Attachment 16
State of Iowa 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.*, Delaware)], 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 [name of state agency]("**State of Iowa**" or "**State**") These security terms shall apply in addition to any other terms and conditions agreed to by the Parties, 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. These terms shall only apply only to the extent applicable to the applicable engagement.

1. For purposes of these security terms, the term "**Confidential Information**" means, subject to the provisions of these security terms, the underlying agreement, and any applicable State and federal laws and regulations, including but not limited to Iowa Code Chapter 22, any confidential or proprietary information or trade secrets disclosed by either Party to the other 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. Any information provided to Vendor by the State or any other Governmental Entity or otherwise accessed, collected, processed, stored, or transmitted by Vendor in connection with the underlying agreement, or any summaries, records, descriptions, modifications, compilations, negatives, drawings, adaptations and other documents or materials prepared by Vendor from such information (**"Work Product"**), shall be considered confidential by Vendor **("State of Iowa Confidential Information"** or **"State Confidential Information")**.

2. For purposes of these security terms, the term "**Governmental Entity**" means any governmental entity as defined in Iowa Code Section 8A.101, or any successor provision to that section, existing now or in the future.

3. **Data Ownership.** All data, including all State Confidential Information, shall be and remain the sole and exclusive property of the State.

4. **Vendor's access to and use of State data.** Vendor and any of its subcontractors, agents, or other third parties acting on its behalf shall not use any State of Iowa Confidential Information for any purpose other than fulfilling Vendor's express obligations and duties pursuant to the underlying agreement, in accordance with the terms and conditions set forth in these security terms.

5. **Data Protection.** Protection of personal privacy and data shall be an integral part of the business activities of Vendor to ensure there is no inappropriate or unauthorized use of the State's Confidential Information at any time. To this end, Vendor shall safeguard the confidentiality, integrity and availability of the State's Confidential Information. In so doing, Vendor shall comply with the following conditions:

5.1. Vendor shall implement and maintain appropriate administrative, technical and organizational security measures to safeguard against unauthorized access, disclosure or theft of State Confidential Information. Such security measures shall be in accordance with recognized industry practice (including, NIST 800-53 Revision 4 and ISO27001:2013 standards and controls) and not less stringent than the measures Vendor applies to its own personal data and non-public data of similar kind. Additionally, such securities measures, to the extent applicable, shall comply with, and shall enable the State to at all time comply fully with, all applicable federal, state, and local laws, rules, ordinances, codes, regulations and orders related to such security measures or other date security or safeguarding requirements.

5.2. All State Confidential Information shall be encrypted at rest and in transit with controlled access, leveraging, to the extent applicable TLS v. 1.1 or 1.2. Unless otherwise expressly provided herein or otherwise agreed to by the Parties in writing, Vendor is responsible for encryption of all State Confidential Information. 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 State Confidential Information, unless the State approves in writing the storage of Confidential Information on a Vendor portable device.

5.3. At no time shall any State Confidential Information be copied, disclosed or retained by Vendor, or any subcontractor, agent, or any party related to Vendor, for use in any transaction that does not include the State.

6. Data Location. Vendor shall provide hosting services to the State and Governmental Entities solely from data centers located in the continental United States of America. Storage of State Confidential Information at rest and all backups shall be located solely in data centers located in the continental United States of America. Vendor shall not allow its personnel or subcontractors to store State Confidential Information on any portable devices, including personal computers, tablets, or cell phones, except for devices that are used and permanently stored at all times only at its continental United States of America data centers. Vendor shall permit its personnel and subcontractors to access State Confidential Information 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.

7. Security Incident/Notification.

7.1. Vendor will notify the State within two (2) hours of Vendor's discovery of any actual or suspected breach of confidentiality, privacy or security (or any unauthorized access) with regard to any State Confidential Information, and/or any breach of Vendor's or the State's data security procedures, which include, but are not limited to, instances in which internal personnel access systems in excess of their user rights or use the systems inappropriately, any breach of security as defined in Iowa Code Chapter 715C, and any other breach of security as defined by any applicable law, rule, or regulation. Such notification to the State must be given in the most expedient time possible and without unreasonable delay. Written confirmation must be sent within forty-eight (48) hours of discovery or notification of the breach or suspected breach.

7.2. Investigations and Remedies. Vendor agrees, at its sole expense, to take all steps necessary to promptly remedy any breach described in section 7.1, above, and to fully cooperate with the State in resolving such breach and mitigating any damage from such breach at Vendor's sole cost. At no additional cost to the State, Vendor will fully cooperate with the State in investigating the breach, including, but not limited to, providing to the State and assisting the State in reviewing system, application, and access logs, conducting forensic audits of relevant systems, imaging relevant media, and making personnel available for interview. On notice of any actual or suspected breach, Vendor will immediately institute appropriate controls to maintain and preserve all electronic evidence relating to the breach in accordance with industry best practices. Vendor will deliver to the State a root cause assessment and future incident mitigation plan with regard to any breach of security or unauthorized access affecting State Confidential Information. Vendor will 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 based on any findings. Vendor agrees that it will not notify any regulatory authority or relating to any such security breach on behalf of the State unless the State specifically requests in writing that Vendor do so. Vendor and the State will work together to formulate a plan to rectify all security breaches.

7.3. Additional Procedures in the Event of Security Breach. Upon the State's determination that a breach of security (including but not limited to any Breach of Security as defined in Iowa Code Chapter 715C, and any other breach of security as defined by any applicable law, rule, or regulation) involving or relating to any State Confidential Information has occurred or is reasonably possible, Vendor shall fully cooperate with the State in rectifying any breach or misuse, including notifying all of the States affected users. The State shall determine, in its sole

discretion, the content and means of delivery of the user notice. Notwithstanding any provision in these security terms or any other agreement between the Parties to the contrary, 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, without limitation, the reasonable value of time of the Iowa Attorney General's Office and the costs, expenses and attorney fees of other counsel retained by any Indemnitee) related to, arising out of or incurred by or on behalf of the State as a result of, any security breach caused directly or indirectly, in whole or in part, by Vendor, its affiliates, employees, or subcontractors, including, but not limited to, the costs of notifications of affected individuals and businesses and any applicable regulators or governmental entities (including, preparation, printing, mailing and delivery); the cost of opening and closing accounts, printing new checks, embossing new cards; the costs of forensic and other audits, investigations, public relations services, call center services, websites and toll-free numbers for affected individuals; the costs of 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 State all such expenses, fees, damages and all other amounts within fifteen (15) business days of the date of any written demand or request delivered by the State to Vendor.

8. Import/Export/Deletion of Confidential Information.

8.1. Import and Export of Data. To the extent State Confidential Information is stored or accessible in electronic format in connection with the hosting services, the State shall have the ability to import or export data and information (including but not limited to State Confidential Information) in whole or in part from hosting services, at no charge to the State, and in such formats as may be acceptable to the State or any Governmental Entity, without interference from Vendor. This includes the ability for the State to import or export, or have imported or exported, such information and data to/from/by other contractors. In the event the State is unable to successfully import or export data and information in whole or in part, Vendor shall assist the State in doing so upon the State's request, at no charge to the State; as it relates to the export of such data and information, Vendor shall provide to or ensure the State has obtained an export of any requested data and information within one day of any request in the format specified by the State.

8.2. Destruction of Data and Return of other Confidential Information. In addition to the requirements of Section 7.1, on the State of Iowa's written request or upon expiration or termination of the underlying agreement, subject to the requirements of Section 9 (Termination/Expiration of Service), Vendor will promptly return (including but not limited to as it relates to State Confidential Information that is not stored or accessible in electronic format in connection with the hosting services) or destroy, at the State's option, all State Confidential Information and provide a notarized written statement to the State certifying that all State Confidential Information has been delivered to the State or destroyed, as requested by the State. To the extent Vendor is required to destroy any State of Iowa Confidential Information, State Confidential Information shall be permanently deleted and shall not be recoverable, according to National Institute of Standards and Technology (NIST)-approved methods. On termination or expiration of this Agreement, the State of Iowa shall, except to the extent otherwise required by applicable laws, rules, procedures or State record retention requirements, return or destroy, at Vendor's option, all of Vendor's Confidential Information (excluding items required for use of any licenses or deliverables previously supplied by Vendor).

9. Termination/Expiration of Service.

9.1. Transition Assistance. Vendor agrees that in connection with any termination or expiration of the underlying agreement, Vendor will continue to perform such services under the underlying

agreement as the State may request for a transition period up to 365 days from the effective date of termination or expiration of the underlying agreement. As part of the State's request, the State will inform the Vendor of the number of days during which the Vendor will continue to host and provide access to the hosting services and State Confidential Information, 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 State to accomplish a complete and timely transition, including but not limited to a full migration of State of Iowa Confidential Information, from the Vendor to the State and/or to any contractor 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 State and any New Contractor, and to fully comply with all requests of the State to effect a smooth and timely transition and to ensure there is no interruption of any services, information or transactions provided or conducted through the services. 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 State and any New Contractor to assist in the effort to accomplish a successful, seamless and unhindered transition of the services, migration of State Confidential Information, and transfer of Vendor's responsibilities under the underlying agreement. Vendor will perform all transition services on an expedited basis, as determined by the State. During the Transition Period, the State agrees to pay to Vendor any fees to which Vendor would be entitled under the underlying agreement for services performed during such period; provided the underlying agreement was not terminated due to Vendor's breach of the agree or pursuant to section 4 (Termination for Non-Appropriation), and Vendor continues to be in full compliance with all terms, conditions, provisions and requirements of the underlying agreement. In the event the State's request for transition assistance does not require Vendor to continue providing all of the services under the underlying agreement, the parties shall negotiate in good faith an equitable adjustment in the fees which are otherwise payable to Vendor for such services as the State requests the Vendor to provide.

9.2. Retention of State Data. Vendor agrees that in connection with any termination or expiration of the underlying agreement, Vendor shall not take any action to intentionally erase any State data for a period of at least 90 days, unless otherwise directed by the State in accordance with Section 9.1.

10. **Background Checks.** Vendor shall conduct nationwide criminal background checks and not utilize any staff, including subcontractors, to fulfill the obligations of the underlying agreement who have been convicted of any crime of dishonesty, including but not limited to criminal fraud, or otherwise convicted of any felony or misdemeanor offense for which incarceration for up to 1 year is an authorized penalty. Vendor shall promote and maintain an awareness of the importance of securing the State Confidential Information among the Vendor's employees, affiliates, subcontractors, and agents.

11. **Vendor Personnel.** Should the State be dissatisfied with the performance, competence, responsiveness, capabilities, cooperativeness, or fitness for a particular task of any Vendor personnel assigned by Vendor to perform or provide services or deliverables, the State of Iowa may request the replacement of such Vendor Personnel. 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 State, in its sole discretion, determines Vendor personnel pose a potential security risk and notifies Vendor of such security risk in its request for replacement, 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 State unless and until the State gives its consent to Vendor's use of such replacement.

12. **Non-disclosure and Separation of Duties.** Vendor shall diligently monitor and enforce separation of job duties, require non-disclosure agreements, and limit staff knowledge of State Confidential Information to that which is absolutely necessary to perform job duties.

13. Security Disclosures, Audits, and Compliance.

13.1. Compliance. Annually throughout the term of the underlying agreement, Vendor shall obtain and provide the State with the following, at no additional cost to the State: a) an independent, third-party certificate of audit certifying that the services comply with NIST 800-53, Revision 4 controls; b) ISO/IEC 27001:2005 certification; c) test or assessment results of an independent, third party assessment of application scans using the Open Web Application Security Project (OWASP) Top Ten List; d) test results of a penetration test conducted by an independent, third-party firm; e) a copy of Vendor's annual SOC 2 type 2 report (for all Trust Services Principles); and f) a Vendor produced remediation plan resulting from items a through e, inclusive.

13.2. Security Audit by the State. During the Term, the State or its third party designee may, but is not obligated to, perform audits of Vendor's environment, including unannounced penetration and security tests, as they relate to the receipt, maintenance, use or retention of the State's Confidential Information. Any of the State's regulators (and any federal agencies providing grant funds used to pay for services, 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.

13.3. Ongoing Security Testing/Compliance. 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 the State. In addition, Vendor shall disclose its non-proprietary security processes and technical limitations to the State, such that adequate protection and flexibility can be attained between the State and Vendor. For example, Vendor shall disclose its security processes with respect to virus checking and port sniffing to the State such that the State is capable of identifying necessary compensating controls to adequately safeguard and protect its data, information, and systems.

13.4. Access to Security Logs and Reports. Vendor shall provide security logs and reports to the State 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 the underlying agreement.

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 **Department of Administrative Services:**	**[Name of Vendor]**
By: _____	By: _____
Name: _____	Name: _____
Title: _____	Title: _____