ATTACHMENT X - INFORMATION SECURITY REQUIREMENTS

This attachment provides the additional information security requirements in addition to the existing Contract, Statement of Work, and the other associated attachments.

1.0 SAFEGUARDING CONFIDENTIAL AND RESTRICTED INFORMATION

Contractor shall implement and maintain administrative, technical, and physical safeguards designed to protect against unauthorized access to or use of Confidential or Restricted Information received from, or on behalf of, State by Contractor pursuant to performance of the agreed upon Services. For purposes of this attachment, Confidential Information includes Restricted Information. Restricted Information is data which requires strict adherence to legal obligations such as federal, state, or local law or required by State policy and so designated. Examples of Restricted Information include, but are not limited to: Protected Health Information (PHI), Federal Tax Information (FTI), Payment Card Information (PCI), Criminal Justice Information (CJI) and Personally Identifiable Information (PII) or data specifically designated by State as Restricted Information. Contractor currently maintains the following:

- An information security program that defines implements, and reviews information security policies and procedures.
- Policies that prohibit the unauthorized disclosure of Confidential and Restricted Information and requesting, on an annual basis, confirmation from Contractor personnel that they have read such policies.
- Processes to encrypt Confidential Information stored on Contractor-provided laptop and desktop computers (using BitLocker Drive Encryption – full disk encryption); processes and security settings to protect Confidential Information stored on Contractor-provided mobile devices (e.g., iPhone and BlackBerries®), such as time out values, PINs, automatic device wipe after a specified number of invalid log-on attempts, and remote wipe capability; and issuing encrypted USB drives to Contractor personnel for use in transferring Confidential Information.
- Training and awareness programs for personnel related to information security policies, information protection standards, and privacy. Additionally, from time to time, publishing privacy and security-related alerts or reminders by standard Contractor internal communication channels.
- Limiting physical access to Contractor offices through the use of one or more of: conventional locks, electronic locks, security guards, identification badges, visitor control programs, and video surveillance programs.
- Anti-virus protection programs (e.g., McAfee), including, centrally managed, commercially available anti-virus software on Contractor-provided computers to which updates are released as they become available from anti-virus software vendors, and a virus containment process that defines responsibilities and outlines procedures.
- Network servers in Contractor's data centers that employ a variety of industry-accepted procedures and tools that are designed to safeguard portions of the network and servers within the data centers. These include combinations of the following:
    - Restricting both physical and network access to authorized users
    - Restricting physical access by card-key control systems
    - Network based intrusion prevention system
    - Firewalls to segment networks
    - Vulnerability assessment processes and tools
    - Change management procedures
    - Patch management processes and tools
    - Periodically backing-up data that is maintained on Contractor network servers, including processes to encrypt back-up media and to store back-up media off-site
    - Server operating system hardening as appropriate
- Periodic review and update of internal Contractor information security policies and procedures.

- Incident Response processes containing escalation procedures for contacting State and Information Security resources.
- Sanitization of any decommissioned or inoperable Contractor-owned machine, storage, media, disk, or drive containing any Confidential or Restricted Information use the following approved sanitization methods:
  Sanitization is divided into three types.

  Type 1, Clearing:
  Clearing an electronic storage media is the lowest level of sanitization that inhibits the recovery of information assets via a robust keyboard attack using data recovery tools. Use of conventional operating system utilities like deleting files or disk formatting only delete the respective directory entries and thus do not inhibit the ability of data recovery tools to retrieve the information assets as the respective data itself is not being overwritten.

  Type 2, Purging:
  Methods of purging are:
  1. Wiping: Overwriting all locations including remapped bad sectors on a re-writable electronic storage media multiple times with different patterns, thereby checking the appropriateness by comparing different locations before and after overwriting. Required technology detail: The necessary number of overwrites, patterns and location checks, which depend on the type of re-writable electronic storage media.
  2. Secure Erasing: Overwriting all locations on an ATA hard disk drive (specific type of electronic storage media that includes PATA and SATA drives) a single time in a reliable manner. The Security Erase Unit command of the ATA specification must be used to initiate secure erasing. If implemented in a specific ATA hard disk drive, the Enhanced Erase Mode should be used. Successful execution must be checked afterwards.
  3. Degaussing: Deleting all information assets stored on a magnetically sensitive electronic storage media using a strong magnetic field.
  4. Resetting: Returning a volatile electronic storage media into its initial delivery state. The power must be switched off and the backup battery removed if battery backed.

  Type 3, Destruction:
  Physically destroying an electronic storage media is the highest level and thus ultimate form of sanitization. Physical destruction is achieved, when no portion of an electronic storage media can be used to extract a significant amount of data. Therefore, simply punching holes – for example into a hard disk – is not sufficient for physical destruction.
  Methods of destroying are:
  1. Shredding: Breaking an electronic storage media into parts. Disintegrating can be used as a synonym term for shredding. Required technology detail: The maximum size of the parts, which depends on the type of the electronic storage media.
  2. Pulverizing: Crushing an electronic storage media into dust or powder.
  3. Melting: Heating an electronic storage media past its melting point transforming it into a molten mass. The necessary melting point depends on the instance of the electronic storage media.
  4. Incinerating: Burning an electronic storage media past its firing temperature transforming it into ash, flue gases and particulates. The necessary firing temperature depends on the instance of the electronic storage media.

The selected sanitization method and procedures selected by the Contractor generates the appropriate unit level logging. A certificate of destruction shall be provided if requested by the State.

2.0 ACCESSING STATE NETWORKS, SYSTEMS, AND INFORMATION

Access to State resources requires the following: Contractor personnel connecting to State computing systems and resources shall only be in the performance of the agreed upon Services.

- Contractor personnel **shall not** knowingly (unless otherwise expressly agreed to by the parties as a function of the Services, or authorized in writing by the State's Information Security Team):
    - Access or attempt to access the State's Confidential or Restricted Information for any purpose outside of the scope of such Services.
    - Connect personal (i.e., non-work related or Contractor-provided) devices to the State's network.
    - Attempt to alter or circumvent any State security controls safeguarding the State's network (e.g., authentication processes, access controls, firewall controls, web site blocking controls, etc.).
    - Install, execute, or modify software, equipment, or peripherals on (or remove software, equipment, or peripherals from) the State network.
    - Install or disseminate malicious code (including computer viruses, worms, and Trojan horses) on the State network.
    - Conduct discovery or vulnerability scans of State networks, applications, or computing systems.
    - Share or disclose any access code or password provided by, or generated on behalf of, the State to Contractor personnel for such access.
- Contractor-provided computer workstations or laptops used to access the State's computing systems and resources will:
    - have commercial anti-virus software installed and configured to automatically signature updates released from the anti-virus software vendor while such computers are connected to Contractor's network or alternatively, in the event that Contractor personnel do not connect their computers to Contractor's network over a certain period of time, while such computers are connected to the Internet.
    - have security software patches installed on such computers, which patches, by the determination of Contractor's Information Security Office, are reasonably necessary to safeguard such computers from access by unauthorized third parties or from outside threats to the integrity and confidentiality of information residing on such computers.
    - have firewall software installed and operating on such computers while such computers are connected to the Internet.
    - have access controls designed to restrict access to such computers to authorized individuals.
    - have 128-bit (or better) AES file-level encryption enabled, which is configured to automatically verify encryption status.
    - have automatic daily back-up of standard directories and files.
- All Contractor personnel shall review the terms and requirements of this attachment prior to accessing State resources.
- The State will provide Virtual Private Network (VPN) access to Contractor personnel in order for them to perform development, testing, and production support activities in a timely manner.
- Remote access will be provided on a 24x7 basis for the Contractor's project team during the duration of this project. Contractor is responsible for planning around the State's reoccurring (planned and emergency) network and system maintenance, upon the State's communication of the same to Contractor, in order to confirm agreed upon Service timelines and deliverables are not impacted.
- Contractor personnel requiring access to production environments to investigate, and analyze production issues, must submit an access request to the State Security team. The State Security team will review, approve/disapprove and grant/deny access to production environment.
- Contractor shall submit an access request for all resources requiring access to State resources. Access requests shall minimally contain:
    - Full Name of Contract Resource

- Assigned Job Title
- Physical Location (City, State, Country of resource's current Contractor office)
- Specific System and Application Access Required (System, Application, or Database)
- Tentative End of Contract Date (to be extended as needed via additional notification)
- Remote Access Required (yes or no)

- Contractor shall submit a termination notice to the State, including full name of Contractor personnel who leave its employment and last day worked, in a timely manner not to exceed 24 hours from termination of that Contractor personnel's last day worked.
- All Contractor personnel must safeguard Confidential and Restricted information in accordance with the requirements described in this attachment.
- The State's Information Security Team will review all Contractor access request and provide approval prior to Contractor personnel being granted access. In the event the Contractor's access request is denied, the State's Information Security Team will provide written justification for review by the Contractor.
- Contractor personnel accessing State resources outside of the United States are strictly prohibited from accessing Restricted Information (directly or indirectly) contained within any application, system, database, or device unless prior written approval is provided by the State's Information Security Team and Agency assigned Data Owner.
- Contractor personnel accessing State resources outside of the United States may be utilized to facilitate agreed upon services by accessing:
  - State Test or Development Environments (Not containing, processing, or transmitting Restricted information)
  - State Test, Development, or Monitoring tool (Not containing, processing, or transmitting Restricted information)
  - State workstations (Not containing, processing, or transmitting Restricted information)

3.0 DATA MANAGEMENT

- The State will provide Contractor personnel with access to PHI, or PII data except as set out in the applicable SOW or otherwise requested in writing by the Contractor-assigned Project Manager and as allowable by law. (This may include, for example, requesting access to the State production environment for investigating potential defects identified during the Warranty Period.) For development and testing purposes, State will not provide the Contractor personnel de-identified data that is representative of production data but that does not contain PHI, PII data.
- State agrees:
  i. to disclose any PHI or PII or other applicable Restricted Information to Contractor, if such disclosure would not violate any applicable law, rule, or regulation.
  ii. not to request Contractor to use or disclose PHI or PII or other applicable Restricted Information in any manner that would not be permissible under any applicable law, rule, or regulation, if such use or disclosure were done by State.
  iii. to disclose to Contractor only the minimum amount of PHI or PII data (if any) reasonably necessary for Contractor to perform agreed upon Services under the applicable SOW.
- Agreed upon Services may require system testing to be performed in non-production environments that are utilized by the Contractor. Testing is controlled through the usage of de-identified or "mock data". "Mock Data" is data created by the Contractor and does not contain PII, PHI, or similarly regulated Restricted Information.
- If requested by the State, Contractor may be authorized to perform de-identification of production Restricted Information utilizing a State approved documented process and a State-owned workstation. This type of de-identification request must be processed through OTS.
- Contractor shall implement security measures such that non-production environments under Contractor's full control, do not contain Restricted Information unless provided with written authorization from the State's Information Security Team as an exception. If the State has access

to enter data, the State is responsible for such data entry to not contain Restricted Information, such as in the UAT or Training environments.

- The State will limit Restricted Information it provides to Contractor (or otherwise makes available to Contractor) to only that which is reasonably necessary to allow Contractor to provide the agreed upon Services.
- Contractor will provide the State with a list of Contractor personnel who are authorized to receive or have access to State resources (systems, applications, and databases). Contractor will maintain and update the access lists as needed.
- Disclosure of Confidential or Restricted Information by State to Contractor shall utilize appropriate security measures by State, including data encryption, to maintain protection of Confidential or Restricted Information being transferred to Contractor by State, and as required by applicable information protection laws.
- State will promptly notify Contractor's Lead Engagement Partner in the event it becomes aware that Restricted Information has been disclosed to Contractor inadvertently or otherwise.
- The State will be responsible that the State legacy systems required to integrate or share data with applications or systems within the scope of the agreed upon Services, shall not expose non-production environments to Restricted Information.

4.0 SECURE DEVELOPMENT

When agreed upon Services require Contractor to develop or configure systems or applications, the Contractor is responsible (unless otherwise authorized in writing by the State's Information Security Team) for:

- Working with the State's Information Security Team to require additional application or system specific Information Security requirements are captured and agreed upon prior to initiating development or technology implementation through the set requirement and design sessions. State's Information Security Team shall actively participate in applicable requirement and design sessions and review such deliverables.
- Performing an Application Risk Assessment that will be presented to the State's Information Security Team prior to production implementation.
- Operationally embedding methods for testing and validating application and system security within the development process. Contractor shall provide methods for all developers and testers to independently run both static and dynamic security testing as part of each development or test cycle.
- Requiring and validating that all input or files provided by the target end user is validated and filtered via server-side processes prior to processing in order to prevent code injection and improve data integrity.
- Requiring and validating all system to system or application to application communication requires authentication and agreed upon secure protocols.
- Requiring and validating passwords are not stored in clear text in any configuration file, source code (compiled or otherwise), or database.
- Requiring and validating web application user session state is dynamic and appropriately managed utilizing currently accepted industry standards, in order to successfully prevent an unauthorized individual obtaining the ability to bypass authentication controls by "hijacking" a valid session.
- Requiring applications integrate with the State's Microsoft Active Directory (AD) and Identity Management (IAM) solutions in such a way that internal State users seamlessly authenticate and are not presented with a logon form, if single-sign on is applicable to the scope of the agreed upon Services and/or set out in the applicable SOW.
- Requiring application or system roles and permissions are managed by the State's AD and IAM solutions.

- Requiring and validating all applicable applications employ Transport Layer Security (TLS) when transmitting Restricted Information.

5.0 SECURE SYSTEM ADMINISTRATION AND MAINTENANCE

When agreed upon Services require Contractor to maintain or administer systems or applications, the Contractor is responsible (unless otherwise expressly agreed to by the parties as to being out-of-scope of the agreed upon Services, set out in the applicable SOW or authorized in writing by the State's Information Security Team) for:

- Following State's change management policies.
- Maintaining and renewing any applicable application security certificates prior to expiration.
- Testing and applying all applicable security patches or updates in a timely manner per the Work Plan.
- The State will test and apply applicable state managed system or application security patches or updates in a timely manner.
- Requiring Systems utilize industry-accepted anti-virus as approved by the State's Information Security Team.
- Requiring Systems are restricted from connecting to the internet directly, unless approved by the State's Information Security Team.
- Requiring and validating Systems and applications are configured or modified to produce the adequate baseline level of audit records and security event logs.
- Requiring that local accounts and local authentication are not utilized unless provided approval by the State's Information Security Team.
- Requiring system access roles are provided by the State's AD and IAM.

6.0 GENERAL REQUIREMENTS

- In the actual or reasonably suspected event the Contractor personnel has materially violated the terms or requirements of this attachment, the State shall be entitled to take action to disable or prevent access to such Contractor personnel until the violation can be investigated and resolved. The State shall notify the Contractor PM within 8 hours and provide a written status of the violation and estimated time of unavailable access. The Contactor agrees that access restrictions resulting from a Contractor personnel's actual or reasonably suspected material violation of the terms or requirements of this attachment causing delay or cost for Contractor will not increase the cost of Services for the State. In the event that the suspected event was not an actual violation, any such delay may require a change request to enable Contractor to meet the work plan, and any SLAs not met due to the unavailability of access will be waived.
- System or Application vulnerabilities discovered by the State (or individuals designated by the State) shall be addressed by the Contractor in a timely manner, not to exceed 60 days, at no additional cost to the State.
- Contractor shall work with the State's designated resources to produce any documentation required to facilitate an Audit (internal or external) of State when needed, in an urgent manner. If estimated effort is above 20 hours for the individual audit request, the State will process a change request to continue contractor support.
  In response to evolving technologies, industry standards, and marketplace expectations, from time to time Contractor may upgrade or modify the processes and controls that it is required to maintain hereunder. Contractor shall not be in breach of this Agreement or any SOW as a result of any such change, provided that such change does not materially diminish the overall level of information security afforded to Confidential or Restricted Information by the processes and controls described hereunder. Any change to technology or processes previously reviewed and approved by the State's Information Security Team require appropriate notification and prior

written approval from the State's Information Security Team in addition to the Contractor's documented validation and testing of the newly proposed technology or process.