Attachment C
Information Protection Provisions and Security Requirements

1. General Definitions

1.1 **"Data Security Obligations"** means, collectively, the obligations of Vendor to: (a) implement reasonable and appropriate measures designed to secure OAG Data according to the Security Measures as set forth in herein; and (b) notify OAG promptly in the event of a data security breach involving OAG Data and provide OAG with a written copy of the results of any investigation of such breach undertaken or commissioned by Vendor.

1.2 **"Loss Event Expenses"** means all losses, liabilities, damages, causes of action, claims, demands, expenses, professional services (including fees and costs for attorneys, crisis management, public relations, investigation, and remediation), and breach notification costs arising from, in connection with, or related to any of the following:

1.2.1 a data security breach involving OAG Data;
1.2.2 a violation of any law, statute, or regulation related to data security or data privacy involving OAG Data;
1.2.3 unauthorized access to or acquisition of OAG Data;
1.2.4 a loss of OAG Data;
1.2.5 a ransom or cyber extortion demand involving OAG Data;
1.2.6 misuse of OAG Data; or
1.2.7 an actual or alleged failure to:
  a. provide adequate notice, choice, consent, access, or security regarding OAG Data;
  b. take appropriate steps to ensure the accuracy of OAG Data;
  c. adequately minimize the collection, processing, use, or retention of OAG Data; or
  d. comply with cross-border data transfer laws and regulations regarding OAG Data.

1.3 **"OAG CISO"** shall mean the OAG's Chief Information Security Officer.

1.4 **"OAG Data"** means shall mean any data including but not limited to OAG Records and Information as defined below, of any kind, in any form provided, generated, or made available, by OAG under the Contract, including all information processed or stored on computers or other electronic media by OAG or on OAG's behalf and provided to or otherwise accessed by Vendor for or during the performance under the Contract;

1.5 **"OAG Records and Information**" means: information that may include confidential and sensitive information, personal identifying information, federal tax information, personal health information, criminal justice information, or any information that is classified as confidential or sensitive by federal or state law, by agency policy, or is defined as "Personal Identifying Information" under Texas Business and Commerce Code

§521.002(a)(1) or "Sensitive Personal Information" as defined by Texas Business and Commerce Code §521.002(a)(2).

1.6 **"Security Incident"** means: an event which results in the accidental or deliberate unauthorized access, loss, disclosure, modification, disruption, or destruction of information of OAG Data or information resources, as defined in TAC 202.1(34) and includes, without limitation, a failure by Vendor to perform its obligations under the "Data Security" and "Physical and System Security" subsections below.

2. General Provisions

2.1 Survival of Provisions and Severability

2.1.1 The OAG's rights and privileges applicable to OAG Data shall survive expiration or any termination of the Contract and shall be perpetual.

2.1.2 If any term or provision of the Contract, including these Information Protection Provisions and Security Requirements, is to any extent illegal, otherwise invalid, or incapable of being enforced, such term shall be excluded to the extent of such invalidity or unenforceability; all other terms hereof, including these Information Protection Provisions and Security Requirements, shall remain in full force and effect; and, to the extent permitted and possible, the invalid or unenforceable term shall be deemed replaced by a term that is valid and enforceable and that comes closest to expressing the intention of such invalid or unenforceable term.

2.2 Inclusion in all Subcontracts. The requirements of these Information Protection Provisions and Security Requirements shall be included in, and apply to, all subcontracts and any agreements the Vendor has with anyone performing services under the Contract on the OAG's behalf.

2.3 Third Parties. The Contract is between the Vendor and the OAG and is not intended to create any independent cause of action by any third party, individual, or entity against the Vendor or the OAG.

2.4 Termination for Non-Compliance. In the event that either Vendor, its employees, subcontractors, or agents fail to comply with any of the Information Protection Provisions and Security Requirements, OAG may exercise any remedy, including but not limited to immediate termination of the Contract.

2.5 Personnel Briefings Training and Acknowledgments. Vendor shall ensure that all persons having access to OAG Data obtained under the Contract are thoroughly briefed on related security procedures, restricted usage, and instructions requiring their awareness and compliance. The Vendor's employees, subcontractors, and agents accessing OAG Data Systems must complete all required security training and execute any required security agreements, acknowledgments, or certifications. The OAG designated contract manager shall provide direction to the Vendor regarding the acquiring of any

necessary access, completion of required security training and execution of required security agreements, acknowledgments, and certifications.

2.6 Key Person Dependence or Collusion. The Vendor shall protect against any key-person dependence or collusion by enforcing policies of separation of duties, restricted job responsibilities, audit logging, and job rotation.

2.7 Confidentiality

2.7.1 Vendor shall implement reasonable and appropriate administrative, physical, and technical safeguards designed to secure OAG Data, so as to prevent accidental or unlawful access or unauthorized or improper disclosure. Vendor shall not voluntarily and affirmatively disclose to any third party OAG Data without the prior written consent of OAG, which may be granted or withheld in OAG's sole discretion. If Vendor becomes aware of any accidental or unlawful access to or unauthorized or improper disclosure of OAG Data, it shall notify OAG promptly, and in any event no later than five (5) business days after becoming aware of thereof . Vendor shall also reasonably assist OAG with preventing the recurrence of such accidental or unlawful access or unauthorized or improper disclosure and with any litigation against third parties deemed necessary by OAG to protect its OAG Data.

2.7.2 Vendor shall not give any of its employees or subcontractors access to the OAG Data for any purpose, except as strictly necessary to perform Vendor's obligations under the Contract and Incorporated Documents and shall use all commercially reasonable efforts to ensure compliance with the Data Security Obligations and avoidance of Loss Event Expenses and their causes.

2.8 HIPAA Compliance

2.8.1 Vendor hereby acknowledges and agrees that OAG Data may include highly sensitive and personally identifiable information subject to the Health Insurance Portability and Accountability Act, (HIPPA) other privacy laws, and other legal privileges and protections.

2.8.2 In the event that OAG Data and/or communications include Protected Heath Information (PHI) as that term is understood within the context of HIPPA, then at all times, whether or not a protective order has been entered in any related ongoing litigation, Vendor shall use appropriate administrative, physical, and technical safeguards as required in the HIPAA final security rule at a minimum to protect the confidentiality, integrity, and availability of the PHI and to prevent its unauthorized use or disclosure. Vendor may only use PHI in providing services within the scope of services contemplated by the Contract, provided that such use would not violate HIPAA. Vendor shall not disclose PHI to any third party for any purpose unless the disclosure is required by law, or the OAG expressly consents in advance to each disclosure. Vendor shall immediately report to the OAG any use or disclosure of PHI not authorized by the Contract of which Vendor becomes aware, including any security incident, as that term is defined by HIPAA,

or breach of confidentiality of any PHI. Vendor shall ensure that Vendor's employees, subcontractors, and agents agree in writing to the restrictions and conditions that apply to Vendor with respect to the handling and safeguarding of PHI (including the restrictions on further disclosure) and agree in writing to implement reasonable and appropriate safeguards to protect PHI. Vendor shall maintain records, sufficient to allow the OAG to comply with their respective obligations relating to accountings of disclosures of PHI to third parties for at least seven (7) years from the time of any disclosure. Copies and access to such records shall be provided to the OAG and any individual's PHI at issue, upon request, in the manner and time frame reasonably requested. Vendor will make Vendor's internal practices, books, and records relating to the use and disclosure of PHI available to the Secretary of the United States Department of Health and Human Services, Office of the State Auditor, and the OAG, for purposes of determining compliance with HIPAA and/or Vendor's compliance with Vendor's contractual obligations, as the OAG may instruct, subject to any attorney-client or attorney work product privilege or other protection. Upon termination of the Contract, Vendor shall, at the direction of the OAG, return to the OAG or destroy all PHI that Vendor received from the OAG. Vendor shall retain no copies of such PHI. If return or destruction is not feasible, Vendor shall continue the protections for such PHI, and limit further use and disclosure of the PHI to those purposes that make the return or destruction of the PHI unfeasible.

2.9 Personal Identifiable Information. This subsection is applicable to OAG Data or any other information, documents, and communications which constitute "personal identifying information," "sensitive personal information," "victim," "driver's licenses," "social security numbers," "identifying financial information," "biometric identifiers," "use of crime victim or motor vehicle accident information," "use of zip code to verify customer's identity," "financial information," "unique electronic identification number, address, or routing code" and "access device" (referred to collectively herein as "Personal Identity Information") as those terms are understood or defined in TEX. BUS. & COMM. CODE § 72.001(2), TEX. BUS. & COMM. CODE Ch. 501, TEX. BUS. & COMM. CODE Ch. 505, TEX. BUS. & COMM. CODE Ch. 521 and/or TEX. GOV'T CODE § 552.136. In the event of an unauthorized disclosure by Vendor of Personal Identifiable Information in the performance of Vendor's contractual duties, under the Contract or any purchase or work order issued thereunder, Vendor shall assume and comply the applicable remedial requirements required by law. In the event of an unauthorized disclosure of Personal Identifiable Information, Vendor shall immediately notify in writing the OAG of such disclosure.

2.10 Materiality of Compliance. The Vendor acknowledges and agrees that all these security procedures, protocols, and all Information Protection Provisions and Security Requirements included in this Attachment C are material and essential to OAG's willingness to enter into any Contract with Vendor.

2.11 Commencement of Legal Action. The Vendor shall not commence any legal proceeding, including a proceeding related to the breach of OAG Data or any other Security Incident relating to OAG Data, on the OAG's behalf without the express written consent of the OAG.

3. Data Security

3.1 Rights in OAG Data. The Vendor and the Vendor's employees, subcontractors, and/or agents possess no special right to access, use, or disclose OAG Data as a result of the OAG's contractual or fiduciary relationship with the Vendor. All OAG Data shall be considered the property of the OAG and shall be deemed confidential.

3.2 Use of OAG Data

3.2.1 OAG Data have been, or will be, provided to the Vendor and the Vendor's employees, subcontractors, and/or agents solely for use in connection with performing services required under the Contract. Re-use of OAG Data in any form is not permitted or authorized. The Vendor agrees that they will not access, use, or disclose OAG Data for any purpose not necessary except for the performance of services required under the Contract

3.2.2 Without the OAG's approval (in its sole discretion), neither the Vendor nor the Vendor's employees, subcontractors, and/or agents shall: (i) use OAG Data other than in connection with providing services required under the Contract; (ii) disclose, sell, assign, lease, or otherwise provide OAG Data to third parties; (iii) commercially exploit OAG Data or allow OAG Data to be commercially exploited; or (iv) create, distribute, or use any electronic or hard copy mailing list of any OAG employees or any other business or individual identified in the OAG Data. Nothing contained in this agreement shall prevent the Vendor from compliance with a lawful request of the Texas Legislature or the United States Congress for OAG Data. Unless prohibited, the Vendor shall notify the OAG of any such request.

3.2.3 In the event of any unauthorized disclosure or loss of OAG Data, the Vendor shall immediately comply with the Notice subsection of the Security Incidents subsection set forth below. The Vendor or the Vendor's employees, subcontractors or agents may, however, disclose OAG Data to the extent required by law or by order of a court or governmental agency; provided that the Vendor shall give the OAG, and shall cause the Vendor's employees, subcontractors or agents to give the OAG, notice as soon as it or they are aware of the requirement; and the OAG shall use its or their best efforts to cooperate with the OAG if the OAG wishes to obtain a protective order or otherwise protect the confidentiality of such OAG Data. The OAG reserves the right to obtain a protective order or otherwise protect the confidentiality of OAG Data.

3.3 Protection of OAG Data. The Vendor shall engage in a continuous cycle of process improvement and vigilance to assess risks, monitor, and test security protection, and implement change to protect OAG Data. The Vendor agrees to perform such continuous

process improvement and to upgrade its security protection during the term of the Contract.

3.4 Statutory, Regulatory and Policy Compliance. The Vendor agrees to comply with all Federal and State policies, standards, and requirements, state and federal statutes, rules, regulations, and standards regarding the protection and confidentiality of OAG Data, for which it has received written notice, as currently effective, subsequently enacted, or as may be amended.

3.5 Data Retention and Destruction. The Vendor shall load and store OAG Data transmitted to it in its data systems and retain the OAG Data in accordance with a mutually agreed upon detailed schedule, which shall be compliant with the OAG Records Retention Schedule ("OAG RRS") promulgated by the Texas State Library and Archives Commission. The schedule will be based upon the Contract services being performed and the Vendor's limited authorization to access, use, and disclose OAG Data. Subsequent to developing and agreeing upon that schedule, Vendor shall:

3.5.1 Retain and destroy OAG Data in accordance with the detailed schedule for its retention and destruction; (According to OAG's data sanitization standards and in compliance with all applicable state laws and regulations regarding data sanitization);

3.5.2 Destroy or purge OAG Data in a manner consistent with state policy and Federal regulations for destruction of private or confidential data and in such a way so that such data is unusable and irrecoverable;

3.5.3 Destroy all hard copy OAG Data by shredding to effect 5/16-inch-wide or smaller strips and then either incinerating or pulping the shredded material; and

3.5.4 Within five (5) business days of destruction or purging, provide the OAG with a completed OAG "Certificate of Sanitation" form. (OAG will provide the requisite form to the Vendor upon request.)

3.5.5 In the event of Contract expiration or termination for any reason, Vendor and the Vendor's employees, subcontractors, and/or agents shall completely purge all OAG Data from the information systems of and no OAG Data will be retained by the Vendor . All hard-copy OAG Data shall (in accordance with the detailed retention schedule agreed to by Vendor and OAG under this Section 3.5.) be destroyed. If immediate purging of all data storage components is not possible, the Vendor agrees that any OAG Data remaining in any storage component will be protected to prevent unauthorized disclosures.

3.5.6 Within twenty (20) OAG Business Days of Contract expiration or termination, Vendor shall provide OAG with a signed statement detailing the nature of the OAG Data purged, destroyed, or to the extent OAG Data was retained, the type of storage media, physical location(s), and any planned destruction date of such retained OAG Data.

3.5.7 In its sole discretion, the OAG may waive notification requirements or request reasonable changes to the detailed schedule for the retention and destruction of OAG Data.

3.6 Requests for Confidential or Public Information

3.6.1 The Vendor and the Vendor's employees, subcontractors, and/or agents expressly do not have any actual or implied authority to determine whether any OAG Data is public or exempted from disclosure. Tex. Gov't Code Chapter 552 defines the exclusive mechanism for determining whether OAG Data is subject to public disclosure. The Vendor is not authorized to respond to public information requests on behalf of the OAG.

3.6.2 The Vendor agrees to forward to the OAG Public Information Coordinator, by facsimile within one (1) business day from receipt, all request(s) for information associated with the Contract. Information requests shall be forwarded to:

Public Information Coordinator
Office of the Attorney General
publicrecords@oag.texas.gov

4. <u>Physical and System Security</u>

4.1 General/Administrative Protections

4.1.1 At all times Vendor shall be fully responsible to OAG for the security of the storage, processing, compilation, or transmission of all OAG Data to which it has access, and of all equipment, storage facilities, and transmission facilities on which or for which such OAG Data are stored, processed, compiled, or transmitted, all of which equipment, storage, facilities and transmission facilities shall be located in the continental United States of America. Vendor shall not and shall ensure that Vendor's employees, subcontractors, and/or agents do not: (1) use the OAG Data to identify or make contact with any individual named in the OAG Data; (2) use the OAG Data to market or promote any service, or to engage in data sharing or any other sales related activity involving OAG Data; (3) violate privacy laws and/or any other laws and regulations applicable to the OAG Data; and/or (4) anonymize OAG Data, aggregate OAG Data or combine it with other data, for any reason.

4.1.2 The Vendor (and Vendor's employees, subcontractors, and/or agents) shall develop and implement internal protection systems, including potential employee and subcontractor background checks, information security access lists and physical security access lists (the "Access Protection Lists"), designed to protect OAG Data in accordance with applicable law and the provisions for Data Security, Physical Security, and Logical/Information System Protections contained in this Attachment C and/or the Contract. The access protection lists shall document the name and other identifying data for any individual authorized to access, use or disclose OAG Data, as well as any special conditions and limitations applicable to each authorization.

4.1.3 The Vendor shall remove individuals from or change the access rights of individuals on the applicable Access Protection List immediately upon such individual no longer requiring certain access or in the event such individual has violated applicable security procedures. At least monthly, the Vendor shall

review and update its Access Protection Lists and ensure that the Access Protection Lists accurately reflect the individuals and their access level currently authorized. At least monthly, the Vendor shall report the results of these reviews and access changes to the OAG designated contract manager.

4.1.4 The OAG shall, upon request, have the right to review the Vendor 's internal protection systems, security procedures and plans, and to Access Protection Lists for all areas of the work site(s) and all individuals authorized to access OAG Data. The OAG may, with or without cause, and without cost or liability, revoke or deny any or all authorizations of individuals performing services under the Contract. If any authorization is revoked or denied by OAG, the Vendor shall be given written notice of the denial/revocation. Vendor shall then immediately use its best efforts to assist the OAG in preventing access, use or disclosure of OAG Data.

4.1.5 OAG, in its sole discretion and without consulting Vendor , may immediately terminate OAG system access for anyone performing services under the Contract.

4.1.6 Vendor shall immediately notify the OAG designated contract manager when any person Vendor authorized to access the OAG systems is no longer authorized to have such access. This notice includes re-assigned or terminated individuals.

4.1.7 The Vendor's physical access security and logical access security systems shall track and log all access attempts and failures. The access security systems shall produce access logs on request. These logs shall identify all access failures and breaches. Notwithstanding anything to the contrary in the Contract, the physical access and logical access security systems logs for any particular calendar year shall be retained for a period of seven (7) calendar years after the last calendar day of the calendar year in which they were created. Thus, a log created on January 1, 2018 may be disposed of, with all other systems access logs created in 2017, on January 1, 2026. All physical access and logical access security systems logs shall be stored to electronic media. Any stored log shall be produced for viewing access and copying upon request of the OAG within five (5) OAG Business Days of the request.

4.1.8 Vendor shall maintain appropriate audit trails to provide accountability for use and updates to OAG Data, charges, procedures, and performance. Audit trails maintained by Vendor shall, at a minimum, identify the supporting documentation prepared by Vendor to permit an audit of the system by tracing the activities of individuals through the system. Vendor 's automated systems shall provide the means whereby authorized personnel have the ability to audit and to verify contractually required performance and to establish individual accountability for any action that can potentially cause access to, generation of, damage to, or modification of OAG Data. Vendor agrees that Vendor 's failure to maintain adequate audit trails and corresponding documentation shall create a presumption that the services or performance were not performed.

4.1.9 Vendor shall only use OAG Data and any OAG information resources to which Vendor receives access for the purpose of the business agreement contemplated by the Contract. OAG Data are not allowed on mobile/remote/portable storage devices; nor may storage media be removed from the facility used by Vendor .

Vendor may submit, to the OAG designated contract manager, a written request for an exception to these prohibitions. If OAG finds it necessary to allow OAG Data on mobile/remote/portable storage devices, or to allow storage media to be removed from a facility used by Vendor , OAG will specify any encryption standard Vendor shall follow for mobile/remote/portable storage devices and the circumstance(s) under which storage media may be removed.

4.2 Physical Security

4.2.1 The computer site and related infrastructures (e.g., Information system servers, protected interface equipment, associated peripherals, communications equipment, wire closets, patch panels, etc.) must have physical security that at all times protects OAG Data against any unauthorized access to, or routine viewing of, computer devices, access devices, and printed and stored data. The Vendor shall ensure that any equipment, servers or other storage device or facility, on which OAG Data is stored, processed, compiled or transmitted by Vendor , has restricted access, locked doors, adequate surveillance, adequate backup mechanisms, fire suppression, flood and humidity control procedures and applicable encryption, password verification, intrusion detection, brute-force login protection, and other security procedures and protocols that are subject to routine audits to verify and improve effectiveness.

4.2.2 OAG Data accessed shall always be maintained in a secure environment (with limited access by authorized personnel both during work and non-work hours) using devices and methods such as, but not limited to alarm systems, locked containers of various types, fireproof safes, restricted areas, locked rooms, locked buildings, identification systems, guards, or other devices reasonably expected to prevent loss or unauthorized removal of manually held data. Vendor shall also use best efforts to protect against unauthorized use of passwords, keys, combinations, access logs, and badges.

4.2.3 In situations such as remote terminals, or office work sites where all of the requirements of a secure area with restricted access cannot be maintained, the equipment shall receive the highest level of protection. This protection shall include (where communication is through an external, non-organization-controlled network [e.g., the Internet]) multifactor authentication that is compliant with NIST SP 800-63, Electronic Authentication Guidance level 3 or 4, and shall be consistent with IRS Publication 1075, Section 4.7. Alternate Work Sites.

4.2.4 Vendor shall protect information systems against environmental hazards and provide appropriate environmental protection in facilities containing information systems.

5. <u>Logical/Information System Protections</u>

5.1 Logical Security. The Vendor shall take all reasonable steps to ensure the logical security of all information systems used in the performance of the Contract, including but not limited to the following:

5.1.1 Independent oversight of systems administrators and programmers.

5.1.2 Restriction of user, operator, and administrator accounts in accordance with job duties.

5.1.3 Authentication of users to the operating system and application software program.

5.1.4 Vendor shall adhere to OAG-approved access methods, and the protection and use of unique identifiers such as user identifications and passwords.

5.1.5 Vendor shall have an authorization process for user access and privileges. Any access not granted is prohibited.

5.1.6 Vendor shall maintain an access protection list in accordance with Subsection 4.1 above that details the rights and privileges with respect to each such user and maintains audit trails for user account adds, deletes, and changes, as well as access attempts and updates to individual data records.

5.1.7 Vendor shall implement protection to prevent unauthorized processing in or changes to software, systems, and OAG Data in the production environment.

5.1.8 Vendor shall implement protection for the prevention, detection and correction of processing failure, or deliberate or accidental acts that may threaten the confidentiality, availability, or integrity of OAG Data.

5.1.9 Vendor shall implement counter-protection against malicious software on Vendor's internal systems used in contract performance.

5.1.10 Vendor shall ensure that relevant Security Incidents as discussed in Section below are identified, monitored, analyzed, and addressed.

5.1.11 Vendor shall apply a high-level of protection toward hardening all security and critical server communications platforms and ensure that operating system versions are kept current.

5.1.12 Vendor shall adhere to mutually agreed upon procedures for authorizing hardware and software changes, and for evaluation of their security impact.

5.1.13 Vendor shall institute a process that provides for immediate revocation of a user's access rights and the termination of the connection between systems, if warranted by the nature of any Security Incident.

5.2 Encryption

5.2.1 All OAG Data must be encrypted while at rest on any media (e.g., USB drives, laptops, workstations, and server hard drives), in transmission, and during transport (i.e., the physical moving of media containing OAG Data). All OAG Data must be encrypted using current FIPS validated cryptographic modules. The Vendor and OAG will agree to specify the minimum encryption level necessary. Any change to this minimum encryption level will be agreed to and communicated in writing between the OAG CISO or their designees.

5.2.2 OAG Data is not allowed on mobile/remote/portable storage devices; nor may storage media be removed from the facility used by the Vendor. This prohibition does not apply to the Vendor's Information Systems backup procedures.

6. Security Audit

6.1 **Right to Audit, Investigate and Inspect.** Without notice, the Vendor shall permit, and shall require the Vendor's employees, subcontractors, and agents to, permit the State Auditor of Texas and any other statutorily authorized state or federal agency to:

6.1.1 Monitor and observe the operations of, and to perform security investigations, audits, and reviews of the operations and records of, the Vendor and the Vendor's employees, subcontractors, and/or agents;

6.1.2 Inspect its information system in order to assess security at the operating system, network, and application levels; provided, however, that such assessment shall not interfere with the daily operations of managing and running the system;

6.1.3 Enter, unannounced, into the offices and places of business of the Vendor and the Vendor's employees, subcontractors, and/or agents for a security inspection of the facilities and operations used in the performance of services under the Contract. Specific remedial measures may be required in cases where either the Vendor and the Vendor's employees, subcontractors, and/or agents are found to be noncompliant with physical and/or data security protection.

6.2 **Place of Audit.** Any audit of documents shall be conducted at the Vendor's principal place of business and/or the location(s) of the Vendor's operations during the Vendor's normal business hours and at the Vendor's expense. Vendor shall provide to OAG and such auditors and inspectors as OAG may designate in writing, on Vendor's premises, (or if the audit is being performed of a Vendor's Agent, the Agent's premises, if necessary) space, office furnishings (including lockable cabinets), telephone and facsimile services, at least one workstation connected to each Vendor system subject to the audit, utilities and office-related equipment and duplicating services as OAG or such auditors and inspectors may reasonably require to perform the audits.

6.3 **Production of data/reports.** Vendor shall supply to the OAG and the State of Texas any data or reports rendered or available in conjunction with any security audit of Vendor or Vendor's employees, subcontractors, and/or agents if those reports pertain, in whole or in part, to the services provided under the Contract. This obligation shall extend to include any report(s) or other data generated by any security audit conducted up to one (1) year after the date of termination or expiration of the Contract.

7. **Security Incidents**

7.1 **Response to Security Incidents**. Contractor shall detect and respond to Security Incidents which might occur. Vendor shall document its relevant procedures and processes into an internal incident response plan and provide such plan for OAG approval no later than thirty (30) days prior to OAG Data being provided to Vendor. The OAG, in its discretion, may withhold fifty percent (50%) of Vendor's monthly invoices for each month until an OAG-approved incident response plan is in place.

7.2 **Notice.** Within one (1) hour of discovering or having any reason to believe that there has been, any physical, personnel, system, or OAG Data Security Incident the Vendor shall initiate risk mitigation and notify the OAG-CISO, by telephone and by email, of the

Security Incident and the initial risk mitigation steps taken. Vendor shall send email notification of incidents to: incidents@texasattorneygeneral.gov

7.3 Investigation and Initial Reporting Obligations

7.3.1 Within twenty-four (24) hours of the discovery, the Vendor shall conduct a preliminary risk analysis of the Security Incident; commence an investigation into the incident; and provide a written report using the attached Security Incident Report (Attachment Two) to the OAG-CISO, fully disclosing all information relating to the Security Incident and the results of the preliminary risk analysis.

7.3.2 This initial report shall include, at a minimum: nature of the incident (e.g., data loss/corruption/intrusion); cause(s); mitigation efforts; corrective actions; and estimated recovery time. Each day thereafter until the investigation is complete, the Vendor shall:

a. Provide the OAG-CSIO or their designee(s) with a daily oral or email report regarding the investigation status and current risk analysis; and

b. Confer with the OAG-CISO or their designee(s) regarding the proper course of the investigation and risk mitigation.

7.3.3 Whenever daily oral reports are provided, the Vendor shall provide, by close of business each Friday, an email report detailing the foregoing daily requirements.

7.4 Final Report

7.4.1 Within five (5) business days of completing the risk analysis and investigation, the Vendor shall submit a written Final Report to the OAG-CISO, which shall include:

a. A detailed explanation of the cause(s) of the Security Incident;

b. A detailed description of the nature of the Security Incident, including, but not limited to, extent of intruder activity (such as files changed, edited, or removed; Trojans), and the particular OAG Data affected; and

c. A specific cure for the Security Incident and the date by which such cure shall be implemented, or if the cure has been put in place, a certification to the OAG-CISO that states the date that the Vendor implemented the cure and a description of how the cure protects against the possibility of a recurrence.

7.4.2 If the cure has not been put in place by the time the report is submitted, the Vendor shall, within thirty (30) calendar days after submission of the final report, provide a certification to the OAG-CISO that states the date that the Vendor implemented the cure and a description of how the cure protects against the possibility of a recurrence.

7.4.3 If the Vendor fails to provide a Final Report or Certification required by this Section 7.4 within forty-five (45) calendar days, or as otherwise agreed to, of the Security Incident, the Vendor agrees the OAG may exercise any remedy in equity, provided by law, or identified in the Contract.

7.5 Independent Right to Investigate. The OAG reserves the right to conduct an independent investigation of any Security Incident, and should the OAG choose to do so, the Vendor shall cooperate fully, making resources, personnel and systems access available.

8. Remedial Action

8.1 Remedies Not Exclusive and Injunctive Relief. The remedies provided in this Section 8 are in addition to, and not exclusive of, all other remedies available within the Contract, or at law or in equity. The OAG's pursuit or non-pursuit of any one remedy for a Security Incident(s) does not constitute a waiver of any other remedy that the OAG may have at law or equity.

8.2 Notice and Compensation to Third Parties.

8.2.1 In the event of a Security Incident, third-party or individual data may be compromised, and The Vendor and OAG hereby agree that the actual harm to such third parties caused by the Security Incident is difficult to estimate.

8.2.2 Furthermore, The Vendor and OAG agree, that a reasonable forecast of just compensation is for the Vendor to provide to individuals whose personal, confidential, or privileged data were compromised or likely compromised as a result of the Security Incident:

a. Notification of the event;
b. Actual damages sustained by the individual as a result of the Security Incident and any prescribed statutory damages; and
c. One year of credit monitoring services, at no-cost to each such individual or entity.

8.2.3 Subject to OAG review and approval, Vendor shall provide notice of the Security Incident, to individuals whose personal, confidential, or privileged data were compromised or likely compromised. The notification shall provide notice of the Security Incident, and include:

a. A brief description of what happened;
b. A description, to the extent possible, of the types of personal data that were involved in the security breach (e.g., full name, SSN, date of birth, home address, account number, etc.);
c. A brief description of what is being done to investigate the breach, mitigate losses, and to protect against any further breaches;
d. Contact procedures for those wishing to ask questions or learn additional data, including a toll-free telephone number, website, and postal address;
e. Steps individuals should take to protect themselves from the risk of identity theft, including steps to take advantage of any credit monitoring or other service that the Vendor shall offer; and
f. Contact information for the Federal Trade Commission website, including specific publications.

8.2.4 Notice of the Security Incident shall comply with Section 504 of the Rehabilitation Action of 1973, with accommodations that may include establishing a

Telecommunications Device for the Deaf (TDD) or posting a larger-type notice on the website containing notice.

8.2.5 Vendor and OAG shall mutually agree on the methodology for providing the notice required in this subsection. Neither Party shall unreasonably withhold such agreement; however, the notice method must comply with the notification requirements of Section 521.053, Texas Business and Commerce Code (as currently enacted or subsequently amended). Provided further that Vendor must also comply with Section 521.053's "consumer reporting agency" notification requirements.

8.2.6 Notwithstanding the foregoing or anything in this Attachment C or the Contract to the contrary, if OAG, in its sole discretion, elects to send notice of the Security Incident in lieu of the Vendor sending notice, then Vendor shall reimburse to the OAG all costs associated with preparing and providing notice. If the Vendor does not reimburse such cost within thirty (30) calendar days of request OAG shall have the right to collect such cost by offsetting or reducing any future payments owed to Vendor.

9. <u>Cloud Computing State Risk and Authorization Management Program</u>

Pursuant to Section 2054.0593(d)-(f) of the Texas Government Code, relating to cloud computing state risk and authorization management program, Vendor represents and warrants that it complies with the requirements of the state risk and authorization management program and Vendor agrees that throughout the term of the Contract it shall maintain its certifications and comply with the program requirements in the performance of the contract.