State of Oklahoma

Office of Management and Enterprise Services

ADDENDUM 1 TO STATEWIDE CONTRACT SW1110 BETWEEN THE STATE OF OKLAHOMA CONTRACT AND GEOSAFE

This Addendum 1 ("Addendum") is an Amendment to the Contract awarded to GeoSafe in connection with Statewide Contract No. 1110 ("SW1110") and is effective 05/01/2019.

Recitals

Whereas, the State issued a Solicitation for proposals to provide a mobile dispatch information system that will allow municipal, county, and state law enforcement officers in the field to communicate and obtain critical information directly from federal, state, and local databases from their vehicles, as more particularly described in the Solicitation;

Whereas, GeoSafe submitted a proposal which contained exceptions to the Solicitation terms and various other Contract Documents; and

Whereas, the State and GeoSafe have negotiated the final terms under which GeoSafe will perform the Services under the Contract.

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. **Addendum Purpose.**

   This Addendum memorializes the agreement of the parties with respect to negotiated terms of the Contract that is being awarded to GeoSafe as of even date with execution of this Addendum. The parties agree that Supplier has not yet begun performance of work contemplated by the Solicitation.

2. **Negotiated Documents of the Contract.**

   2.1. The parties have negotiated certain terms of the Contract as follows:

   i. certain exceptions to the Solicitation as contained in Attachment A to this Addendum titled Negotiated Exceptions to the Solicitation;

ii. revisions to the Service Level Agreement proposed by GeoSafe as contained in Attachment B to this Addendum titled Service Level Agreement; and

iii. the Hosting Agreement proposed by the State of Oklahoma as contained in Attachment C to this Addendum titled, Hosting Agreement.

2.2. GeoSafe submitted certain exceptions to the Solicitation, only those listed on Attachment A herein are accepted, all others are hereby denied.

2.3. The parties shall in good faith negotiate a statement of work to further define the scope of any State Entity or Affiliate acquisition specific engagement.

3. **Purchasing Instructions.**

The Parties acknowledge that any agency of the Executive Branch of the State of Oklahoma wishing to utilize the goods or services integrated with state law enforcement systems, provided in this Contract, shall work through the Office of Management and Enterprise Services and the Department of Public Safety.

State of Oklahoma

By: ____________________

Name: James L. Reese, II

Title: Chief Information Officer

Date: May 20, 2019

GeoSafe

By: ____________________

Name: Moshe Gutman

Title: CEO

Date: May 17, 2019

ATTACHMENT A TO ADDENDUM 1 TO SW1110 BETWEEN THE STATE OF OKLAHOMA AND GEOSAFE

Negotiated Exceptions to the Solicitation

The Solicitation is hereby amended as set forth below and supersedes all prior Exceptions submitted by GeoSafe or discussed by the parties.

RFP Section	Exception
A. General Provisions, A.45 Ownership Rights, A.45.1	**Section A, General Provisions, A.45. is hereby modified to add the following provisions:** At the time of the execution of this Contract, the parties agree that the scope of the engagement does not include any Work Product for the State. This Contract is not a "works made for hire" relationship. Supplier owns the title, copyright, and other intellectual property rights of the Supplier products and services. Access to the Service is licensed, not sold. Should the scope of the engagement change at a later date to include Work Product then the following provision shall apply: As between Supplier and the State, the Work Product and intellectual property rights therein are and shall be owned exclusively by the State, 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 the state. To the extent that the Work Product, under applicable law, may not be considered works made for hire, Supplier hereby agrees that the Contract effectively transfers, grants, conveys, assigns, and relinquishes exclusively to the State all right, title and interest in and to all ownership rights and all Intellectual Property Rights in the Work Product, without the necessity of any further consideration, and the State 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 the State do not intend Supplier to be a joint author of the Work Product within the meaning of the Copyright Act of 1976. The State 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 the State, 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. The term ("Work Product") means any and all deliverables produced by Supplier solely for the State under a statement of work executed by

ATTACHMENT A TO ADDENDUM 1 TO
SW1110 BETWEEN THE STATE OF OKLAHOMA AND GEOSAFE

RFP Section	Exception
	the parties and issued pursuant to this Contract, including any and all tangible or intangible items or things that have been or will be prepared, created, developed, invented or conceived solely for such deliverables, including but not limited to any (i) works of authorship (such as manuals, instructions, printed material, graphics, artwork, images, illustrations, photographs, computer programs, computer software, scripts, object code, source code or other programming code, HTML code, flow charts, notes, outlines, lists, compilations, manuscripts, writings, pictorial materials, schematics, formulae, processes, algorithms, data, information, multimedia files, text web pages or web sites, other written or machine readable expression of such works fixed in any tangible media, and all other copyrightable works), (ii) trademarks, service marks, trade dress, trade names, logos, or other indicia of source or origin, (iii) ideas, designs, concepts, personality rights, methods, processes, techniques, apparatuses, inventions, formulas, discoveries, or improvements, including any patents, trade secrets and know-how, (iv) domain names, (v) any copies, and similar or derivative works to any of the foregoing, (vi) all documentation and materials related to any of the foregoing, and (vii) all intellectual property rights in any of the foregoing, and which are or were created, prepared, developed, invented or conceived for the use of benefit of the State in connection with the statement of work for the deliverables

ATTACHMENT B TO ADDENDUM 1 TO
SW1110 BETWEEN THE STATE OF OKLAHOMA AND GEOSAFE

The Service Agreement ("Agreement") is hereby amended as set forth below and supersedes all prior documents submitted by GeoSafe or discussed by the parties.

GeoSafe

Service Agreement

This Agreement is between GeoSafe and the State of Oklahoma, by and through the Office of Management and Enterprise Services ("State").

1.0

DEFINITIONS

"Customer" is defined as any State Entity or Interlocal Entity authorized to utilize this Contract.

"User Account" is defined as an account used to access the GeoSafe Mobile Service.

"Agency" is defined as a group of user accounts that a Customer manages.

"Locality" is defined as a group of Agencies.

"User" is defined as a person that uses the Service.

"CAD system" is defined as a computerized system used to dispatch units and personnel.

1.1

INITIATION OF SERVICE

To initiate a subscription to the GeoSafe Mobile Service, the Customer must submit a Service Subscription Order Form to GeoSafe. After GeoSafe approves the Order Form, GeoSafe agrees to grant access to the GeoSafe Mobile Service (hereinafter referred to as "Service") to Customer via a GeoSafe Mobile client application (hereinafter referred to as "Client").

1.2

CANCELLATION OF SERVICE

To cancel Service, Customer shall provide cancellation notice in writing to GeoSafe. Customer will be responsible for payment of services delivered and accepted up to the date of termination. In the event of cancellation of Service, access to the Service will be terminated, and the Client shall be uninstalled, removed, and its use be discontinued immediately by Customer. GeoSafe and the State may terminate the Contract in whole or in part after a thirty (30) day written notice of default and thirty (30) days option to cure. GeoSafe and the Customer may terminate an Ordering Form after a thirty (30) days written notice of default and thirty (30) day option to cure.

1.3

BILLING

GeoSafe shall invoice Customer for using the Service. Customer is responsible for paying the invoice according to Solicitation Contract §A.14. Non-payment of an invoice may result in cancellation of Service upon a thirty (30) day written notice of default and a thirty (30) day cure period. The cure period may be extended by the party claiming default or other just cause; provided, however, extension of the cure period shall not automatically operate as a waiver of such party's claim.

1.4

USER ACCOUNT MANAGEMENT

Customer will designate at least one (1) "Administrator" for managing user accounts.

The Administrator will be responsible for establishing, activating, modifying, reviewing, disabling, and removing user accounts. The Administrator can establish an Agency to group user accounts together.

The Administrator shall:

a. only grant access to users who have a need and right to access the Service;
b. disable a user's access to the Service when a user is terminated, or any other reason deemed necessary;
c. monitor and report user accounts with suspicious activity;
d. review user accounts regularly and remove or disable accounts that are no longer needed;
e. only establish user accounts in an Agency if the user is an employee, staff member, or officer of that entity;
f. name the Agency with its official entity name;
g. be responsible for the configuration of data sharing features between Agencies and Localities;

To use the Service, all Users consent to the following:

h. The user is accessing a restricted information system.
i. System usage may be monitored, recorded, and subject to audit.
j. Knowingly unauthorized use of the system is prohibited and may be subject to criminal and/or civil penalties.
k. Use of the system indicates consent to monitoring and recording, only to the extent necessary for performance of the Service.

1.5

INSTALLATION

GeoSafe agrees to let Customer install the following:

a. One (1) installation of GeoSafe server software on a Customer server.
b. Site-wide installations of Client software on Customer administered devices.

GeoSafe will install and configure the server software on the designated Customer server. Customer will be responsible for the installation of Client software on Customer administered devices. GeoSafe will provide guidance and recommendations to Customer for the deployment of the Client. GeoSafe will require access to the Customer CAD system database to allow Customer to view 911-call information.

GeoSafe will receive data from the Customer CAD system as a part of providing the Service. GeoSafe may require the CAD system vendor to provide an API so that GeoSafe may extract data from the CAD system. The Customer will be responsible for fees, if any, that are charged by the CAD system vendor.

2.1

PRICING INFORMATION

2.1.1 Customer must purchase a Locality license in order to use the Service.

2.1.2 One (1) User Account cannot be used to access the Service from more than three (3) devices simultaneously.

2.1.3. Any user requiring OLETS access must have their own User Account and the Law enforcement add-on. OLETS fees are not included as a part of the Service. Customer is responsible for these costs.

2.1.4. Hardware costs are not included as a part of the Service. Customer is responsible for these costs.

2.1.5. Cellular service (or other Internet connection) costs are not included as a part of the Service. Customer is responsible for these costs.

2.1.6. Customer's CAD vendor may require additional fees so that GeoSafe may access CAD data. These fees are not included as a part of the Service. Customer is responsible for these costs.

2.1.7. A user account is considered active if it was used at least once in a calendar month.

2.1.8. GeoSafe charges for active user accounts on a monthly prorated rate (one twelfth of the yearly rate).

2.1.9. After the end of a calendar quarter, GeoSafe will bill the Customer for the usage during the three (3) months comprising the quarter.

2.2
PRICING TABLE

Product	Government price
User Account	$120/year
Law enforcement add-on	$60/year
Locality license	$10,200/year
On-site training	$850/event/day

3.1
SUPPORT CONTACT

Customer will designate a "Support Contact" person for communicating with GeoSafe.

GeoSafe product support staff shall be available via email (support@geosafe.com) for assistance with the Service. Customer can expect a response within 12 hours.

3.2
MAINTENANCE RESPONSIBILITIES

Customer agrees to install and use the newest version of the Client provided by GeoSafe.

GeoSafe guarantees that the Client will perform as intended. Errors in the Client will be classified by the following priority levels:

a. Level 1 – Software errors that make the product unusable
Initial Response Time: 2 hours

b. Level 2 – Software errors that make the product difficult to use
Initial Response Time: 12 hours

c. Level 3 – Minor software errors
Initial Response Time: 24 hours

GeoSafe will correct software errors according to their priority level, where Level 1 has the highest priority. GeoSafe shall use reasonable efforts to provide a solution to the software errors at its discretion.

The Support Contact should notify GeoSafe in the event of a software error. Customer agrees to use reasonable efforts to assist GeoSafe in its efforts to find reported software errors.

3.3
ADDITIONAL FEATURE REQUESTS / MODIFICATIONS

GeoSafe and Customer will agree on additional feature requests and modifications to existing features in the Client on a case-by-case basis. The parties shall agree in writing to any modification, additional feature, and/or charge prior to implementation of the same. An additional charge may be required for changes additional features or modification to the Client. For the avoidance of doubt, this charge does not apply if the feature or modification is required to fix an error or issue that rendered the Client unusable. To the extent any modification is customized or developed exclusively for the Customer, Section A.46 of the Solicitation will apply. No modification will be developed exclusively for the Customer.

3.4
LIMITATIONS ON MAINTENANCE

Modifications to the Client not authorized by GeoSafe are prohibited and are not supported. GeoSafe will not be responsible for hardware malfunctions and errors resulting from hardware malfunctions. GeoSafe will not be responsible for interruptions in network connectivity that limit the ability to use the Client and Service, unless the connectivity interruption is the result of an error or malfunction in the Client.

3.5
EXTERNAL DATA SOURCES

The Service uses a variety of external data sources beyond the control of GeoSafe, including but not limited to: Customer CAD data, Customer GIS data, and state and federal criminal justice information. If access to a data source is discontinued, then our ability to support it will also need to end at that time. GeoSafe may also choose to discontinue support of an external data source for any other reason.

3.6
GEOSAFE IS A DATA PROCESSOR

As part of providing the Service to Customer, GeoSafe may transfer, store, and process Customer data. GeoSafe is a data processor and Customer is a data controller with respect to Customer data.

3.7
DATA SECURITY

3.7.1 All GeoSafe facilities used to store and process Customer data will adhere to industry security standards. These standards ensure the security and confidentiality of Customer data. GeoSafe protects against anticipated threats or hazards to the security or integrity of Customer data, and protects against unauthorized access to Customer data.

3.7.2 GeoSafe has the affirmative duty to resubmit the state's security certification and accreditation form six (6) months from the Effective Date addressing its steps to fully implement the following controls:

1. SCA 0 – General Provisioning;
    a. SCA 0.5 & 0.5.1 – Security Posture Review Process & Documentation.

        i. Draft of initial plan to regularly review and update security controls, policies, processes, and procedures.
            1. Ensure that within this draft there is a scheduled time to regularly review and update security controls, policies, processes, and procedures. This is to be set on a yearly bases at minimum.
    b. SCA 0.6 – 0.6.2 – DR & BC Planning
        i. Draft of an initial Disaster Recovery and Business Continuity plan based on industry best practices and guidelines.
            1. Resource – NIST – (https://www.nist.gov/).
            2. Ensure that within this draft there is a scheduled time to regularly review and update these plans. This is to be set on a yearly bases at minimum.

2. SCA 11 – Risk Management;
    a. SCA 11.1 Risk Assessment
        i. Draft of initial risk assessment process to evaluate hazards.
            1. Ensure a process to highlight risks and hazards and the correct steps needed to remediate and or mitigate as needed.
            2. Ensure that within this draft there is a scheduled time to regularly review and update this plan. This is to be set on a yearly bases at minimum.
3. SCA 12 – Staffing;
    a. SCA 12.1 – Draft an initial staffing plan that shows backups to key personnel.
4. SCA 14 – Personal Computer Usage;
    a. SCA 14 – Draft an initial computer usage policy.
        i. MDM utilization and controls in place.
5. SCA 22 – Mobile Computing;
    a. SCA 22 – Draft an initial mobile computing usage policy.
        i. MDM utilization and controls in place.
6. SCA 28 – Segmentation of Duties;
    a. SCA 28.1 – Draft an initial policy to segment our sensitive duties to prevent collusion and fraudulent transactions.
        i. Ensure activity logs are utilized as needed.

3.7.3. To the extent GeoSafe is still not in compliance as determined by the State in its sole discretion, GeoSafe shall, within thirty (30) days, work with the State in good faith to become compliant. If said compliance is not achieved within thirty (30) days (or any other reasonable period agreed upon between the parties) State may terminate this Contract, without further liability, but shall remain responsible for all fees for Services rendered and products provided and shall solely be permitted a pro-rata refund of any pre-paid unused fees for the remainder of the then-current term.

3.8

DATA SHARING

Unless GeoSafe and Customer specifically agree in writing to share Customer data with third parties, the data will not be disclosed, unless required by law. GeoSafe will give Customer the chance to challenge such a disclosure.

4.1

GRANT OF LICENSE

GeoSafe grants Customer ("you") a non-exclusive, non-transferrable license for the Client, subject to the following restrictions:

a. **Redistribution of Software.** The Client may only be used on Customer administered devices. Any other use is prohibited. The Client may not be rented, borrowed, given, or redistributed to any 3rd party.
b. **License Grant for Documentation.** The documentation that accompanies the Client is licensed for internal, non-commercial reference purposes only.
c. **Reservation of Rights and Ownership.** GeoSafe reserves all rights not expressly granted to you in this Contract. The Client is protected by copyright and other intellectual property laws and treaties. GeoSafe or its suppliers own the title,

copyright, and other intellectual property rights in the Client. The Client is licensed, not sold. This Agreement does not grant you any rights to trademarks or service marks of GeoSafe.

d. **Limitations on Reverse Engineering, Decompilation, and Disassembly.** You may not reverse engineer, decompile, or disassemble the Client, except and only to the extent that such activity is expressly permitted by applicable law notwithstanding this limitation.

e. **Links to third party sites.** GeoSafe is not responsible for the contents of any third-party sites or services, any links contained in third-party sites or services, or any changes or updates to third-party sites or services. GeoSafe is providing these links and access to third-party sites and services to you only as a convenience, and the inclusion of any link or access does not imply an endorsement by GeoSafe of the third-party site or service.

4.2

LIMITATION ON REMEDIES

Warranty: GeoSafe's sole and exclusive liability for any defective Client shall be, at GeoSafe's option, to repair or replacement of the Client, at no cost to the Customer. If repair or replacement of the Client is not reasonably feasible, then GeoSafe shall refund the amount paid for the current quarter's Service.

Limitation of Liability:

Unless otherwise provided under the applicable law or within this Agreement, neither party shall be liable for consequential damages, incidental, punitive, exemplary or indirect damages, lost profits or other business interruption damages, in tort or contact, even if the parties have been advised of the possibility of such damages. Except for intellectual property infringement, GeoSafe's fraud or willful misconduct, in no event shall GeoSafe be liable for losses, damages or indemnities arising out of or related to this contract exceed the amount paid or to be paid to GeoSafe for its services under the specific engagement, statement of work, or other similar contract document giving rise to the claim. This provision shall not apply to or limit damages, expenses, costs, actions, claims and liabilities arising from or related to property damage, bodily injury or death only directly, but not proximately, caused by GeoSafe; the indemnification obligations set forth in this Contract; GeoSafe's confidentiality obligations set forth in this Contract; data security and breach notification obligations set forth in the Contract; the bad faith, gross negligence or intentional misconduct of GeoSafe or its employees agents and subcontractors; or other acts for which applicable law does not allow exemption from liability.

4.3

TRADEMARK, COPYRIGHT, PATENT, AND OTHER PROPERTY RIGHTS

GeoSafe warrants that it is the sole entity authorized to use and enter into contracts for the use of the Software that is the subject of this contract. Should a lawsuit be initiated against GeoSafe or its representatives on the grounds of any property right infringement, the initiation of which would involve the Software discussed herein, GeoSafe shall notify Customer of such lawsuit within ten (10) days of its receipt of the petition. Upon notification of the lawsuit, Customer shall have the right to terminate the contract with ten (10) days written notice to GeoSafe. This provision is in addition to the rights afforded to both parties set forth in the Contract.

If sent to the State:

Office of Management and Enterprise Services
Chief Information Officer
3115 N. Lincoln Blvd.
Oklahoma City, Oklahoma 73105

With a copy, which shall not constitute notice, to:

Deputy General Counsel
3115 N. Lincoln Blvd.
Oklahoma City, Oklahoma 73105

If sent to GeoSafe:

GeoSafe Inc.
1313 Newbury Drive
Norman, OK 73071

[THE REMAINDER OF THIS PAGE INTENTIONALLY LEFT BLANK]

ATTACHMENT C TO ADDENDUM 1 TO
SW1110 BETWEEN THE STATE OF OKLAHOMA AND GEOSAFE

HOSTING AGREEMENT

This Hosting Agreement ("Hosting Agreement") is a Contract Document in connection with the Contract issued as a result of Solicitation No. 0900000327 (the "Contract") and entered into between GeoSafe ("Vendor") and the State of Oklahoma by and through the Office of Management and Enterprise Services ("State" or "Customer"), the terms of which are incorporated herein. This Hosting Agreement is applicable to any Customer Data stored or hosted by Vendor in connection with the Contract. Unless otherwise indicated herein, capitalized terms used in this Hosting Agreement 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 Customer in connection with the Contract, excluding any confidential information of Vendor.

b. "Data Breach" shall mean the unauthorized access by an unauthorized person that results in the access, 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 Vendor 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. Vendor 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. Vendor 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. Vendor 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, Vendor shall not respond to subpoenas, service or process, FOIA 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 Vendor's proposed responses. Vendor agrees to provide its completed responses to the Customer with adequate time for Customer review, revision and approval.

c. Vendor 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 Vendor. Vendor will promptly notify Customer of any loss, damage to, or unauthorized access of Customer Data. Vendor will use commercially reasonable efforts to reconstruct any Customer Data that has been lost or damaged by Vendor as a result of its negligence or willful misconduct. If Customer Data is lost or damaged for reasons other than as a result of Vendor's negligence or willful misconduct, Vendor, 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. Vendor 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. Vendor 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 Vendor 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 Vendor is responsible for encryption of Personal Data.

c. Vendor represents and warrants to the Customer that the hosting equipment will be routinely checked with a commercially available, industry standard software application with up-to-date virus definitions. Vendor will regularly update the virus definitions to ensure that the definitions are as up-to-date as is commercially reasonable. Vendor 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 Vendor, Vendor 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 Vendor has used to remediate the virus. Should the virus propagate to Customer's IT infrastructure, Vendor is responsible for costs incurred by Customer for Customer to remediate the virus.

d. Vendor 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. Vendor 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. Vendor shall permit its personnel and contractors to access Customer Data remotely only as required to fulfill Vendor's obligations under the Contract.

e. Vendor 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. Vendor 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. Vendor 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.

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. Vendor 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 Vendor 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. Vendor agrees not to migrate State's data or otherwise utilize a different third-party hosting vendor in connection with key business functions that are Vendor'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, Vendor acknowledges and agrees it may not utilize such third-party vendor in connection with key business functions that are Vendor's obligations under the Contract, until such third party meets such requirements.

V. **Security Incident Notification and Responsibilities**: Vendor shall inform Customer of any Security Incident or Data Breach

a. Vendor 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, Vendor will coordinate with Customer prior to making any such communication.

b. Vendor 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. Vendor 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 Vendor; and (iv) documents all Security Incidents and their outcomes.

VI. **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 Vendor.

a. Vendor, unless stipulated otherwise, shall promptly notify the Customer identified contact within 24 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. Vendor 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 Vendor's breach of its obligation to encrypt Personal Data and Non-Public Data or otherwise prevent its release, Vendor 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 – (2), (3) and (4) 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 Vendor based on root cause.

c. If a Data Breach is a direct result of Vendor's breach of its obligations to encrypt Personal Data and Non-Public Data or otherwise prevent its release, Vendor 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: Contact information for Customer for notifications pursuant this Hosting Agreement are consistent with the Contract with a copy sent to:

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

For immediate notice which does not constitute written notice:
OMES Help Desk
405-521-2444
helpdesk@omes.ok.gov
Attn: Chief Information Security Officer

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

a. The product and services provided under this Hosting Agreement do not infringe a third party's patent or copyright or other intellectual property rights.

b. Vendor 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, the Hosting Agreement and any ancillary documents and the consummation of the transactions contemplated by the Contract or any ancillary documents by Vendor 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 Vendor and any third parties retained or utilized by Vendor to provide goods or services for the benefit of the Customer.

d. Vendor 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. Vendor's Duty of Indemnification. Vendor 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 Vendor's breach of its express representations and warranties or other obligations in this Hosting Agreement and the Contract. If a third party claims that any portion of the products or services provided by Vendor under the terms of the Contract or this Hosting Agreement infringes that party's patent or copyright, Vendor shall defend and indemnify the State of Oklahoma and Customer against the claim at Vendor'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 Vendor of any third party claims and to the extent authorized by the Attorney General of the State, allow Vendor 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 Vendor, Vendor shall be granted authorization to equally participate in any proceeding related to this section but Vendor 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 Vendor's opinion, be likely to become the subject of a claim or an injunction preventing its use as contemplated under this Hosting Agreement, Vendor 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, Vendor shall implement an orderly return of Customer Data in a mutually agreeable format at a time agreed to the parties and the subsequent secure disposal of Customer Data.

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

c. In the event of termination of any services or agreement in entirety, Vendor 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, Vendor 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. Vendor 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.