Attachment #7
State of Iowa Security Terms ("Security Terms")

These Security Terms are entered into by and between [name of Vendor], a [entity type (*e.g.*, limited liability company, limited liability partnership, or corporation)] registered in the State of [State of registration (*e.g.*, Iowa)], with its principal place of business at [address of Vendor's principal place of business] ("**Vendor**") and the State of Iowa, acting by and through the Iowa Department of Administrative Services ("**State of Iowa**" or "**State**"). These Security Terms shall apply in addition to any other terms and conditions agreed to by the Parties, as amended, (**"Underlying Agreement(s)"**), and to the extent of any conflict or inconsistency between the specific provisions of these Security Terms and the terms of any other agreement between the Parties, these terms shall prevail. The parties may be referred to herein individually as a **"Party"** or collectively as the **"Parties"**; provided, however, that where the context clearly requires, the term **"Party"** or **"Parties"** may refer to or include the Governmental Entity making the individual purchase(s) pursuant to the applicable Underlying Agreement(s). Notwithstanding anything in these Security Terms or any Underlying Agreement(s) to the contrary, individual purchases made by Governmental Entities other than the Governmental Entity, including but not limited to OCIO, entering into this Agreement on behalf of the State of Iowa more broadly shall be deemed, upon making such purchase, to incorporate the terms and conditions of these Security Terms and shall constitute a separate, distinct and independent agreement between the applicable Governmental Entity and Vendor, and such Governmental Entity shall be solely responsible for any payments due and duties and obligations owed under these Security Terms and any Underlying Agreement(s).

1. Definitions. Capitalized terms not defined herein are as defined in the Underlying Agreement(s). The following capitalized terms shall have the following meanings:

1.1. **"Authorized Contractors"** means independent contractors, consultants, or other Third Parties (including other Governmental Entities) who are retained, hired, or utilized by any Governmental Entity to use, maintain, support, modify, enhance, host, or otherwise assist a Governmental Entity with any Services or Deliverables provided pursuant to an Underlying Agreement(s).

1.2. **"Confidential Information"** means, subject to any applicable federal, State, or local laws and regulations, including Iowa Code Chapter 22, any confidential or proprietary information or trade secrets disclosed by either Party (**"Disclosing Party"**) to the other Party (**"Receiving Party"**) that, at the time of disclosure, is designated as confidential (or like designation), is disclosed in circumstances of confidence, or would be understood by the Parties, exercising reasonable business judgment, to be confidential. Confidential Information does not include any information that: (i) was rightfully in the possession of the Receiving Party from a source other than the Disclosing Party prior to the time of disclosure of the information by the Disclosing Party to the Receiving Party; (ii) was known to the Receiving Party prior to the disclosure of the information by the Disclosing Party; (iii) was disclosed to the Receiving Party without restriction by an independent third party having a legal right to disclose the information; (iv) is in the public domain or shall have become publicly available other than as a result of disclosure by the Receiving Party in violation of this Agreement or in breach of any other agreement with the Disclosing Party; (v) is independently developed by the Receiving Party without any reliance on Confidential Information disclosed by the Disclosing Party; (vi) is disclosed or is required or authorized to be disclosed pursuant to law, rule, regulation, subpoena, summons, or

the order of a court, lawful custodian, governmental agency or regulatory authority, or by applicable regulatory or professional standards; or (vii) is disclosed by the Receiving Party with the written consent of the Disclosing Party.

1.3. **"Customer Data"** means all information, data, materials, or documents (including Confidential Information of or belonging to any applicable Governmental Entity) originating with, disclosed by, provided by, made accessible by, or otherwise obtained by or from a Governmental Entity making purchases pursuant to an Underlying Agreement(s), including Authorized Contractors of the foregoing, or otherwise related to an Underlying Agreement(s) in any way whatsoever, regardless of form, including all information, data, materials, or documents accessed, used, or developed by Vendor, Vendor Contractors, or Vendor Personnel in connection with any Services or Deliverables provided pursuant to an Underlying Agreement(s).

1.4. **"Customer Property"** means any property of or belonging to a Governmental Entity making purchases pursuant to an Underlying Agreement(s), including Customer Data, software, hardware, programs or other property possessed, owned, or otherwise controlled or maintained by a Governmental Entity.

1.5. **"Deliverables"** means all of the goods, Services, work, work product, items, materials, and property to be created, developed, produced, delivered, performed or provided by or on behalf of, or otherwise made available through, Vendor, Vendor Contractors, or Vendor Personnel, directly or indirectly, in connection with any Underlying Agreement(s).

1.6. **"Governmental Entity"** shall mean any Governmental Entity, as defined in Iowa Code Section 8A.101, or any successor provision thereto. The term Governmental Entity includes without limitation Participating Agencies, agencies, independent agencies, the Judicial Branch, the Legislative Branch, courts, boards, authorities, institutions, establishments, divisions, bureaus, commissions, committees, councils, examining boards, public utilities, offices of elective constitutional or statutory officers, and other units, branches, or entities of government.

1.7. **"I.T. Governance Document(s)"** or **"Governance Document(s)"** means any Information Technology policies, standards, processes, guidelines, or procedures developed by OCIO pursuant to Iowa Code section 8B, *available at*: https://ocio.iowa.gov/ (navigate to policies, standards, rules, respectively), and which are generally applicable to Participating Agencies, absent a waiver granted pursuant to Iowa Code section 8B.21(5) or any corresponding implementing rules.

1.8. **"Office of the Chief Information Officer"** or **"OCIO"** means the Office of the Chief Information Officer of the State of Iowa created by Iowa Code chapter 8B.

1.9. **"Participating Agency"** shall have the same meaning ascribed it under Iowa Code section 8B, including any subsequent amendments or successor provisions thereto.

1.10. **"Purchasing Instrument"** means documentation issued by a Governmental Entity to Vendor for the purchase of Deliverables under an Underlying Agreement(s), including a **"Purchase Order"** or **"Statement of Work"** executed thereunder, regardless of form, and which identifies the Deliverables to be purchased and any other requirements deemed

necessary by the applicable Governmental Entity, such as compensation and delivery dates.

1.11. **"Security Breach"** means the unauthorized acquisition of or access to Customer Data by an unauthorized person that compromises the security, confidentiality, or integrity of Customer Data, including instances in which internal personnel access systems in excess of their user rights or use systems inappropriately. **"Security Breach"** shall also be deemed to include any breach of security, confidentiality, or privacy as defined by any applicable law, rule, regulation, or order.

1.12. "**Services**" include, without limitation, all services performed or provided by or on behalf of, or otherwise made available through, Vendor, Vendor Contractors, or Vendor Personnel, directly or indirectly, in connection with any Underlying Agreement(s), including but not limited to the System or any corresponding hosting, implementation, migration, or configuration services related thereto.

1.13. **"System"** means any system provided or otherwise made available by or through Vendor, Vendor Contractors, or Vendor Personnel, directly or indirectly, in connection with any Underlying Agreement(s), including any software, programs, or applications associated therewith or included or incorporated therein, regardless of the method of delivery, including but not limited to any Internet-enabled, Web-based or other similar delivery method.

1.14. **"Third Party"** means a person or entity (including, any form of business organization, such as a corporation, partnership, limited liability corporation, association, etc.) that is not a party to any Underlying Agreement(s).

1.15. **"Vendor Contractor(s)"** means any of Vendors authorized subcontractors, affiliates, subsidiaries, or any other Third Party acting on behalf of or at the direction of Vendor, directly or indirectly, in performing or providing Deliverables under any Underlying Agreement(s).

1.16. **"Vendor Personnel"** means employees, agents, independent contractors, or any other staff or personnel acting on behalf of or at the direction of Vendor or any Vendor Contractor performing or providing Deliverables under any Underlying Agreement(s).

2. Security/Privacy, Business Continuity, and Disaster Recovery.

2.1. Data Ownership. All Customer Data shall be and remain the sole and exclusive property of the applicable Governmental Entity.

2.2. Vendor's access to and use of Customer Data. Vendor, Vendor Contractors, and Vendor Personnel shall not use any Customer Data for any purpose other than fulfilling Vendor's express obligations and duties under the Underlying Agreement(s) in accordance with the terms and conditions set forth therein, these Security Terms, and any applicable laws, rules, and regulations.

2.3. Data Protection. Vendor, Vendor Contractors, and Vendor Personnel shall safeguard the confidentiality, integrity, and availability of Customer Data. In so doing, Vendor, Vendor Contractors, and Vendor Personnel shall comply with the following:

2.3.1. Implement and maintain reasonable and appropriate administrative, technical, and physical security measures to safeguard against unauthorized access, disclosure, theft, or modification of Customer Property. Such security measures shall be in accordance with recognized industry standards and controls (including NIST 800-53 Revision 4 and ISO27001:2013), and not less stringent than the measures Vendor, Vendor Contractors, and Vendor Personnel utilize to safeguard their own data/information of like importance. In addition, such security measures shall comply with, and shall enable the applicable Governmental Entity to at all times comply fully with, all applicable federal, state, and local laws, rules, standards, policies, or procedures ordinances, codes, regulations, and orders or other security, privacy, or safeguarding requirements, including applicable I.T. Governance Document(s) or any applicable Governmental Entity's then-current security policies, standards, or procedures that have been supplied to Vendor or Vendor Contractors by the applicable Governmental Entity.

2.3.2. All Customer Data shall be encrypted at rest and in transit with controlled access and shall utilize TLS v. 1.1 or 1.2. Unless otherwise expressly provided herein or otherwise agreed to by the Parties in writing, Vendor, Vendor Contractors, and Vendor Personnel are responsible for encryption of Customer Data in their possession. Additionally, Vendor shall ensure hard drive encryption consistent with validated cryptography standards as referenced in Federal Information Processing Standards (FIPS) 140-2, Security Requirements for Cryptographic Modules for all Customer Data, unless the applicable Governmental Entity approves in writing the storage of Customer Data on a portable device that does not satisfy these standards.

2.3.3. Storage, processing, transmission, retention, or other maintenance of Customer Data at rest and all backups shall occur solely in the continental United States of America. Vendor shall not allow Vendor Personnel to access, store, process, or retain Customer Data on any portable devices, including personal computers, tablets, or cell phones, except to the extent such devices are used and permanently stored or backed up at all times only in the continental United States of America.

2.3.4. Vendor may permit Vendor Personnel to access Customer Data remotely only as required to provide technical support. Vendor may not provide technical user support on a 24/7 basis using a Follow the Sun model.

2.4. Hosting Terms. In addition to other terms herein that would be applicable to hosting, infrastructure, other "as a service" delivery models, or other similar Services, the following shall apply:

2.4.1. *Compliance/Audits*.

2.4.1.1. Compliance. Annually throughout the term, Vendor shall obtain and provide OCIO, upon request, at no additional cost:

2.4.1.1.1. An independent, Third-Party certificate of audit certifying that the Services/System complies with NIST 800-53, Revision 4 controls;

2.4.1.1.2. An ISO/IEC 27001:2005 certification;

2.4.1.1.3. Test or assessment results of an independent, Third-Party assessment of application scans using the Open Web Application Security Project (OWASP) Top Ten List;

2.4.1.1.4. Test results of a penetration test conducted by an independent, Third-Party;

2.4.1.1.5. A copy of Vendor's annual SOC 2 type 2 report (for all Trust Services Principles); and

2.4.1.1.6. A Vendor produced remediation plan resulting from items 2.4.1.1.1 through 2.4.1.1.5, inclusive.

2.4.1.2. Ongoing Security Testing. Vendor will periodically test its systems for potential areas where security could be breached. During the term, to the extent Vendor engages a Third-Party auditor to perform an SSAE 16 of Vendor's operations, information security program, and/or disaster recovery/business continuity plan, Vendor shall promptly furnish a copy of the test report or audit report to OCIO or its Authorized Contractors. In addition, Vendor shall disclose its non-proprietary security processes and technical limitations to OCIO or its Authorized Contractors to enable OCIO to identify compensating controls necessary to adequately safeguard and protect Customer Data, or to otherwise assist OCIO or any other Governmental Entity in complying with any laws, rules, regulations, orders, or corresponding audits. For example, Vendor shall disclose its security processes with respect to virus checking and port sniffing to OCIO.

2.4.1.3. Security Audit by OCIO. During the term, OCIO or its Authorized Contractor(s) may perform security audits/scans of Vendor's environment, including unannounced penetration and security tests. Any Governmental Entity's regulators (and any federal agencies providing grant funds used to pay for such Deliverables, in whole or in part) shall have the same right upon request. Vendor agrees to comply with all reasonable recommendations that result from such inspections, tests, and audits within reasonable timeframes.

2.4.1.4. Access to Security Logs and Reports. Vendor shall provide security logs and reports to OCIO or its Authorized Contractors in a mutually agreeable format upon request. Such reports shall include at least latency statistics, user access summaries, user access IP address summaries, user access history and security logs for all State files related to any Underlying Agreement(s).

2.4.2. *Backup and Recovery*. Vendor is responsible for maintaining a backup of Customer Data and shall maintain a contemporaneous backup of Customer Data that may be recovered within two (2) hours at any point in time. Additionally, Vendor shall store a backup of Customer Data in an off-site "hardened" facility no less than daily, maintaining the security of Customer Data, and consistent with the security requirements set forth in this Section. To the extent applicable,

any backups of Customer Data shall not be considered in calculating any fees levied pursuant to any Underlying Agreement(s).

2.4.3. *Import and Export of Customer Data.* To the extent Customer Data is stored, retained, or otherwise maintained in electronic format in connection with any hosting, infrastructure, or other similar Services, the applicable Governmental Entity or its Authorized Contractors shall have the ability to import or export data or information, including Customer Data, in whole or in part to or from such Services, at no charge, and in such formats as may be acceptable to the Governmental Entity, without interference from Vendor, Vendor Contractors, or Vendor Personnel. In the event a Governmental Entity is unable to successfully import or export Customer Data in whole or in part, Vendor shall assist the Governmental Entity in doing so at no charge. As it relates to the export of such data and information, Vendor shall provide to or ensure the applicable Governmental Entity has obtained an export of any requested Customer Data within a timeframe mutually agreed between the Parties in the format specified by the Governmental Entity.

2.4.4. *Retention/Return/Destruction of Customer Data*. Upon termination or expiration of any Underlying Agreement(s), Vendor may be required to promptly return or destroy, at the applicable Governmental Entity's sole option, all Customer Data, and provide a notarized written statement to the applicable Governmental Entity certifying that all Customer Data under or in Vendor's, Vendor Contractor's, or Vendor Personnel's control or possession has been delivered to the applicable Governmental Entity or destroyed, as requested by the applicable Governmental Entity. To the extent Vendor is required to destroy Customer Data, such Customer Data shall be permanently deleted and shall not be recoverable, according to National Institute of Standards and Technology (NIST)-approved methods. Vendor agrees that in connection with any termination or expiration of any Underlying Agreement(s), Vendor shall not take any action to intentionally erase any Customer Data without first providing prior notice to and consent from the applicable Governmental Entity in writing. On termination or expiration of any Underlying Agreement(s), the applicable Governmental Entity shall, except to the extent otherwise required by applicable laws, rules, regulations, policies, or procedures, including but not limited to record-retention requirements, or as otherwise required for use of any licenses, Services, or Deliverables previously supplied by Vendor, return or destroy, at Vendor's option, all of Vendor's Confidential Information.

2.5. Personnel Safeguards.

2.5.1. *Background Checks.*

2.5.1.1. Floor. Vendor shall conduct nationwide criminal background checks on Vendor Personnel and shall not utilize any such personnel in the performance of any Underlying Agreement(s) who have been convicted of any crime of dishonesty, including fraud, or otherwise convicted of any felony or misdemeanor offense for which incarceration for up to one (1) year is an authorized penalty.

2.5.1.2. Additional Screening. Governmental Entities reserve the right to subject Vendor Personnel to additional background checks at any time prior to or during any engagement. Such background checks may include a work history, financial review, request for criminal history data, or local or state criminal history check, national criminal history check through the Federal Bureau of Investigation (**"FBI"**), or other background check requirement imposed by law, rule, regulation, order, or policy. Vendor Personnel may be required to authorize the release of the results of criminal history checks, including those through the FBI, to one or more Governmental Entities, including OCIO. Such background checks may be conducted by the applicable Governmental Entity or its Authorized Contractor. A Governmental Entity may also require Vendor to conduct a work history or financial review of Vendor Personnel. Vendor shall provide Governmental Entities with these background check results in a mutually agreeable form and manner prior to the commencement of any engagement by Vendor Personnel.

2.5.1.3. Vendor shall be responsible for payment of all costs associated with any and all background checks to which Vendor Personnel are subjected, regardless of whether such background checks are conducted by Vendor or a Governmental Entity or its Authorized Contractor.

2.5.2. *Right to Remove Individuals.* Should a Governmental Entity be dissatisfied with the performance, competence, responsiveness, capabilities, cooperativeness, or fitness for a particular task of any Vendor Personnel, the Governmental Entity may request the replacement of such Vendor Personnel (**"Replacement Request"**). The Replacement Request shall be in writing and upon receipt of the request, Vendor shall make reasonable efforts to furnish a qualified and acceptable replacement within fifteen (15) business days. If the applicable Governmental Entity, in its sole discretion, determines Vendor Personnel pose a potential security risk and notifies Vendor of such security risk in its Replacement Request, Vendor shall immediately remove such individual; any replacement furnished by Vendor in connection with such a request may not perform or provide Services or Deliverables to the applicable Governmental Entity unless and until the applicable Governmental Entity gives its consent to Vendor's use of such replacement. Vendor shall notify OCIO immediately upon receiving a Replacement Request from another Governmental Entity and promptly provide a copy of such Replacement Request to OCIO.

2.5.3. *Security Awareness Training.* Vendor shall promote and maintain an awareness of the importance of securing Customer Property, including Customer Data, among Vendor Personnel.

2.5.4. *Separation of Job Duties.* Vendor shall diligently monitor and enforce separation of job duties, require all Vendor Contractors and Vendor Personnel to execute non-disclosure agreements, and limit access to and knowledge of Customer Property to those Vendor Personnel to which such access and knowledge is

absolutely necessary to provide Services and Deliverables pursuant to any Underlying Agreement(s).

2.5.5. *Non-disclosure/Confidentiality Agreements*. Vendor Personnel may be required to sign a Governmental Entity's standard confidentiality or non-disclosure agreement(s), or other confidentiality or non-disclosure agreement(s) as may be required by applicable law, rule, regulation, or policy.

2.6. Security Breaches.

2.6.1. *Reporting*. Vendor or Vendor Contractors will report to the applicable Governmental Entity and OCIO within two (2) hours of Vendor's or Vendor Contractor's discovery of any actual or suspected Security Breach. Such report must be given in the most expedient time possible and without unreasonable delay. Written confirmation must be sent to the applicable Governmental Entity and OCIO within forty-eight (48) hours of discovery or notification of the actual or suspected Security Breach. Such written confirmation shall include an explanation of the nature of and circumstances surrounding such actual or suspected Security Breach.

2.6.2. *Investigations in Response to Actual or Suspected Breach*. Vendor and Vendor Contractors agree, at their sole expense, to take all steps necessary to promptly remedy any actual or suspected Security Breach and to fully cooperate with the applicable Governmental Entity and OCIO in resolving and mitigating any damage from such actual or suspected Security Breach at Vendor's sole cost. At no additional cost to the applicable Governmental Entity or the State of Iowa, Vendor and Vendor Contractor will fully cooperate with the applicable Governmental Entity, OCIO, and the Authorized Contractors of either of the foregoing in investigating such actual or suspected Security Breach, including reviewing and assisting in reviewing system, application, and access logs, conducting and assisting in conducting forensic audits of relevant systems, imaging and assisting in imaging relevant media, and making personnel available for interview. On notice of any actual or suspected Security Breach, Vendor and Vendor Contractor will immediately institute appropriate controls to maintain and preserve all electronic evidence relating to such actual or suspected Security Breach in accordance with industry best practices. Vendor and Vendor Contractor will deliver to the applicable Governmental Entity and OCIO a root cause assessment and future incident mitigation plan, and deliver a preliminary assessment and plan as soon as practical and regularly maintain and update such assessment and plan throughout the course of any investigation. Vendor agrees that it will not notify any regulatory authority relating to any actual or suspected Security Breach unless the applicable Governmental Entity specifically requests Vendor do so in writing.

2.6.3. *Additional Remedies in the Event of Actual Breach*. Upon the applicable Governmental Entity's determination that a Security Breach involving or relating to Customer Data has occurred, Vendor and Vendor Contractors shall fully cooperate with the applicable Governmental Entity and OCIO in fully rectifying/responding to such Security Breach, including notifying all of the Governmental Entity's affected users. The applicable Governmental Entity shall determine, in its sole discretion, the content and means of delivery of any such

notifications. Notwithstanding any provision in these Security terms or any Underlying Agreement(s), Vendor will be solely responsible and liable for all costs, expenses, damages, fines, penalties, taxes, assessments, legal fees, claims, service fees, and any and all other amounts of any kind or nature whatsoever (including the reasonable value of time of the Iowa Attorney General's Office or the costs, expenses and attorney fees of other counsel retained by the State or any other Governmental Entity) related to, arising out of, or incurred by or on behalf of any Governmental Entity as a result of, any Security Breach caused directly or indirectly, in whole or in part, by Vendor Personnel, including the cost of: notifying affected individuals and businesses or reporting to applicable regulators or Governmental Entities (including preparation, printing, mailing and delivery); opening and closing accounts, printing new checks, embossing new cards; forensic and other audits, investigations, public relations services, call center services, websites and toll-free numbers for assisting affected individuals; obtaining credit-monitoring services and identity-theft insurance for any person or entity whose information has or may have been acquired or compromised; and all other costs associated with corrective or other actions that are taken to mitigate or address the Security Breach. Vendor will reimburse or pay to the applicable Governmental Entity all such expenses, fees, damages, and all other amounts within fifteen (15) business days of the date of any written demand or request delivered to Vendor.

2.7. Business Continuity/Disaster Recovery.

2.7.1. *Creation, Maintenance and Testing.* Vendor and Vendor Contractors shall maintain a Business Continuity and Disaster Recovery Plan for all Services provided hereunder (**"Plan"**), and implement such plan in the event of any unplanned interruption of Services. Vendor or Vendor Contractors shall provide Governmental Entities upon request, with a copy of Vendor's or Vendor Contractor's current Plan, revision history, and any reports or summaries relating to past testing of the Plan. Vendor and Vendor Contractors shall actively test, review, and update the Plan on at least an annual basis using American Institute of Certified Public Accountants standards and other industry best practices as guidance. Vendor and Vendor Contractors shall promptly provide the applicable Governmental Entities with copies of all reports and/or summaries resulting from any testing of the Plan and with copies of any resulting updates to the Plan. Throughout the term of any Underlying Agreement(s), Vendor and Vendor Contractors shall maintain disaster avoidance procedures designed to safeguard Customer Data and the accessibility and availability of the Services or Deliverables.

2.7.2. *Activation of Plan*. Vendor and Vendor Contractors shall immediately notify any adversely affected Governmental Entities and OCIO of any disaster or other event in which the Plan is activated. If Vendor or Vendor Contractors fail to reinstate Services or Deliverables within the time periods set forth in the Plan, in addition to any other remedies available to applicable Governmental Entities hereunder, the applicable Governmental Entity may immediately terminate the Underlying Agreement or adversely affected Purchasing Instrument(s) without any penalty or liability. Without limiting Vendor's obligations under this

Agreement, whenever a disaster causes Vendor or Vendor Contractors to allocate limited resources between or among Vendor's or Vendor Contractor's customers, Governmental Entities procuring Services or Deliverables hereunder shall receive at least the same treatment as comparable Vendor or Vendor Contractor's customers with respect to such limited resources. The provisions of any force majeure clause in any Underlying Agreement(s) shall not limit Vendor's obligations under this Section.

2.8. Ancillary Agreements and Non-Disclosure Agreements. Vendor or Vendor Contractors will execute any agreements to address any compliance, legal, confidentiality, or privacy concerns that may be unique to an applicable Governmental Entity making purchases hereunder, such as a Business Associate Agreement (**"BAA"**) or Criminal Justice Information System (**"CJIS"**) Security Addendum, or any other non-disclosure or confidentiality agreements in connection with this Agreement or any related agreement deemed necessary by the applicable Governmental Entity (**"Ancillary Agreement(s)"**).

2.9. Transition Assistance. Vendor agrees that in connection with any termination or expiration of any Underlying Agreement(s), Vendor will continue to perform such Services or provide Deliverables under any Underlying Agreement as the applicable Governmental Entity may request for a transition period up to 365 days from the effective date of termination or expiration of any Underlying Agreement. As part of any such request, the applicable Governmental Entity will inform Vendor of the number of days during which the Vendor will continue to provide such Services or Deliverables, and perform transition and other related services under this Section (the **"Transition Period"**). During the Transition Period, Vendor will take all actions as may be necessary or requested by the applicable Governmental Entity to accomplish a complete and timely transition, including but not limited to a full migration of all Customer Data from Vendor to the applicable Governmental Entity or its Authorized Contractor(s) hired or utilized by the State to provide any replacement or similar services related to the services (the **"New Contractor"**). Vendor will use its best efforts to cooperate with the applicable Governmental Entity and any New Contractor, and to fully comply with all requests of the same to affect a smooth and timely transition and to ensure there is no interruption of any services, information, or transactions provided or conducted through the Services or Deliverables. Vendor agrees that it will perform all transition services in good faith and in a professional and businesslike manner, and shall comply with all requests of the applicable Governmental Entity and any New Contractor to assist in the effort to accomplish a successful, seamless, and unhindered transition of the Services or Deliverables, migration all Customer Data or information, and transfer of Vendor's responsibilities under any Underlying Agreement(s). Vendor will perform all transition services on an expedited basis, as determined by the applicable Governmental Entity. During the Transition Period, the applicable Governmental Entity agrees to pay to Vendor any fees to which Vendor would be entitled under any Underlying Agreement for Services or Deliverables performed during such period; provided such Underlying Agreement was not terminated due to Vendor's breach of such Underlying Agreement or for reasons related to the non-appropriation of funds as defined by such Underlying Agreement, and Vendor continues to be in full compliance with all terms, conditions, provisions and requirements of any Underlying Agreement and these Security Terms. In the event a Governmental Entity's request for transition assistance does not require Vendor to continue providing all of the Services or Deliverables under any Underlying Agreement,

the Parties shall negotiate in good faith an equitable adjustment in the fees which are otherwise payable to Vendor for such Services or Deliverables as the State requests the Vendor to provide.

2.10. Vendor shall include the terms and conditions in this Section in all of its contracts, subcontracts, or other agreements with Vendor Contractors.

IN WITNESS WHEREOF, the Parties have caused their respective duly authorized representatives to execute these Security Terms, which is effective as of the last date of signature hereto.

STATE OF IOWA, acting by and through the **Iowa Department of Administrative Services**	**[Name of Vendor]** IDEMIA I&S
By: Craig Trotter	By:
Name: Craig Trotter	Name: Casey Mayfield
Title: Purchasing Agent III	Title: Senior Vice President Justice and Public Safety