**Information Security Provisions**

**Definitions**

“Authorized Persons” means (i) Authorized Employees; and (ii) Service Provider’s contractors, subcontractors, agents, outsourcers and auditors to this Agreement who have a need to know or otherwise access any Restricted Use Information that enables Service Provider to perform its obligations under this Agreement, and who are bound in writing by confidentiality obligations sufficient to protect Restricted Use Information in accordance with the terms and conditions of this Agreement.

“Restricted Use Information” means information provided to Service Provider by or at the direction of Customer, or to which access was provided to Service Provider by or at the direction of Customer, in the course of Service Provider’s performance under this Agreement that: (i) identifies or can be used to identify an individual (including, without limitation, names, signatures, addresses, telephone numbers, e-mail addresses and other unique identifiers); or (ii) can be used to authenticate an individual (including, without limitation, employee identification numbers, government-issued identification numbers, passwords or PINs, financial account numbers, credit report information, biometric or health data, answers to security questions and other personal identifiers).

“Security Breach” means (i) any act or omission that materially compromises either the security, confidentiality or integrity of Restricted Use Information or the physical, technical, administrative or organizational safeguards put in place by Service Provider (or any Authorized Persons) that relate to the protection of the security, confidentiality or integrity of Restricted Use Information, or (ii) receipt of a complaint in relation to the privacy practices of Service Provider (or any Authorized Persons) or a breach or alleged breach of this Agreement relating to such privacy practices.

**Standard of Care**

1. Service Provider acknowledges and agrees that, in the course of its engagement by Customer, Service Provider may receive or have access to Restricted Use Information. Service Provider shall comply with the terms and conditions set forth in this Agreement in its collection, receipt, transmission, storage, disposal, use and disclosure of such Restricted Use Information and be responsible for the unauthorized collection, receipt, transmission, access, storage, disposal, use and disclosure of Restricted Use Information under its control or in its possession by all Authorized Persons. Service Provider shall be responsible for, and remain liable to, Customer for the actions and omissions of all Authorized Persons that are not Authorized Employees concerning the treatment of Restricted Use Information as if they were Service Provider’s own actions and omissions.
2. Restricted Use Information is deemed to be Confidential Information of Customer and is not Confidential Information of Service Provider. In the event of a conflict or inconsistency between this Provision and other provisions of this Agreement, the terms and conditions set forth in this Provision shall govern and control.
3. In recognition of the foregoing, Service Provider agrees and covenants that it shall:
	1. keep and maintain all Restricted Use Information in strict confidence, using such degree of care as is appropriate to avoid unauthorized access, use or disclosure;
	2. use and disclose Restricted Use Information solely and exclusively for the purposes for which the Restricted Use Information, or access to it, is provided pursuant to the terms and conditions of this Agreement, and not use, sell, rent, transfer, distribute, or otherwise disclose or make available Restricted Use Information for Service Provider’s own purposes or for the benefit of anyone other than Customer, in each case, without Customer’s prior written consent; and
	3. not, directly or indirectly, disclose Restricted Use Information to any person other than its Authorized Employees/Authorized Persons, including any subcontractors, agents, outsourcers or auditors (an “Unauthorized Third Party”), without express written consent from Customer unless by applicable law and/or the Kansas Open Records Act (K.S.A. 45-215 *et. seq.)*, in which case, Service Provider shall (1) notify Customer before such disclosure or as soon thereafter as reasonably possible; (2) be responsible for and remain liable to Customer for the actions and omissions of such Unauthorized Third Party concerning the treatment of such Restricted Use Information as if they were Service Provider’s own actions and omissions; and (3) require the Unauthorized Third Party that has access to Restricted Use Information to execute a written agreement agreeing to comply with the terms and conditions of this Agreement relating to the treatment of Restricted Use Information.
4. Insurance Requirements. The Service Provider shall procure and maintain insurance against claims for injuries to persons, which may arise from, or in connection to, the fulfillment of this Agreement, by the Service Provider, its agents, representatives, employees, or Subcontractors. The insurance shall be secured by the Service Provider, at the Service Provider’s expense, and maintained in force, at all times during the term of this Agreement, and, for any claims-made (as opposed to occurrence-based) policies, for a period of not less than two (2) years thereafter.
	1. Minimum Coverage. Errors and Omissions, or Professional Liability Insurance, or Insurance by any other name, covering the following:
		1. All acts, errors, omissions, negligence, infringement of intellectual property (except patent and trade secret) in an amount not less than $1,000,000 per occurrence, and as an annual aggregate.
		2. Network security and privacy risks, including, but not limited to, unauthorized access, failure of security, breach of privacy, wrongful disclosure, collection, or other negligence in the handling of confidential information, related regulatory defense, and penalties in an amount not less than

$1,000,000 per occurrence, and as an annual aggregate.

* + 1. Data breach expenses, in an amount based on the number of Restricted Use Information records: 1 through 3000 records minimum coverage of $400,000 per occurrence; 3001 through 100,000 records minimum coverage of $1,000,000 per occurrence; 100,001 through 1,000,000 records minimum coverage of $5,000,000 per occurrence or greater than 1,000,000 records minimum coverage of $10,000,000 per occurrence, and payable, whether incurred by the Customer or the Service Provider; for and on behalf of the Customer, including, but not limited to: Consumer notification, whether or not required by law; Forensic investigations; Public relations and crisis management fees; and Credit or identity monitoring, or similar remediation services. The policy shall affirm coverage for contingent bodily injury and property damage arising from the failure of the Service Provider’s technology services, or an error, or omission, in the content of, and information from, the Service Provider. If a sub-limit applies to any element of the coverage, the certificate of insurance must specify the coverage section and the amount of the sub- limit.
	1. Other Provisions. Unless explicitly waived by the Customer, the insurance policies shall contain, or be endorsed to contain, the following provisions:
		1. The Service Provider’s insurance coverage shall be the primary and contributory. Any insurance or self-insurance maintained by the Department for its officers, agents, and employees shall be in excess of the Provider's insurance and shall not contribute to it.
		2. The Service Provider's insurance shall apply separately to each insured against whom claim is made or suit is brought, except with respect to the limits of the insurer's liability.
		3. The Service Provider shall furnish the Customer with certificates of insurance, and with those endorsements, if any, affecting coverage, required by these Insurance Requirements. The certificates and endorsements for each insurance policy are to be signed by a person authorized by the insurer to bind coverage on its behalf. All certificates and endorsements are to be received and approved by the Customer before this Agreement commences. The Customer reserves the right to require complete, certified copies of all required insurance policies at any time.
		4. All policies should contain a revised cancellation clause allowing thirty (30) days’ notice to the Customer in the event of cancellation for any reason, including nonpayment.
		5. The Customer will not grant the Service Provider, or any sub-contractor of the Service Provider, “Additional Insured” status and the Customer will not grant any Service Provider a “Waiver of Subrogation”.

**Compliance**

1. Service Provider represents and warrants that its collection, access, use, storage, disposal and disclosure of Restricted Use Information does and will comply with all applicable federal and state privacy and data protection laws, as well as all other applicable regulations and directives.
2. Without limiting Service Provider’s obligations under paragraph (a) of this provision, Service Provider shall implement administrative, physical and technical safeguards to protect Restricted Use Information that are no less rigorous than accepted industry practices including the International Organization for Standardization (ISO) 27000 series standards, the Control Objectives for Information and related Technology (COBIT) standards, the National Institute of Standards and Technology (NIST) 800-53v5 –or other applicable industry standards for information security, and shall ensure that all such safeguards, including the manner in which Restricted Use Information is collected, accessed, used, stored, processed, disposed of and disclosed, comply with applicable data protection and privacy laws, as well as the terms and conditions of this Agreement.
3. If, in the course of its engagement by Customer, Service Provider has access to or will collect, access, use, store, process, dispose of or disclose credit, debit or other payment cardholder information, Service Provider shall at all times remain in compliance with the Payment Card Industry Data Security Standard (“PCI DSS”) requirements, including remaining aware at all times of changes to the PCI DSS and promptly implementing all procedures and practices as may be necessary to remain in compliance with the PCI DSS, in each case, at Service Provider’s sole cost and expense.
4. At a minimum, Service Provider’s safeguards for the protection of Restricted Use Information shall include:
	1. limiting access of Restricted Use Information to Authorized Persons.
	2. securing business facilities, data centers, paper files, servers, back-up systems and computing equipment, including, but not limited to, all mobile devices and other equipment with information storage capability.
	3. implementing network, device application, database and platform security
	4. securing information transmission, storage and disposal.
	5. implementing authentication and access controls within media, applications, operating systems and equipment
	6. encrypting Restricted Use Information stored on any mobile media.
	7. encrypting Restricted Use Information transmitted over public or wireless networks
	8. strictly segregating Restricted Use Information from information of Service Provider or its other customers so that Restricted Use Information is not commingled with any other types of information
	9. implementing appropriate personnel security and integrity procedures and practices, including, but not limited to, conducting background checks consistent with applicable law
	10. providing appropriate privacy and information security training to Service Provider’s Authorized Persons.
5. During the term of each Authorized Person’s employment by Service Provider, Service Provider shall at all times cause such Authorized Persons to abide strictly by Service Provider’s obligations under this Agreement and Service Provider’s standard policies and procedures. Service Provider further agrees that it shall maintain a disciplinary process to address any unauthorized access, use or disclosure of Restricted Use Information by any of Service Provider’s officers, partners, principals, employees, agents or contractors. Upon Customer’s written request, Service Provider shall promptly identify for Customer in writing all Authorized Persons as of the date of such request.
6. Upon Customer’s written request, Service Provider shall provide Customer with a network diagram that outlines Service Provider’s information technology network infrastructure and all equipment used in to fulfill obligations of this Agreement, including, without limitation:
	1. connectivity to Customer and all third parties who may access Service Provider’s network to the extent the network contains Restricted Use Information
	2. all network connections including remote access services and wireless connectivity
	3. all access control devices (for example, firewall, packet filters, intrusion detection and access-list routers)
	4. all back-up or redundant servers
	5. permitted access through each network connection.
7. Upon Customer’s declaration of any of the following federally regulated or controlled data, Service Provider agrees to comply with all additional applicable compliance requirements.
	1. Federal Tax Information (FTI). This data classification applies to information provided to the Customer directly from the Internal Revenue Service (IRS). The FTI data classification has extensive compliance requirements; these requirements are detailed in IRS Publication 1075, this publication and supporting documents can found at: https://[www.irs.gov/privacy-disclosure/safeguards-program.](http://www.irs.gov/privacy-disclosure/safeguards-program) NOTE: any agreement that directly or may indirectly include access to data subject to this classification, must include Exhibit 7 of IRS Publication 1075. The Exhibit 7 language can also be found at https://www.irs.gov/pub/irs-pdf/p1075.pdf
	2. Social Security Information (SSA). This data classification applies to information provided to the Customer directly from the SSA or from the State Transfer Component (STC). The SSA data classification has common cybersecurity compliance requirements, however the publication detailing these requirements is not publicly available. Upon contract award this publication will be provided. NOTE: any agreement that directly or may indirectly include access to data subject to this classification, must include the language provided by the SSA, which is provided at https://oits.ks.gov/info-security/assurance-and-compliance- resources.
	3. Office of Child Support Enforcement (OCSE) Requirements for National Directory of New Hires (NDNH). This data classification applies to information provided to the Customer directly from the IRS. The OCSE or NDNH data classification requires that any agreement that directly or may indirectly include access to data subject to this classification, must include specific language that can be found at https://oits.ks.gov/info-security/assurance-and-compliance-resources.
	4. Health Information Portability Accountability Act (HIPAA). This data classification applies to information declared as Personal Healthcare Information (PHI) by the Customer. The HIPAA data classification requires that any agreement that directly or may indirectly include access to PHI requires a Business Associate Agreement (BAA). The BAA must be incorporated and agreed to prior to execution of the agreement.
	5. Kansas Criminal Justice Information Systems (KCJIS). This data classification applies to information declared as Criminal Justice Information (CJI) by the Customer. The CJI data classification requires that any agreement that directly or may indirectly include access to CJI requires Security Addendum addressing CJI. Pursuant to Title 28 of the Code of Federal Regulations: § 20.33 Dissemination of criminal history record information. a) Criminal history record information contained in the Interstate Identification Index System and the Fingerprint Identification Records System (FIRS) may be made available: 1) To criminal justice agencies for criminal justice purposes, which purposes include the screening of employees or applicants for employment hired by criminal justice agencies. 2) To noncriminal justice governmental agencies performing criminal justice dispatching functions or data processing/information services for criminal justice agencies; and 3) To private contractors pursuant to a specific agreement with an agency identified in paragraphs (a)(1) or (a)(6) of this section and for the purpose of providing services for the administration of criminal justice pursuant to that agreement. The agreement must incorporate a security addendum approved by the Attorney General of the United States, which shall specifically authorize access to criminal history record information, limit the use of the information to the purposes for which it is provided, ensure the security and confidentiality of the information consistent with these regulations, provide for sanctions, and contain such other provisions as the Attorney General may require. The power and authority of the Attorney General hereunder shall be exercised by the FBI Director (or the Director’s designee). KCJIS policy and regulatory requirements can be found at https://cjisaudit.khp.ks.gov/launchpad/cjisdocs/docs.cgi?cat\_id=10.

(vi) Kansas Information Technology Executive Committee (ITEC) and Customer Policies. Regardless of data classification, Service Provider agrees to comply with all applicable ITEC and Customer policies. When policies, agreements, regulation or law are in conflict, the more stringent requirement applies. ITEC Policies can be found at https://oits.ks.gov/info-security/assurance-and-compliance-resources.

(h) Compliance Oversight. Upon Customer’s written request, to confirm Service Provider’s compliance with this Agreement, as well as any applicable laws, regulations and industry standards, Service Provider grants Customer or, upon Customer’s election, a third party on Customer’s behalf, permission to perform an assessment, audit, examination or review of all controls in Service Provider’s or Authorized Person’s physical and/or technical environment in relation to all Customer Information being handled and/or services being provided to Customer pursuant to this Agreement. Service Provider shall fully cooperate with such assessment by providing access to knowledgeable personnel, physical premises, documentation, infrastructure and application software that processes, stores or transports Customer Information for Customer pursuant to this Agreement. In addition, upon Customer’s written request, Service Provider shall provide Customer with the results of any audit by or on behalf of Service Provider performed that assesses the effectiveness of Service Provider’s information security program as relevant to the security and confidentiality of Customer Information shared during the course of this Agreement.

**Information Security Management**

1. Offshore sourcing. Offshore sourcing either directly or through Service Provider’s contractors, subcontractors, or agents for technology services, technology support services, data storage or data processing of any kind is prohibited without written consent of the Customer.
2. Return or destruction of Customer Information. At any time during the term of this Agreement at the Customer’s written request or upon the termination or expiration of this Agreement for any reason, Service Provider shall, and shall instruct all Authorized Persons to, promptly return to the Customer all copies, whether in written, electronic or other form or media, of Customer Information in its possession or the possession of such Authorized Persons, or securely dispose of all such copies, and certify in writing to the Customer that such Customer Information has been returned to Customer or disposed of securely. Service Provider shall comply with all reasonable directions provided by Customer with respect to the return or disposal of Personal Information.
3. Security breach.
	1. Service Provider shall: (1) provide Customer with the name and contact information for an employee of Service Provider who shall serve as Customer’s primary security contact and shall be available to assist Customer twenty-four (24) hours per day, seven (7) days per week as a contact in resolving obligations associated with a Security Breach; (2) provide notification in accordance with all applicable federal regulatory compliance requirements and notify Customer of a Security Breach as soon as practicable, but no later than twenty-four (24) hours after Service Provider becomes aware of it.
4. Immediately following Service Provider’s notification to Customer of a Security Breach, the parties shall coordinate with each other to investigate the Security Breach. Service Provider agrees to reasonably cooperate with Customer in Customer’s handling of the matter, including, without limitation: (1) assisting with any investigation; (2) providing Customer or Customer’s agent with physical access to the facilities and operations affected; (3) facilitating interviews with Service Provider’s employees and others involved in the matter; and (4) making available all relevant records, logs, files, data reporting and other materials required to comply with applicable law, regulation, industry standards or as otherwise reasonably required by Customer.
5. Service Provider shall take reasonable steps to/use best efforts to immediately remedy any Security Breach and prevent any further Security Breach at Service Provider’s expense in accordance with applicable privacy rights, laws, regulations and standards. Service Provider shall reimburse Customer for reasonable costs incurred by Customer in responding to, and mitigating damages caused by, any Security Breach, including all costs of notice and/or remediation.
6. Service Provider agrees that it shall not inform any third party of any Security Breach without first obtaining Customer’s prior written consent, other than to inform a complainant that the matter has been forwarded to Customer’s legal counsel. Further, Service Provider agrees that Customer shall have the sole right to determine: (1) whether notice of the Security Breach is to be provided to any individuals, regulators, law enforcement agencies, consumer reporting agencies or others as required by law or regulation, or otherwise in Customer’s discretion; and (2) the contents of such notice, whether any type of remediation may be offered to affected persons, and the nature and extent of any such remediation.
7. Service Provider agrees to reasonably cooperate at its own expense with Customer in any litigation or other formal action deemed reasonably necessary by Customer to protect its rights relating to the use, disclosure, protection and maintenance of Customer Information.
8. In the event of any Security Breach, Service Provider shall promptly use its reasonable efforts to prevent a recurrence of any such Security Breach.
9. Service Provider shall maintain during the term of the agreement, a security policy that explicitly addresses and provides guidance to employees and non-employee workers to ensure the confidentiality, integrity and availability of information and systems maintained or processed by Service Provider. The policies shall be approved by senior management and contain penalties or sanctions for non-compliance. The Service Provider’s security policy shall provide a framework for information security management within its overall organization. That policy must have an explicit section on the handling and management of customer data. Explicit procedures must exist that describe how customer data is to be managed, including disposal and destruction of data after its useful life.
10. Personnel Screening.
	1. Service Provider shall ensure that written confidentiality agreements are signed by all employees, non- employee workers, consultants, agents, temporary workers and other persons, such as third-party vendors and subcontractors, who may have access to Customer data, systems, networks or facilities.
	2. Service Provider shall perform pre-employment screening for all employees, non-employee workers, consultants, temporary workers and other persons, such as vendors, hired or engaged after the date of this agreement and who may provide services to or for the Customer. The screening process must incorporate a list of disqualifiers, which must be positively adjudicated before unsupervised access to Customer data, systems, networks or facilities is authorized.
	3. a copy of adjudication disposition shall be maintained in personnel files.
	4. A copy of the Service Provider’s list of disqualifiers shall be provided to the Customer.
11. Customer retains the right to reject any of the Service Provider's Authorized Persons whose abilities and qualifications, in the Customer’s judgment, are not appropriate for the performance of this Agreement. In considering the Service Provider's employees' abilities and qualifications, the Customer shall act reasonably and in good faith.
12. During the course of this Agreement, the Customer reserves the right to require the Service Provider to reassign or otherwise remove any of its employees found unacceptable by the Customer. In considering the Service Provider's employees' acceptability, the Customer shall act reasonably and in good faith.
13. In signing this Agreement, the Service Provider certifies to the best of its knowledge and belief that it, and all persons associated with this Agreement, including any Authorized Persons, including persons or corporations who have critical influence on or control over this Agreement, are not presently debarred, suspended, proposed for debarment, declared ineligible, or voluntarily excluded from participation by any Federal or State department or agency.
14. During the course of this Agreement, the Customer reserves the right to request a background check on any of the Service Provider’s Authorized Persons that are in any way involved in the performance of this Agreement
15. Cybersecurity Awareness Training. All employees, non-employee workers, consultants, temporary workers and other persons, such as third-party vendors and subcontractors who may have access to Customer data, systems, networks, or facilities shall be made aware of, and be required to adhere to, the security policies of the Service Provider and have training in security practices including the handling of sensitive or confidential Customer information.
16. Remote Access. Employee remote access solutions must technically prevent the export of data of, Service Provider’s customers, or such customers’ customers to the person’s local computer situated outside the Service Provider’s facilities and must make use of multifactor authentication.
17. Storage of Data on Mobile Devices.
	1. No Service Provider or Customer data storage devices that may contain Customer data are permitted to leave Service Provider’s facility without written permission from Customer.
	2. Use of personal electronic devices to fulfill the obligations of this agreement is prohibited without written consent of the Customer.
	3. No storage devices not belonging to the Service Provider shall be allowed access to such data. “Storage device” includes, but is not limited to, laptop computers, flash drives, MP3 players, camera phones, or other electronic devices with storage capability.
	4. If any storage device, laptop or other mobile hardware contains data, such data shall be encrypted with a minimum 256-bit encryption key length.
	5. Suspected loss or theft of any device which may contain Customer data, must be reported immediately by Authorized Persons to the Service Provider, and reported immediately by Service Provider to Customer.
18. Outsourcing/Subcontracting/Service Provider’s Third Parties. If Service Provider outsources or subcontracts the provision of services or products to or for Customer to third parties, or otherwise relies on third parties to fulfill Service Provider’s information technology or Security functions, then, in addition to the requirements set forth in the Agreement, the Service Provider shall require the following:
	1. Formal written agreements that require the security controls employed by the third parties to be consistent with the Agreement, Service Provider’s security practices and the Agreement. In addition, Service Provider must enter into written confidentiality agreements with such third parties that, at a minimum require such third parties to protect such Confidential Information on terms no less protective than those contained in the Agreement.
19. Vendor shall review or have an independent audit group within Service Provider assess, the third party’s security posture.
20. All such outsourcing, subcontracts or other reliance after the date of the Agreement to which this Attachment relates must be reviewed and approved by Customer in writing in advance. Service Provider will not be permitted to perform services outside the United States or to permit its subcontractors to perform services for Service Provider outside the United States without written permission from the Customer.
21. Backup and Business Continuity. Service Provider shall have a data backup and offsite storage process, including backup/storage schedules and control requirements that address:
	1. Service Provider shall have business continuity plans in place which define contingency plans and provide for the testing of such contingency plans.
	2. Data backups stored both on and off the Service Provider’s site shall be maintained in a secure climate- controlled environment with sufficient controls to ensure the backup media are actually being received by the storage facility and that transportation boxes containing such media have not been tampered with, diverted or lost during transport.
	3. Customer Information shall be irreversibly removed, to the extent possible per current technology and subject to any applicable law, from all storage mechanisms and electronic media when such data is no longer needed for the provision of services or products to or for Customer, as reasonably determined by both Customer and Service Provider.
22. Solution Delivery. Service Provider is required to ensure that any solution used, provided or developed by the Service Provider does not hinder the Service Provider or the Customer from conforming to the compliance requirements as declared by the Customer.
23. Software Development. Service Provider shall store and process production data in a production environment only. Service Provider shall ensure that non-production environments used for development, testing, or any non- production activity, other than error correction procedures, which may be temporarily performed in a test region, shall only use test data, and in such cases the test data shall not contain any production data or Restricted Use Information.