ATTACHMENT K – IS SECURITY PROVISIONING DOCUMENT

Please note, contracts involving particular classes of sensitive data may result in revisions to the terms below.

DISCLAIMER: Terms may change or be adjusted without notice.

Additional Contract Terms Related to Hosting Services

The parties agree to the following provisions in connection with any Customer Data stored or hosted by or on behalf of Supplier in connection with the Contract. Unless otherwise indicated herein, capitalized terms used in this Attachment without definition shall have the respective meanings specified in the Contract.

I. Definitions

a. "Customer Data" shall mean all data supplied by or on behalf of a Customer in connection with the Contract, excluding any confidential information of Supplier.

b. "Data Breach" shall mean the unauthorized access by an unauthorized person that results in the use, disclosure or theft of Customer Data.

c. "Non-Public Data" shall mean 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.

d. "Personal Data" shall mean 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) contains electronic protected health information that is subject to the Health Insurance Portability and Accountability Act of 1996, as amended.

e. "Security Incident" shall mean the attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with the hosted environment used to perform the services.

II. Customer Data

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

b. 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.

c. 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.

III. Data Security

a. 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.

b. 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.

c. 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.

d. 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.

e. 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.

f. 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.

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

IV. Security Assessment

a. The State requires any entity or third-party vendor 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.

b. To the extent Supplier requests a different sub-contractor than the third-party hosting vendor 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 vendor in connection with key business functions that are Supplier's obligations under the contract until the State approves the third-party hosting vendor's State Certification and Accreditation Review, which approval shall not be unreasonably withheld or delayed. In the event the third-party hosting vendor 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 vendor in connection with key business functions that are Supplier's obligations under the contract, until such third party meets such requirements.

V. Security Incident or Data Breach Notification: Supplier shall inform Customer of any Security Incident or Data Breach.

a. 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.

b. 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).

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

d. 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.

VI. Breach 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.

a. Supplier, unless stipulated otherwise, shall promptly notify the Customer identified contact within 2 hours or sooner, unless shorter time is required by applicable law, if it confirms that there is, or reasonably believes that there has been a Data Breach. 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.

b. 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.

c. 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.

VII. Notice: In addition to notice requirements under the terms of the Contract otherwise, contact information for Customer for notifications in connection with hosting services provided by Supplier are:

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

And

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

And

OMES Information Services General Counsel
3115 N. Lincoln Blvd
Oklahoma City, OK 73105

VIII. Supplier Representations and Warranties: Supplier represents and warrants the following:

a. 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.

b. 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.

c. 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.

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

IX. Indemnity

a. Supplier's Duty of Indemnification. Supplier agrees to indemnify and shall hold the State of Oklahoma and State, its officers, directors, employees, and agents harmless from all liabilities, claims, damages, losses, costs, expenses, demands, suits and actions of third parties (including without limitation reasonable attorneys' fees) (collectively "Damages") (other than Damages that are the fault of Customer) arising from or in connection with Supplier's breach of its express representations

and warranties in this Hosting Agreement and the Contract. If a third party claims that any portion of the products or services provided by Supplier under the terms of the Contract or this Hosting Agreement infringes that party's patent or copyright, Supplier shall defend and indemnify the State of Oklahoma 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 of Oklahoma and/or Customer. The State of Oklahoma 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 of Oklahoma 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 of Oklahoma for all associated costs, damages and fees incurred by or assessed to the State of Oklahoma 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.

X. Termination and Suspension of Service:

a. In the event of a termination of the contract, Supplier shall implement an orderly return of Customer Data in a mutually agreeable format at a time agreed to by the parties and the subsequent secure disposal of State Data.

b. During any period of service suspension, Supplier shall not take any action to intentionally erase any Customer Data.

c. In the event of termination of any services or agreement in entirety, Supplier shall not take any action to intentionally erase any Customer Data for a period of:

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

   ii. 30 days after the effective date of termination, if the termination is for convenience

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

After such period, Supplier shall have no obligation to maintain or provide any Customer Data and shall thereafter, unless legally prohibited or otherwise stipulated, delete all Customer Data in its systems or otherwise in its possession or under its control.

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

e. Supplier shall securely dispose of all requested data in all of its forms, such as disk, CD/DVD, backup tape and paper, when requested by the Customer. 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 days of its request for disposal of data.