem that supports the customer's operational needs.

Value-Added Reporting Services

List price: \$300 per hour. Note: after discovery, additional bundle discounts may apply.

As part of our comprehensive suite of value-added services, we offer specialized reporting solutions that extend beyond standard software implementation. While our full BI Reporting Platform provides robust self-service capabilities for customer report developers, we recognize that many organizations prefer to leverage specialized expertise rather than allocating internal resources to report development and maintenance.

Our Report Development as a Service offering provides Customers with access to a dedicated team of reporting specialists who possess deep understanding of both the BHL Platform implementation and underlying data models. This specialized team delivers several key advantages at no additional cost:

- Platform-Optimized Reporting: Our specialists remain continuously aligned with the BHL Platform's evolution, ensuring reports maintain functionality and performance as the system grows and expands
- Data Model Expertise: Reports are developed with comprehensive understanding of data relationships, ensuring accuracy and reliability of business intelligence outputs
- Resource Optimization: customer's staff can focus on core responsibilities while still receiving customized, high-quality reporting solutions
- Proactive Maintenance: Our team monitors and updates reports to accommodate platform changes, preventing disruptions to critical business intelligence

This service-oriented approach to reporting aligns perfectly with the State's interest in maximizing value while minimizing administrative burden.

Value-Added Program Evaluation Services

List price: \$500 per hour.

Note: Final hourly rate is based on the subject matter expertise required

BHL's program evaluation services enhance our technology solutions while enabling customers to engage in meaningful, data-driven continuous quality improvement. Through collaboration with our Program Evaluation experts, customers gain deeper insights into the performance, efficiency, and effectiveness of their behavioral health services.

Service Offerings

Our program evaluation services are tailored specifically to the needs of each customer, ranging from targeted quality improvement initiatives to comprehensive evaluations of entire programs:

- Needs Assessment: Defining the need for a program or service delivery change through rigorous assessment methodologies.
- Evaluation Planning: Preparing for successful inquiry by developing clear roadmaps that link evaluation questions to appropriate data sources while establishing accountability for all stakeholders.
- Process and Formative Evaluation: Assessing the overall quality of program implementation, how the program functions in its formative phase, and identifying opportunities for improvement over time.
- Outcome and Impact Evaluation: Understanding a program's ability to provide services for an identified need and measuring the overall impact the service has on the target population.
- Participatory Frameworks: Engaging service recipients and providers as part of the evaluation process to enhance the quality of evaluation work products and ensure findings represent diverse perspectives.

Methodological Approach

Our program evaluation services offer quantitative, qualitative, and mixed-methods designs to answer the diverse array of evaluation questions that our customers have about their operations. We tailor our methodological approach based on program maturity:

- For emerging programs, we provide needs assessments along with process and formative evaluations
- For established services, we deliver robust outcome and impact evaluations that capture program contributions to addressing target population needs

Value to Oklahoma State Agencies

For state agencies committed to accountability, excellence, and leadership in delivering quality services, our program evaluation capabilities provide the necessary tools to:

- Generate actionable, data-driven insights
- Support evidence-based decision making
- Demonstrate program effectiveness to stakeholders
- Identify opportunities for service optimization
- Ensure resources are allocated to maximize impact

These services directly support the State's objective to reduce expenses while optimizing services to participating agencies and Interlocal Entities, delivering the highest level of customer service through continuous improvement.

Integration with Software Solutions

While our technology platform provides access to operational data through reports and dashboards, program evaluation services transform this data into strategic insights. Our evaluation team works alongside customers to ensure they derive maximum value from both their technological investment and their service delivery models.

Professional services: Behavioral Health Consulting

Service List price: \$500 per hour.

Note: Final hourly rate is based on the subject matter expertise required

BHL applies its extensive subject matter expertise through both software and consultation, serving our shared mission of crisis care excellence. Recognized nationally as a behavioral health pioneer since establishing the first statewide "air traffic control" crisis response system in 2006, BHL offers tailored consulting to help organizations build, optimize, and integrate comprehensive crisis care systems. Whether enhancing call centers, mobile crisis operations, implementing statewide networks, tracking quality care measures, or integrating innovative technologies, BHL's expert team helps customers deliver scalable, data-driven solutions that transform crisis response.

BHL's Crisis System Design & Strategy services recognize each crisis system's uniqueness. Working closely as partners, BHL helps assess current workflows, identify gaps, and develop strategic roadmaps that align with 988 guidelines, state policies, and national best practices. These strategies prioritize the integration of technology with real-world, scalable solutions that meet evolving crisis needs.

BHL also provides Crisis Services Program Implementation Support & Training for both crisis hotlines and mobile teams. Recognizing that a system is only as strong as its people, BHL guides clients through policy creation, accreditation compliance, and 988 standards adherence. The team shares proven strategies for effective staff recruitment, hiring, and retention while delivering customized training for crisis counselors.

Additionally, BHL's consultants help partners enhance Workplace Wellness & Staff Retention through wellness strategies, mental health support programs, and leadership training on supporting frontline staff. By prioritizing staff well-being, BHL helps organizations reduce burnout and turnover while enabling crisis teams to remain resilient and effective in delivering lifesaving services.

ATTACHMENT E5

THIRD PARTY TERMS

Intentionally left blank.

ATTACHMENT E6

Integrated Health Resources dba Behavioral Health Link Service Level Agreement (SLA)

BHL Platform SLAs

During the term of the applicable SOW or Service Order, the BHL Covered Services (defined below) will be operational and available to Customer at least 99.9% of the time in any calendar quarter (“**BHL SLA**”). If BHL does not meet the BHL SLA, and if Customer meets its obligations under this BHL SLA, Customer will be eligible to receive the Service Credits described below. This Service Level Agreement states the Customer’s sole and exclusive remedy for any breach of the BHL SLA by BHL. Capitalized terms used but not defined herein shall have the meanings assigned to them in the Master Service Agreement (“**Agreement**”) between BHL and Customer.

Definitions. The following definitions shall apply to the BHL SLA:

“Downtime” means any period during which the BHL Covered Services are either:

1. Unavailable — The BHL Covered Services are completely inaccessible to the Customer due to a failure within the BHL system; or
2. Critically Degraded — The BHL Covered Services are available but fail to meet the minimum performance thresholds defined below for a sustained period of more than five (5) consecutive minutes:
 - App Services Response Time (Latency): Average above *850 milliseconds* over a 5 minute period.
 - Data Transfer Completion Rate: Failure to complete scheduled or real-time data transfers within agreed processing windows.

Downtime does not include unavailability or degraded performance resulting from:

- Issues caused by Customer equipment, software, or network connectivity
- Scheduled maintenance within agreed maintenance windows
- Failures caused by third-party services outside of BHL’s reasonable control unless otherwise designated as a critical covered dependency in the SLA

“BHL Covered Services” means the BHL Platform components of the Services, limited to BHL Crisis Hub, BHL Mobile Dispatch, BHL Outpatient Referral and Bed Registry, and BHL Follow-up. The BHL Platform does not currently contain any third-party services designated as a critical covered dependency. If, during implementation, any third-party



service is identified as a critical covered dependency, it will be documented and added to the list of Covered Dependencies, and such dependencies will be included in the scope of coverage under this SLA.

“Quarterly Uptime Percentage” means the total number of minutes in an average calendar quarter minus the number of minutes of Downtime suffered by Customer in a calendar quarter, divided by the total number of minutes in an average calendar quarter. Total number of minutes in an average calendar quarter means total number of minutes in one calendar year (based on 365 days) divided by four (4) quarters. For purposes of clarification, Quarterly Uptime Percentage is calculated on a per country basis.

“Service Credit” means percentage-based monetary credits applied against the Customer’s subscription fees for the applicable quarter in which the SLA target was not met. Credits will be calculated as a percentage of the total quarterly subscription fees paid for the impacted BHL Covered Services:

Quarterly Uptime Percentage - Credit Percentage Applied to Quarterly Fees:

99.0% to < 99.9% - 3%

95.0% to < 99.0% - 7%

< 95.0% - 15%

Service credits will be applied to the Customer’s next invoice or, if the Service Term has ended, will be refunded within 60 days. Credits are the Customer’s sole and exclusive remedy for failure to meet the Quarterly Uptime Percentage commitment.

Maximum Service Credit

The aggregate maximum number of Service Credits to be issued by BHL to Customer for all Downtime in a given country that occurs in a single calendar quarter shall not exceed fifteen (15) days of Service added to the end of Customer's term for the Service for such country.

Service Credits may not be exchanged for, or converted to, monetary amounts.

Measurement Period

Performance metrics will be measured and calculated on a monthly basis.

Maintenance

BHL may provide maintenance on the BHL Covered Services from time to time, for scheduled maintenance purposes and updates. Under certain conditions, BHL may need to perform urgent or emergency preventative maintenance, such as installing security patches. Service disruptions due to scheduled or emergency maintenance and updates are referred to herein as **“Excused Downtime.”**

“Maintenance.” Except for urgent or emergency maintenance, BHL shall use reasonable commercial efforts to (i) perform maintenance and updates outside of business hours in the United States; and (ii) provide the Customer with no less than five (5) days’ prior written notice of such maintenance and updates, which notice may be given by a posting on BHL’s website or portal.



Escalation Procedures BHL will follow its established Incident Response Policy for all incidents impacting BHL Covered Services. This policy defines incident classification, notification timelines, escalation paths, and resolution procedures.

For SLA purposes:

- Critical Incidents will be escalated immediately to the on-call technical lead and BHL executive management, with customer notification within 30 minutes of detection and updates at least every 60 minutes until resolution.
- High Incidents will be escalated to the on-call technical lead within 1 hour, with updates at least every 2 hours until resolution.
- Customers may request escalation at any time by contacting the Service Desk and referencing the incident ID.

The full Incident Response Policy, including detailed escalation procedures, is available to customers upon request.

BHL SLA Exclusions

The BHL SLA does not apply to any performance or availability issues: (i) caused by factors described in the "Force Majeure" section of the Agreement; (ii) that resulted from Customer's equipment or third-party equipment, or both (not within the primary control of BHL); (iii) resulting from Excused Maintenance; or (iv) resulting from Customer's breach of the Agreement or Customer's failure to adhere to any required configurations, or follow any policies for acceptable use, or Customer's use of the Services in a manner inconsistent with the features and functionality of the Services.

Other Limitations

In the event that Customer is in breach of the Agreement (including Customer's payment obligations) at the time of the incident giving rise to a Service Credit, Customer shall not be entitled to receive the Service Credit.

Termination Rights

If Supplier fails to meet the same SLA for three (3) consecutive months, or for any four (4) months within a twelve (12) month period, Customer may terminate the Agreement without penalty upon thirty (30) days written notice.

ATTACHMENT E7

STATEMENT OF WORK TEMPLATE

This Statement of Work is as set forth below and supersedes all prior documents submitted by Integrated Health Resources dba Behavioral Health Link. The parties agree to use this Statement of Work or a document substantially similar in the form of this Statement of Work.

This Statement of Work ("SOW") is made pursuant to the Contract awarded under Solicitation SW1041 between [CUSTOMER NAME] ("Customer") and [YOUR COMPANY NAME] ("Supplier"), dated [CONTRACT DATE] ("Contract").

1. PROJECT OVERVIEW

[Brief description of the project/services to be provided]

2. TERM AND RENEWAL

2.1 Initial Term: This SOW shall commence on [START DATE] and continue for a period of [TERM LENGTH] ("Initial Term"), unless earlier terminated in accordance with the Contract.

2.2 Renewal: This SOW will automatically renew for successive terms of the same length as the Initial Term (each a "Renewal Term") at Supplier's standard rates in effect at the time of such renewal, unless either party delivers the other written notice of non-renewal at least sixty (60) days prior to expiration of the then-current term. Any increase in the applicable fees will not exceed five percent (3%) per year.

3. PROJECT CONTACTS

Customer Contacts:

Role	Name	Phone	Email
[Primary Contact]			
[Technical Contact]			
[Billing Contact]			

Supplier Contacts:

Role	Name	Phone	Email
Project Manager			
Technical Lead			
Account Manager			

4. SCOPE OF SERVICES

4.1 **Software Products:** [List of software products with version numbers and quantities]

4.2 **Implementation Services:** [Detailed description of implementation services]

4.3 **Training:** [Description of training to be provided]

4.4 **Support and Maintenance:** [Description of ongoing support and maintenance services]

4.5 **Deliverables:** [List of specific deliverables with acceptance criteria]

5. TIMELINE AND MILESTONES

[List of project milestones with target dates]

6. CUSTOMER RESPONSIBILITIES

6.1 Customer will designate an administrator ("Account Administrator") who will grant and manage access to individual employees or other end users.

6.2 Customer will be solely responsible for all actions of any individual who accesses the Applications using the Login Information.

6.3 Customer shall:

- Require users to utilize strong form, alpha numeric login Information
- Protect the confidentiality of all login Information
- Notify Supplier of any breach of the confidentiality of any login Information
- Notify Supplier if any individual who knows the Login Information leaves the employment of Customer, is no longer authorized to use the Login Information, or misuses the Login Information

6.4 Customer will maintain sufficient Internet access, network connectivity, and power to enable use of the Services.

6.5 Customer will be responsible for collecting, entering, and updating the Customer Data.

7. PRICING AND PAYMENT TERMS

7.1 **Software License/Subscription Fees:** [Detailed breakdown of software costs]

7.2 **Implementation Services Fees:** [Breakdown of implementation costs]

7.3 **Training Fees:** [Breakdown of training costs]

7.4 **Support and Maintenance Fees:** [Details of support and maintenance costs]

7.5 **Payment Schedule:** [Timeline for payments tied to milestones or deliverables]

7.6 **Payment Terms:** Payment of Supplier's invoices is due within forty-five (45) days of Customer's receipt of the invoice. If Supplier fails to receive timely payment of any fees, it may, in its sole discretion, suspend or terminate Customer's account.

7.7 **Expenses:** Customer shall reimburse Supplier for preapproved, out-of-pocket expenses reasonably incurred in rendering any services ordered hereunder.

8. INTELLECTUAL PROPERTY RIGHTS AND LICENSES

Reservation of Rights: Customer acknowledges that Supplier's grant of a term subscription to use the Application(s) is only a limited license to access and use the Application(s) and is not a sale or other transfer of rights in the Application(s). Supplier reserves all rights not expressly granted to Customer by this Agreement.

8.1 **Authorized Scope of Use:** Customer may only access and use the Application(s) for the scope of use authorized in this SOW. The Application(s) may be used only for, by, or on behalf of the Customer and only to process its own data.

8.2 **Restrictions:** Customer may not, except as permitted herein, copy, modify, adapt, publicly display, publicly perform, or create derivative works of the Application(s) or any portion thereof, or remove any copyright or other proprietary rights notices thereon. Customer shall not sell, re-sell, assign, sublicense, distribute, lease, make available as a service bureau, disclose, divulge, or otherwise transfer, make available or allow any third parties any right or access to the Application(s). Notwithstanding the foregoing, BHL acknowledges and agrees that that Customer may transfer licenses to a successor agency or other subdivision of the state resulting from a reorganization imposed by the state legislature.

9. DATA SECURITY AND PRIVACY

9.1 **Customer Data:** Customer will be solely responsible for collecting, entering, and updating the Customer Data. "Customer Data" means data and/or information regarding Customer, its Affiliates and/or Customer's end users provided to Supplier or to which Supplier has access or control in connection with the provision of the Application(s) and Services, including all personally identifiable information.

9.2 **Security Measures:** Supplier will take commercially reasonable precautions, including technical, administrative, and physical measures, to help safeguard Customer Data.

9.3 **Third-Party Services:** Certain Services allow Customer to connect to various third-party services via API or other integrations ("Linked Services"). Supplier is providing these connections to Customer only as a convenience, and the inclusion of any connection or link does not imply endorsement by Supplier. Customer's access and use of such Linked Services is governed solely by the terms and conditions of such Linked Services. Supplier is not responsible for the contents or behavior of any Linked Services.

10. [OMITTED]

11. DATA EXPORT UPON TERMINATION

Upon Customer's written request and at no additional cost, Supplier will provide Customer with access to export Customer's data via a mutually agreed format for up to 30 days after the Effective date of termination, if the termination is termination by convenience. If the termination is termination for cause, then Supplier will provide Customer with access to export data via a mutually agreed format for up to 60 days after the contract ends. The export will be in .csv format or another mutually agreed format. At the end of the 60-day period, Supplier will permanently delete or permanently remove the Customer's data from Supplier's platform.

12. CHANGE MANAGEMENT

Any changes to this SOW must be made via a written Change Order signed by authorized representatives of both parties. Change Orders shall include:

- Description of the change
- Impact on schedule
- Impact on cost
- Any other relevant impacts

13. ASSUMPTIONS AND CONSTRAINTS

[List of assumptions and constraints for the project]

14. SPECIAL TERMS AND CONDITIONS

14.1 **Integration with Third-Party Systems:** Supplier is not responsible for third-party system functionality or delays caused by third-party vendors.

14.2 **Remote Work:** The Parties acknowledge and agree that all work performed by Supplier hereunder is to be accomplished on a remote basis.

IN WITNESS WHEREOF, the parties hereto have caused this Statement of Work to be executed by their duly authorized representatives.

CUSTOMER

By: _____

Name: _____

Title: _____

Date: _____

SUPPLIER

By: _____

Name: _____

Title: _____

Date: _____