State of Louisiana

Information Security Policy

Division of Administration

Office of Technology Services

Date Published: 12/16/2015

Approval

The Information Security Policy was reviewed, approved, and published on Wednesday, December 16, 2015.

Dustin Glover,

Chief Information Security Officer

Neal Underwood,

Deputy CIO / Chief Operating Officer of OTS

Richard "Dickie" Howze,

Chief Information Officer

Stafford Olivia Palmieri,

Commissioner of Administration

Updates

A description and log of any and all future updates shall be contained within this policy section.

Contact Information

Call

Information Security Hotline

Toll-free @ (844) 692-8019, or

Local @ (225) 342-9288

Email

Information Security Team @ InfoSecTeam@la.gov

Chief Information Security Officer @ CISO@la.gov

Policy Contents

Appendix

A. Request for Exception Form

B. End User Agreement

C. Password Requirements

D. Access Request Requirements

E. Change Management Process

F. Request for Change Form

G. Approved Network Services, Protocols, and Ports

H. System Configuration Process

I. System Configuration Records

J. Vulnerability Management Process

K. Approved End User Facing Technologies

L. Encryption Requirements

M. Incident Response Plan

N. Risk Assessment Standards and Requirements

O. Third Party Information Security Questionnaire

P. Risk Acceptance Form

Q. Audit Logging Standards and Requirements

R. Data Sanitization Standards and Requirements

S. Safeguarding Federal Tax Information

T. Chain of Custody

Introduction and Overview

Purpose

The State of Louisiana is committed to defining and managing the information security requirements for maintaining data privacy and protection. This policy sets forth the information security policies for accessing, protecting, managing, storing, transmitting, sanitizing, and distributing data to ensure its availability, integrity, authenticity, non-repudiation and confidentiality.

This policy is designed to clearly inform State Agencies, Employees, third parties and applicable operational entities of their roles, responsibilities, and requirements, as this is critical to the overall success of the State of Louisiana's Information Security Program.

Scope

All entities under the authority of the Office of Technology Services (OTS), pursuant to the provisions of Act 712 of the 2014 Regular Legislative Session, shall comply with this policy.

Definitions

(For the purposes of this document)

Agreement - A legally binding arrangement that is accepted by all parties to a transaction (e.g., Mutual Non-Disclosure Agreement (NDA), Business Associate Agreement (BAA), Data Sharing Agreement (DSA), Memorandum of Understanding (MOU), formal contract, etc.).

Awareness - Efforts designed to remind, improve behavior, or reinforce proper information security practices and processes.

Baseline - An approved system, application, or service configuration standard by which future changes can be measured or compared.

Change - A functional or technical modification or patch, including changes in configuration, installation, maintenance or management, which could affect the security, accessibility, functionality or integrity of the State's computing systems, applications, or service.

Computing Systems - Includes all electronic systems, in addition to all computers, servers, network devices, and other computing devices.

Control - The means of managing risk, including policies, procedures, guidelines, organizational structures, which can be of administrative, technical, management, or legal nature.

Data - Includes all information in electronic or in paper format that can be created, stored, used, received or transmitted. Data may include data assets, data elements, data records, and information assets.

Data Breach - The successful compromise of security, confidentiality, or integrity of electronic or physical data that results in, or there is a reasonable basis to conclude has resulted in, the unauthorized acquisition of and access to Confidential or Restricted Data maintained, managed, or held in trust by the State, its Agency, or Office.

Data Center - Any State owned, managed, or leased facility, or area within, hosting one or more servers that store, transmit, or process data.

Data Encryption - Refers to ciphers or algorithms utilized to modify data in such a way that it is unreadable to anyone without the specific key in order to protect its confidentiality. Data encryption can be required during data transmission or data storage depending on the level of protection required data classification. Technical details and requirements for data encryption are located within the Encryption policy section.

Data Storage - Refers to data at rest.

Data Transmission - Refers to the methods and technologies used to transmit (i.e. move) data or copy (i.e. replicate) data between systems, applications, networks, and workstations.

Device - Any device or system owned, managed, or utilized by the State, Agency, or the Office of Technology Services (OTS) to transmit, store, or process data. Examples include, but are not limited to, laptops, desktops, servers, routers, firewalls, smart phones, PDAs, tablets, USB drives, tablets, monitoring systems, printers, fax machines, copiers or network storage devices.

DMZ - The outward (i.e. external or internet) facing level of the network architecture used to provide services to external users or systems without allowing direct access to data stores, protected services, or systems within the State's internal network.

Electronic Media - Includes electronic and storage media including tapes, disks, CDs, cassettes, DVDs, USB drives, removable storage devices, and portable computing equipment.

Emergency - When there exists an unforeseen service outage or imminent threat related to the public health, welfare, safety, or public property under emergency conditions as defined in accordance with regulations.

Employee - Any full-time, part-time, or temporary employee of the State, including interns and student workers employed by the State or its Agency.

Eradication - Is the necessary action taken to eliminate technical components related to an incident.

Incident - An attempted, suspected, or successful unauthorized access, use, disclosure, modification or destruction of data; interference with information technology operations; or a violation of End User Agreement.

Incident Response Team (IRT) - Lead by the Chief Information Security Officer (CISO), or designee, and further defined within the State's Incident Response Plan.

Independent Contractor - Any person or entity that is not an Employee of the State and who provides services to an Agency pursuant to an independent contractor or consulting agreement.

Individual - Any State Employee, third party, independent contractor, consultant, partner, or supplier.

Internal Systems - Network devices, workstations, systems, servers, or applications, directly connected to the State's internal network.

Least Privilege - The principle of least privilege (also known as the principle of least authority) is an important concept in information security, requiring minimal user profile privileges on systems and applications based on users' job necessities.

Malware - Short for "malicious software", which is any software used to disrupt computer operation, gather sensitive information, or gain unauthorized access to computing systems.

Network - A group of interconnected computers and network devices.

Network Devices - Include firewalls, routers, switches (managed or unmanaged), wireless routers, wireless access points (managed or unmanaged), wireless controllers, modems, physical taps, and intrusion prevention systems (IPS) or intrusion detection systems (IDS).

Privileged User - An individual authorized to access the State's enterprise technical resources and has the capability to alter the properties, behavior, or control of any information system(s), application(s), or network (e.g., a super user, root, or administrator). Additionally, an individual is a Privileged User if granted such elevated access to perform critical business or technical function(s).

Remediation - Implementation of an information security control or set controls to any system(s) or application(s) when correctly applied completely mitigates a specific vulnerability or reduces the impact of a vulnerability to an acceptable level of risk defined by the organization.

Risk - The likelihood of a threat successfully leveraging an identified vulnerability and the level of negative impact on any asset, system, data, or operational process.

Security Event - An observable event, or collection of events, that may indicate a potential incident and shall be reviewed or investigated and may or may not be required for promotion to an Incident.

Separation of Duties - The concept of having more than one person required to complete a task which has a significant inherent risk.

Server - A computer system that provides services to other client programs and their users, in the same or a different network. A physical or virtual system that provides a service is also a server.

Service-Level Agreement (SLA) - An agreement related to the provision of goods or services that sets forth the terms, expected duties (typically including processing or response time), and responsibilities of the parties.

System - A system may be either electronic or manual and refer to servers, network devices, data sources, network components, telecommunication components, data communication services, business processes and other applications. Systems include all computing systems.

System Administrator - An individual responsible for the installation and maintenance of a System. The System Administrator is responsible for ensuring effective system utilization, adequate security parameters are incorporated in the System, and that the System complies with the Information Security Policy and procedures.

Third Party - Any individual or entity that is not either the State Agency or an Employee of the State and is providing a good or service to an Agency.

Threat - Any source of danger that can cause negative impact to an asset, data, and/or business operations (e.g., act of nature, system vulnerability, manmade disasters, hacker, Employee, etc.).

Training - Efforts focused to review relevant security knowledge and improve or establish skill and competence. The most significant difference between training and awareness is that training seeks to teach skills that allow a person to perform a specific function, while awareness seeks to focus an individual's attention on an issue or set of issues.

User - Any Employee, independent contractor, or third party with authorized access to or that interacts with State data or data stored, processed, or transmitted by the State. The user is responsible for using the data in a manner that is consistent with the purpose intended and in compliance with the Information Security Policy while also reporting any intentional or non-intentional violations of the Information Security Policy.

Visitor - An individual or entity that is visiting a State facility and is not the Agency, an Employee of the Agency, or a third party providing a good or service to an Agency.

Virus - Any piece of code, or computer program that may be capable propagating itself and typically has a detrimental effect, such as corrupting the system or destroying data.

Vulnerability - Any weakness or flaw in a system that results in the loss of confidentiality, integrity, accountability, or availability or any combination thereof if successfully exploited.

Education, Awareness, and Training

Requirements for continuous information security education, awareness, and training are located in the Training and Awareness policy section.

Policy Enforcement

Privacy and Security Audits

The State may, from time to time, conduct audits of Agency privacy and security practices to confirm conformance with the Information Security Policy.

Complaints of Privacy Violations

Any person may report suspected violations of the Information Security Policy. Complaints may be lodged directly with the Chief Information Security Officer (CISO) or the Information Security Team (IST), and may be in writing, by telephone, or by email. Anonymous privacy complaints may be left on the Information Security Hotline or with the Office of Technology Services (OTS), End User Computing, Support Services Team.

Reporting Obligations

It is the duty of all State Employees to immediately report, using one of the methods described above, any known or suspected violations of the Information Security Policy by an Agency, its Employees, third parties, and independent contractors. The intentional failure to report violations shall subject the non-reporting party to sanctions as outlined below.

Investigation of Complaints

All complaints regarding privacy and security policies and practices, and compliance therewith will be accepted and considered. Upon receipt of a privacy complaint, the Chief Information Security Officer (CISO), or a designee, shall investigate the allegations. In so doing, the CISO may interview Employees, collect documents, and review logs detailing access and use of data. All Employees shall cooperate fully with the CISO to ascertain all facts and circumstances regarding such complaints. The CISO shall create a report of findings in response to any privacy or security complaints, and shall include the proper assurance functions such as Human Resources (Human Capital Management), Legal, and Compliance entities during the course of an investigation, as needed. The CISO shall ensure all complaints are reported to the Commissioner of Administration and CIO immediately as practical. In addition, the CISO shall produce periodic reports for the Information Security Governance Board (ISGB) and The Office of Technology Services (OTS) Executive Leadership Team concerning the status of privacy and security complaint(s) involving an Agency, its Employees, third parties, or independent contractors.

Non-Retaliation

Neither an Agency nor any Employee(s) shall undertake any action to intimidate, threaten, coerce, discriminate against, or any other retaliatory action (“reprisal”) against persons who report a violation of the Information Security Policy. Persons who engage in acts of reprisal shall be subject to sanctions as outlined below.

Sanctions

Violations of the Information Security Policy may result in disciplinary action, up to and including dismissal. Accordingly, the State shall notify the appointing authority responsible for the individual that has violated this policy. In addition, if the State has a reasonable belief that the individual has violated the law, the State shall refer violators to the relevant entity for prosecution, as well as commence legal action to recover damages from the individual.

Violators may also be required to complete remedial training.

Policy Exceptions

Except as otherwise stated in this policy, any Agency or individual may request an exception to this policy by having their section director (or higher) submit a Request for Exception Form to the Chief Information Security Officer (CISO). The Agency or operational entity must receive documented authorization prior to taking any action that directly or indirectly conflicts with the requirements and responsibilities within this policy.

Where an exception to the policy presents a risk that cannot be remediated or mitigated using alternative security measures, a Risk Acceptance Form shall be completed and signed by the Statewide Chief Information Officer (CIO), Chief Information Security Officer (CISO), and the Agency's Executive Director for the purpose of setting forth a risk management strategy.

In cases where the requester deems the CISO's denial is unacceptable, the request may be appealed by the Agency's Executive Director to the Information Security Governance Board (ISGB).

The CISO shall not, under any circumstance, approve any exception which violates or conflicts with any Federal or State law.

The CISO shall present the ISGB with a report of all current exceptions at least annually.

Changes and Amendments

The Information Security Policy is reviewed annually by the CISO, taking into account any changes to environments, technology in use, operational objectives and processes, identified threats, effectiveness of implemented controls, and external events, such as changes in legal or regulatory environments, changed contractual obligations, and changes in the social climate. Any policy changes or amendments shall be proposed to the ISGB for review and approval. Any amendments to this Policy may be proposed by any member of the Information Security Team (IST) for the review and approval by the ISGB at any time.

Roles and Support Functions

Statewide Chief Information Security Officer (CISO)

The CISO is responsible for the maintenance and implementation of the Information Security Policy. The CISO will work with various operational sections, assurance functions, state agencies, and internal and external parties to implement, monitor, and evaluate the Information Security Policy.

Information Security Team (IST)

The IST is comprised of the CISO and specifically selected OTS resources at various operational levels with the primary responsibility of performing operational information security functions. Lead by the CISO, the IST works with applicable OTS, Agency, and Third-Party resources to develop, implement, communicate, and apply the Information Security Policy to State systems, data, and processes.

Information Security Officers (ISO)

The CISO will assign specific members of the IST to serve as an ISO. An ISO will assist in leading information security initiatives related to specific regulatory environments. An ISO will also function as a dedicated resource for agencies to assist with planning, audits, incident response, notifications, and ensure regulatory requirements are implemented in a verifiable manner.

Information Security Governance Board (ISGB)

The ISGB is comprised of members of the Division of Administration's Executive Staff and Agency Leadership. Additions and changes to the membership of the ISGB may be proposed and approved by the ISGB. The ISGB is responsible for confirming that the State aligns the Information Security Strategy with the State's operational strategies, while managing information security risks though appropriate risk tolerance levels and risk policies.

Assurance Functions

Legal, Compliance, and Regulatory

The State's legal, compliance, and regulatory departments or resources shall be engaged to provide the CISO and IST legal and regulatory compliance guidance and on-going direction to support continuous improvement of the Information Security Policy.

Audit Assurance Groups

The CISO and IST shall work with the Division of Administration Internal Auditors (IA), Louisiana Legislative Auditors (LLA), and third parties, where applicable, to monitor, develop, and assess the effectiveness of the Information Security Policy.

Internal Audit (IA)

The assessments, risk ratings, audit findings and recommendations issued by the IA will assist the CISO and IST in the annual review of the Information Security Policy. The CISO and IST may seek assistance from and cooperate with IA to help facilitate compliance with the Information Security Policy and applicable regulations, standards, and best practices.

Louisiana Legislative Audit (LLA)

The CISO and IST working with IA, shall cooperate with LLA, as stated by State law [RS 24:513], to implement and maintain financial reporting controls, including key information technology general computer controls and access controls.

Third Parties

When deemed necessary by the Chief Information Security Officer (CISO), the Information Security Team (IST) may contract with third parties for the following:

- Recommendations, guidance, or creation of policies, processes, and procedures.
- Formal Risk Assessments
- Application Security or Penetration Testing
- Industry certifications

Office of State Human Capital Management (OSHCM)

Due to OSHCM's direct and constant relationship with existing Employees, as well as its interaction with new and former State Employees, the IST shall work closely with OSHCM resources to confirm compliance with critical processes and procedures required by the Information Security Policy.

- The IST shall work with OSHCM to develop policies and procedures to address any information security issues prior to employment, during on-boarding, during employment, dismissal, or position changes.
- The IST shall also work with OSHCM to align Information Security awareness, education, and training with the Information Security Policy.

Office of Risk Management (ORM)

The IST will coordinate with ORM to administer a cost effective comprehensive risk management program for all information technology services in order to mitigate financial liability associated with the delivery of these services.

Office of State Procurement (OSP)

OSP is comprised of three internal sections: Central Purchasing; Professional Contracts; and State Travel/Purchase Cards. Each section is responsible for providing timely and efficient procurement of goods and services.

- The IST shall work with OSP to standardize, facilitate, and supervise the procurement of all information technology goods, services, and Professional Services (professional, personal, consulting) required by the State or its Agencies.
- The IST shall review and approve RFPs and contracts for information technology related goods and services to ensure language provided meets or exceeds the standards required in the Information Security Policy.
- The IST will ensure that staff, contracted staff augmentation personnel or their subcontractors, receive and meet Training and Awareness requirements for the protection of Agency data.
- The IST will provide assistance and review of contracts related to information technology or information exchange to ensure compliance with Data Sanitization requirements.

Change Management Board (CMB)

The CMB is responsible for overseeing the change management process and confirming that the proper review, documentation, testing, approval, implementation and archival of changes performed. The CMB is comprised of Office of Technology Services Leadership selected by the Chief Information Officer (CIO) and meets periodically. The Chief Information Security Officer (CISO) shall be a voting member of the CMB.

Note: Additional information including, responsibilities for Information Security Management and Support Roles can be found in the State's Information Security Program Charter.

Data Classification and Handling

Purpose and Scope

This policy section provides a clear definition and responsibilities for classifying data accordingly to the requirements and risks associated with the use, storage, transmission, or processing of data by an Agency or entity.

This policy section applies to all data owned, maintained, processed, held in trust, or licensed to the State or its Agency.

Data Handling

Agencies shall appropriately appoint roles, responsibilities, operational processes, and classify data in accordance with the classification system defined within this policy.

In addition to the responsibilities defined within this policy, all agencies shall comply with any applicable Federal and State regulations related to data protection.

Data Roles and Responsibilities

Data Owner

The Data Owner is the individual, team, group, or section within an Agency or entity directly responsible for the data. The Data Owner shall be knowledgeable about how the data is used, acquired, transmitted, stored, deleted, and otherwise processed. Unless otherwise specified by the Agency or appointed by higher authority, the Data Owner is the leader of the operational area, group, or team that is responsible for the process or service requiring the data. The Data Owner is also referred to as the record "custodian" within the State's Public Records Law.

The Data Owner, or authorized delegate, shall determine the appropriate Classification Level of the data and shall review the Classification Level periodically to verify it is still applicable and appropriate.

The Data Owner shall be personally liable for the misuse, unauthorized use, or intentional disclosure of Restricted Data which shall result in actions by the State as defined in Policy Enforcement.

Data Custodian

The Data Custodian is individual or group assigned by the Data Owner, responsible for implementing and maintaining the requirements for the data classified by the Data Owner.

Data Handler

A Data Handler is anyone who has been authorized by the Data Owner to utilize the data in accordance with assigned duties or responsibilities. A Data Handler is responsible for understanding the data classification and requirements set forth by the Data Owner.

Data Labeling

Data must be labeled with the appropriate Classification Level where possible.

For example, where possible, electronic documents should be labeled in the header or footer with the appropriate Classification Level; printed material should contain the Classification Level on the cover sheet, and system, database, or application entry points should display the Classification Level within the logon banner where deemed feasible by the Information Security Team (IST).

Data Classification Levels

Public (or Unrestricted)

Public Data is data that does not qualify as Confidential or Restricted Data and is in the public domain or has been released for public use in accordance with applicable Federal, State, or Agency policy. Public Data is accessible to all users (i.e., general public) and distributed without the need for restriction. Release of this data has no measurable adverse impact on individuals, Agency, or the State of Louisiana.

- *Examples of Public Data*:

  Include, but not limited to, approved press statements, louisiana.gov content, forms and templates used by workers or residents, marketing materials, etc.

Uncategorized (or Internal)

Uncategorized Data is data that is not actively published to the public; however, is subject to the State's Public Records Law. Inadvertent disclosure would unlikely have an adverse effect on any individual, supplier, partner, Agency, or the State of Louisiana. Any data **not** classified as Restricted, Confidential, or Public shall be classified as Uncategorized Data.

- *Examples of Uncategorized Data:*

  May include, but not limited to, Internal Memos not containing Confidential or Restricted Data, Meeting Minutes **not** containing Confidential or Restricted Data, Internal Project Reports, Departmental Operating Procedures, Business Contact information, etc.

Confidential (or Sensitive)

Confidential Data is data that the unauthorized disclosure of could seriously and adversely impact an Agency, third party, suppliers, individuals, or the State of Louisiana. Additionally, Confidential Data has been specifically excluded or granted exemption within the State's Public Records Law.

- *Examples of Confidential Data:*

  Include, but not limited to, Source Code, Audit or Risk assessment reports, demographic research, strategic plans, employee performance reviews, etc.

Restricted

Restricted Data is data that requires strict adherence to legal obligations such as Federal, State, or local law, specific contractual agreements, or data specifically designated as Restricted Data in applicable state or Agency policy. The unauthorized disclosure of Restricted Data is expected to have a severe or catastrophic adverse effect on an Agency, partners, individuals, or the State of Louisiana. Additionally, Restricted Data has been specifically excluded or granted exemption within the State's Public Records Law.

- *Examples of Restricted Data:*

  Include, but not limited to, Usernames and Passwords, Federal Tax Information (FTI), Protected Health Information (PHI), Personally Identifiable Information (PII), education records, credit or payment card information (PCI), Criminal Justice Information (CJI), employee payroll records, state tax payer data, etc.

Requests for Public Records

In order to ensure Confidential and Restricted Data is not unintentionally released, an Agency shall create, maintain, and disseminate procedures for processing Requests for Public Records. Agency procedures shall contain named individuals authorized by the appointed authority to release information once the request has been appropriately reviewed by the Agency's Data Owner (or designee) and legal counsel.

All Employees, when presented with a Request for Public Records, shall follow the Agency's procedures for processing Requests for Public Records, regardless of the Classification Level assigned to the records being requested.

Access and Identity Management

Purpose and Scope

This policy section clearly outlines the responsibilities and actions required to ensure identities and credentials are appropriately managed for authorized users and tailored to job roles or responsibilities. This section also applies to any and all applications, systems, clients, servers, devices, portals, or third party used by an Agency.

Access permissions are managed, incorporating the principles of least privilege and separation of duties. Security validation or Screening shall be included within the Office of State Human Capital Management (OSHCM) processes, including performing background checks on a periodic or as needed basis. Screening checks may also include personal credit validation when deemed necessary by the Data Owner.

Identity Management

All systems, applications, and software utilized by an Agency or the Office of Technology Services (OTS) shall comply with the following list of requirements:

- Each user, including Employee, independent contractor, third party users, shall review and sign the End User Agreement.
- Each user shall be assigned a unique ID that is created in approved identity management repositories.
- User accounts or IDs issued to third parties or independent contractor shall be configured to automatically expire at the end of the contract or engagement date.
- User accounts or IDs **shall not** be created locally within applications, devices, and systems unless approved by the Information Security Team (IST).
- User accounts or IDs used for guest networks shall be strictly limited and isolated for guests only and access shall be automatically removed or disabled upon completion of engagement or 30 days, whichever occurs first.
- A user account or ID and password must be presented each time a user logs into the network.
- System Administrator accounts will not be granted direct remote access to any State network or application. System administrators shall authenticate to the network using their standard user account credential and then, if performing any system administrative job function, authenticate using their unique privileged level account credentials.
- System administrators shall use privileged accounts only for approved system administrator purposes.

Passwords

All users, systems, and applications shall comply with the following:

- Passwords **must not** be stored in clear text or reversible encryption formats.
- Passwords **must not** be transmitted in clear text or insecure protocols.
- Passwords must comply with Password Requirements.
- Passwords must be stored and transmitted in compliance with Encryption.

For any user account issued by the Agency, the Office of Technology Services (OTS), or approved third party or any additional user account created to facilitate operational processes for the State, all users shall take reasonable precautions to protect the confidentiality, integrity, and secrecy of their password, including but not limited to:

- Notify the Information Security Team (IST) in the event of an actual or suspected password compromise.
- **Never** share their passwords with any other person.
- **Never** write down passwords or use and store passwords in a readable electronic form, including batch files, automatic login scripts, software or keyboard macros, or terminal function keys.
- Where possible, not locally "cache" any passwords or select the option to "remember my password" within a client application as selecting this option will likely store the password in an insecure manner.
- **Never** store or "cache" passwords within any system or application not approved, managed, owned, or hosted by the State. (i.e. Cloud or Internet services)
- **Never** transmit passwords over email or other forms of electronic communication without use of data encryption compliant with Encryption.

Note: It is not the intention of this policy to create inefficient or frustrating processes for users of any technology; and as such, the IST will gladly review any proposed solution that may securely ease the burden of authentication for any Agency process.

Onboarding New Users

Screening

In accordance with relevant Federal and State laws and regulations, the Office of State Human Capital Management (OSHCM) shall perform background verification checks or credit checks on existing Employees or candidates for Employment.

Terms and Conditions of Access

Prior to granting access to Restricted, Confidential, or Uncategorized Data, OSHCM or IST shall verify that the End User Agreement is signed by Employees, independent contractors and third party users of information assets.

OSHCM will maintain all Employee related records as the appropriate process owner and IST shall maintain records of all independent contractor and third party user security agreements.

Access Control

Access to data and systems shall be configured based (1) on the Data Classification Level and (2) by the user's job role or responsibility. All systems should be tailored to restrict access to users who need such information to perform their job function (least privilege). All data shall be protected via access controls so that data is not improperly accessed, disclosed, modified, deleted, or rendered unavailable.

Default Minimum Access

All users shall be allowed to have read access to systems, applications, and resources that contain solely Public Data.

Access Based on Job Role

Access to systems that contain Restricted, Confidential, or Uncategorized Data shall be granted based on job role or responsibility. The parameters of the access are based on user attributes proposed by the supervisor of the Agency section and will be subject to the additional approval of the IST or Data Owner. Reviews of users' attributes with their access needs are to be performed by the application, system, or Data Owner on a periodic basis to confirm that the access is still necessary and required for that job role. The application, system, or Data Owner shall notify the Information Security Team (IST) if the role or access is no longer needed or appropriate.

Elevated Access

If access is required beyond the initially approved scope of the Job Role and is deemed necessary by the Data Owner, then the Data Owner or delegate must submit an Access Request and receive approval from the IST. Any extensions of temporary Elevated Access must be submitted to and approved by the IST. The IST shall keep all Access Request documentation of extensions on file in accordance with data retention policies. The Data Owner shall review users with Elevated Access periodically to confirm that the access is still necessary and required and shall notify the IST and the user (or the user's manager, if appropriate) if the Elevated Access is no longer needed or appropriate. Users no longer needing Elevated Access will have such access modified or removed.

Third Party Access

Third Party or independent contract users shall only be granted the access necessary to perform their contracted obligation as determined by the Data Owner and deemed appropriate by the IST.

On an annual basis, the Data Owner, assisted by the IST, shall perform a review of third party access.

Emergency Access

In the event of an emergency requiring immediate access, the same access control processes shall be followed, except that if the Data Owner is not available and the need for additional access is critical for continued operations or to address an active incident, then the Chief Information Security Officer (CISO), Chief Information Officer (CIO), or Deputy CIO may authorize such access. The emergency access shall be documented with an Access Request and the emergency access shall be removed once the situation is resolved.

Resolution of the emergency is determined by Data Owner (or higher authority), CIO, and CISO.

Remote Access

OTS and Agencies shall ensure:

- Reasonable and appropriate technologies and measures to control remote access of systems.
- Secure authentication and cryptographic technologies utilized comply with Password and Encryption requirements.
- An additional factor of authentication (multi-factor) is required for privileged users, users accessing Restricted Data remotely, or for systems designated by the Data Owner or CISO to require multi-factor authentication.
- System configurations maintain the latest antivirus updates and operating system updates pursuant to the requirements within System Configuration.
- Third party access to systems is restricted, unless specifically required to fulfill services contained within a signed agreement.

Removal or Suspension of Access

Suspension of Access

If the Information Security Team (IST) has evidence or suspicion that an user account or ID is being used in violation of a State policy or in a manner that may cause potential damage to Agency systems, then the IST may immediately suspend or disable the user or account ID. The IST shall provide notification of the suspended access to the user's direct supervisor.

Standard Removal of Access

Employee, independent contractor, and third party user accounts or IDs created or issued by an Agency or OTS, or an account used solely for Agency processes shall be disabled or decommissioned upon dismissal or termination of contract.

Supervisors or responsible parties shall notify the assigned Office of State Human Capital Management (OSHCM) contacts as soon as possible, but no later than two business days, following the decision to dismiss an Employee. For contractors, or third party users, the responsible parties shall notify the IST and assigned Office of State Procurement (OSP) contacts no later than two business days, following the decision to terminate a contract or services.

For planned dismissals, OSHCM or any other responsible party shall notify the IST of the planned date of dismissal and the affected the user(s). Access shall be removed for the Employee, contractor, or third party user as soon as possible, but no later than two business days after the date of dismissal.

Sensitive Removal of Access

Removal of access shall be considered sensitive when the user is being dismissed and:

- Has access to systems containing Confidential or Restricted Data.
- Has been granted privileged access.
- May inappropriately use Agency data after dismissal.

In the event that access requires sensitive removal, the user's supervisor, the relevant Data Owner, or designee shall notify the OSHCM and IST two days prior to the date of the planned dismissal, or earlier if operationally possible.

The IST shall work with the Data Owner, Agency Leadership, or designee, to coordinate the actions required for removing access at a time closely aligned with the dismissal of the user.

At a minimum, sensitive dismissals requires access to be removed before the close of business that same day.

Change in Role or Position

In situations where the user has changed roles or positions and requires reduced or enhanced access, the user's manager should notify the IST and work with the relevant Data Owner to provide the user with appropriate access that is consistent with his or her job responsibilities.

Unnecessary or Inappropriate Access

In situations where a user has received unnecessary or inappropriate access, is abusing access, or otherwise violating policy, the IST may remove, disable, or restrict access upon becoming aware of the situation or receiving a request from the relevant Data Owner or supervisor.

Based on the potential operational impact, nature of the inappropriate access associated with the situations outlined above, or when deemed necessary by the Chief Information Security Officer (CISO), the IST shall further investigate the event. In instances where the CISO determines the actions by the Data Owner are clearly negligence or misuse, actions shall be taken in accordance with Policy Enforcement.

System Configuration

Purpose and Scope

This policy section sets forth standards for all computing systems connected to the State's network. All systems in production or intended for production use, whether managed by the Office of Technology Services (OTS), an Agency, or third party, must be built, deployed and configured in accordance with this policy section. The Information Security Team (IST) must perform pre and post evaluation and validation of the security configurations of all such systems. Computing systems that are not owned or leased by OTS or the Agency shall not be allowed to directly connect to the State's network unless approved by the IST.

Computing System Build and Deployment

All computing system deployments or modifications shall adhere to the System Configuration Process established by OTS and approved by the IST. Any request for an exception to the System Configuration Process must be approved by the IST using the processes required by Policy Exceptions.

Computing systems shall be built, configured, deployed, and maintained in compliance with the technical and non-technical requirements defined below.

System Configuration Record

A System Configuration Record must be generated for all initial system baselines and changes to system baselines at the time of installation by the system developers, maintainers or administrators and maintained accordingly.

Note: User-preference variables such as screen backgrounds, ring-tones, and other user based settings are exempt from this requirement.

Secure Baseline

The IST, working with the appropriate operational OTS sections, shall document a secure baseline of the applicable security settings, controls, configurations of the operating system (OS) while including any additional application, hardware, or service settings specifically relied upon to address an identified risk.

Patch Deployment

All current patches, hot-fixes, and service packs shall be installed, when applicable on computing systems prior to deployment into the production environment. Any future patches, hot fixes, and service packs shall be installed in accordance with Vulnerability Management and Change Management.

File Integrity Monitoring

Where possible or deemed required by CISO, File Integrity Monitoring (FIM) solutions shall be implemented on systems storing or processing Confidential or Restricted Data to alert on unauthorized modification of critical system files (e.g., system and application executable), configuration and parameter files, and security event logs.

Application Control

Where possible or deemed required by CISO, application control solutions shall be implemented to ensure the computing system remains in compliance with the approved system configuration baseline.

Computer Firewalls

When applicable, computer (or Host) firewalls shall be utilized to address the risk of computing systems connecting to untrusted networks.

Anti-virus Software

Anti-virus software shall be applied to computing systems in accordance with Antivirus.

Encryption

Encryption shall be applied to computing systems in accordance with Encryption.

Network Time Protocol (NTP)

All Office of Technology Services (OTS) and Agency systems shall be configured to use the NTP server(s), authorized by the Information Security Team (IST) to maintain time synchronization with other systems in the environment.

Network Storage Configuration for Confidential Restricted Data

Storage devices utilized by OTS or an Agency that store Confidential or Restricted Data must be on an internal network segregated from any DMZ. Access to storage devices must be configured in accordance with Access and Identity Management requirements.

Configuration of local shares

All shared resources (e.g., mapped folders, drives, and devices) must have permissions set to allow only those individual accounts or groups that require access to that resource. Sharing folder resources from a workstation is prohibited and server resources must be used for sharing purposes using the guidelines as described in Access and Identity Management.

Where applicable, all approved shared files and folders must be configured to use NTFS (New Technology File System) sharing via Active Directory Groups with exceptions to approved Service or System accounts. Granting permissions to files and folders directly is allowed for service and system accounts only.

Login Notice

Any computing system owned, operated, leased or managed by OTS or an Agency shall be configured with login banners, where feasible, reminding users of the permissible and authorized uses of the computing system. Where applicable, warning banners should be used advising users of safeguarding requirements.

Software Installation

Users may not install software on computing systems operated within the State's network. If the requested software is on the approved End User Facing Technologies List, OTS will obtain and track the licenses, test new software for conflict and compatibility, and perform the installation. If particular software is not on the End User Facing Technologies List, the appropriate Agency management must submit a request to OTS for review and approval prior to production installation.

Change Management

Purpose and Scope

This policy section sets forth the policy under which a change to systems shall be proposed, reviewed, tested, and implemented. The purpose of this section is to minimize disruptions and mitigate risks associated with changes. A change is a functional or technical modification or patch, including changes in configurations, installation, maintenance or management, which could affect the security, accessibility, functionality or integrity of the Office of Technology Services (OTS) or Agency systems.

Change Management Board (CMB)

The Change Management Board (CMB) is responsible for overseeing the change management processes and confirming that the proper review, documentation, testing, approval, implementation and archival of the changes performed.

Change Management Procedure

The approval, testing, and implementation of changes must be made in accordance with the Change Management Process, as may be revised by the CMB. Change requests must be submitted by the appropriate Agency or OTS section. The change request must identify the change impact, priority, and type and whether the change relates to systems that contain Confidential or Restricted Data. OTS shall then follow the process set forth in the Change Management Process.

Change Releases

High Priority Releases

If an Agency, Information Security Team (IST), or OTS believes a change must occur prior to the next CMB meeting and the change has been designated as “high priority”, it can be released using the High Priority Release Request as defined within the Change Management Process.

Emergency Releases

Changes may be released on an emergency basis pursuant to the Change Management Process if the Agency, IST, or OTS determines that an interruption requires immediate response due to the number of users affected, the involvement of systems that are critical to State or Agency operations, or the involvement of systems that contain Confidential or Restricted Data.

Change Implementation

Changes must have a deployment plan that contains implementation in addition to a roll back plan as required by the Change Management Process. The roll back plan must be executed if there are any discrepancies between expected results and actual results that impact systems, unless such discrepancies are documented and accepted by the Agency and the CMB.

Where deemed feasible by the Chief Information Officer (CIO), OTS and Agency Leadership, separate environments and systems shall be maintained solely dedicated to development, testing, and deployment of the changes to reduce risk. Environments shall be separated by logical, technical, or physical controls as appropriate. In addition, where appropriate, separate personnel are to be responsible for each of these environments (separation of duties) to avoid risk of unauthorized access, tampering, and changes.

Change Documentation

Changes must be documented and retained as outlined in the Change Management Process. All source code owned or created by an Agency or OTS shall be stored in a secure source code repository, and OTS shall establish and maintain operational processes for authorizing development users to check out\in code for version and audit purposes.

Network Devices and Communications

Purpose and Scope

This policy section clearly indicates the responsibilities and actions required to implement and maintain mechanisms that ensure communications and network segments that process or transfer Confidential or Restricted Data are adequately protected.

All firewalls, routers, switches, wireless routers, intrusion detection systems, and other network devices on any Agency network, whether managed by the Office of Technology Services (OTS), Agency, or by a third party, shall comply with this section.

Network Device Management Responsibilities

Network devices must be implemented, configured, maintained to effectively filter and protect against unauthorized access to OTS and Agency systems that store, process, or access Restricted and Confidential Data.

Network device management responsibilities may be delegated to third parties, in accordance with this policy section, Third Party and Data Sharing Agreements, and written approval from the Information Security Team (IST).

Device Management Responsibilities Include:

- A list shall be created and maintained of all approved protocols and services permitted on firewalls, routers, switches, and other applicable network devices. Documentation for Approved Network Services, Protocols and Ports must contain a justification for business need and description of purpose.
- Apply security access rules to firewalls, routers, and other network devices sufficient to protect OTS and Agency systems containing Restricted, Confidential, and Uncategorized Data from external Security Events and external attacks.
- Source routing must be disabled on all firewalls and external routers.
- Implement a network perimeter defense between trusted and untrusted environments.
- Access control to network devices shall adhere to Access and Identity Management requirements.
- Network devices shall not expose any management interface to any external network or the internet.
- Document firewall and router security rule changes using Approved Network Services, Protocols and Ports.
- All network devices must be capable of and configured to generate logs sufficient to address Audit Logging and Event Monitoring requirements.
- Network diagrams must be created and maintained for the entire network, clearly labeling all network devices and protection mechanisms.
- Ensure all routers, firewalls, and other network device configuration files are secured and synchronized properly.
- Network device configuration backups shall be captured at a frequency that is operationally feasible and approved by the IST.
- Manage and apply any patches or fixes for routing protocols or network devices in accordance with Change Management and Vulnerability Management.
- Network diagrams shall be updated after any change affecting the environment and reviewed on a quarterly basis to confirm they are accurate and up to date.
- Conduct bi-annual review of all network perimeter routers, firewall, IPS, and core network device configurations and record results of the review in the device's System Configuration Record. The configuration baselines for Agency network devices are to be reviewed on an annual basis and updates to the System Configuration Record should be made when necessary.
- Requests for internal systems or applications to establish direct connections to internet services must be submitted to the IST for review and approval. If approved, network devices will be configured to only permit sessions to the specific destination IP addresses and ports provided in the request.

Authorized Services, Protocols, and Ports

Approved services, protocols, and ports, with their corresponding justifications and purpose, are listed in the Approved Network Services, Protocols and Ports. Any changes to the list shall be made in accordance with Change Management.

Every connectivity path (both inbound and outbound), protocols, and services that have not been approved and listed on as Approved Network Services, Protocols and Ports shall be blocked by OTS or Agency firewalls, routers and network devices.

Network Connection Paths and Configuration Requirements

Each network path leading to Uncategorized, Confidential, or Restricted Data must utilize logical or physical network segregation using appropriate technologies (e.g., VLANs, IPSec, and VPN) and have a firewall installed at each Internet connection. A firewall shall be installed between any demilitarized zone (DMZ) network, public or untrusted network, third party networks, and where applicable for the internal network zones.

For network connections directly connected to the internet, public network, or otherwise untrusted environment, requires all traffic to be filtered by a monitored intrusion detection/prevention system that is managed by the Information Security Team (IST), or IST approved resources.

In no circumstance shall a network device be configured to allow systems within the internal network to be directly accessed from the internet or public network.

Virtual Private Networks (VPN)

VPN connections are utilized to ensure the privacy and integrity of the data passing over a public or untrusted network. VPN connections shall:

- Be used for any external connections to internal systems.
- Be used for any connection between firewalls over any public or untrusted network.
- Be implemented in adherence to the configurations within Encryption Requirements.
- Allow only authorized users and partners in accordance with Access and Identity Management requirements.
- Be considered an extension of the trusted network, and as such, shall comply with the other applicable sections of the Information Security Policy.

Modem Connections

- Where a modem line is used for call out purpose only, auto answer mode must be turned off.
- Allow only authorized users and partners in accordance with Access and Identity Management requirements.
- Where a modem is used to remotely access the network, the call-back function must be configured for authentication on dial-in.

Wireless Network Requirements

Only wireless routers or access points which are owned, managed, acquired, or configured by OTS and approved by the IST are permitted on Agency networks.

The IST is authorized to perform periodic assessments of applicable State facilities to review wireless network configuration and attempt to identify unauthorized wireless routers or access points.

All wireless routers must be physically protected against theft, unauthorized use, or damage.

All wireless networks in production use must be protected using the requirements set forth in the Encryption Requirements.

Wireless networks with access to internal systems or applications is granted to authorized users only.

Wireless networks utilized by guests or public resources must be strictly isolated and prevent any access to internal systems, applications, resources, or data.

Host or Personal Firewalls

End User computing systems must incorporate host or personal firewall functionality where deemed technically feasible by the Information Security Team (IST). Applications or services providing such firewall functionality must be reviewed, configured, and approved by the IST.

Additionally, all host or personal firewall solutions shall be implemented in such a way that prevents unauthorized changes.

Network Administrators

Individuals granted privileged user authorization to manage network devices shall maintain strict confidentiality regarding network infrastructure, including but not limited to, information regarding access, configuration, Agency communication systems, modem access, network diagrams. Any information regarding the configuration or communication of network devices or systems shall not be posted on any public bulletin boards, listed in telephone directories, placed on business cards, or made available to third parties without the written permission from the IST.

Vulnerability Management

Purpose and Scope

The ability to manage vulnerabilities reliably is a crucial component of the Information Security Program. Vulnerability Management is the process of assessing, detecting, validating, documenting, and remediating vulnerabilities present on devices, systems, and applications, in a timely manner. This policy section establishes responsibilities and actions required to effectively manage vulnerabilities.

All devices, systems, and applications owned, leased, managed, or utilized by the State or utilized by any individual conducting business on behalf of the State, shall be managed in accordance with this section.

Identification and Notification

User Identification

If a user becomes aware of a vulnerability applicable to any Office of Technology Services (OTS) or Agency computing system, the user shall inform the Information Security Team (IST) of the vulnerability as soon as operationally feasible.

Commercial Software Vendor or Third Party Identification

OTS and their partners shall subscribe or implement approaches to maintain awareness of potential vulnerabilities.

Additionally, any third party hosting, managing, or maintaining any software, system, or process on behalf of the State shall contact the IST immediately as practical upon becoming aware of a vulnerability.

Automated Identification

OTS shall deploy and schedule technical solutions that assist in on-going detection and identification of system or application vulnerabilities.

Continuous Assessment

Scanning and Testing

The IST, or approved designee, is responsible for conducting consistent internal and external vulnerability scans.

Testing and Scanning after a Significant System Change

Vulnerability testing shall be performed on all network devices, operating systems, databases, and applications which use, store, or transmit any Confidential or Restricted Data after any significant change (e.g., new system component installations, changes in network topology, firewall rule modifications, or product upgrades).

Penetration Testing or Ethical Hacking

Only qualified resources approved by the Chief Information Security Officer (CISO), with the expertise required for penetration testing or ethical hacking may perform internal and external network or application assessments. The IST may perform this function as needed.

Intrusion Detection Software

Networks or systems that transmit, store, or process Confidential or Restricted Data shall be protected by a monitored host or network intrusion detection or prevention system that alerts personnel of potential risks. Event logs generated by Intrusion Detection or Prevention systems shall be monitored and managed in accordance with Audit logging and Event Monitoring.

Risk Assessments

As part of Risk Management, the Chief Information Security Officer (CISO) shall identify and assess any existing or new threats and vulnerabilities to verify that the Information Security Policy is appropriately aligned with the Information Security Program and Strategy.

Severity Ratings

Each identified vulnerability shall be assigned one of the following ratings:

Critical

A vulnerability making it possible for an unauthorized individual to easily or remotely gain control at the administrator level of an affected system, application, device, or directly access Confidential or Restricted Data. Unless otherwise assessed by the CISO, this class of vulnerability is considered to introduce the highest level risk.

High

A vulnerability making it possible for an unauthorized individual to locally gain administrative access to a system or application or possibly gain access to Uncategorized Data.

Medium

A vulnerability that may allow an unauthorized individual to gain access to any information stored within a system or application.

Low

A vulnerability that while exists, does not pose an immediate threat to the system or application and poses no overall increase in risk to the State. Low vulnerabilities may be mitigated through firewalls and intrusion prevention systems that filter or block external access.

Unless otherwise specified by the Information Security Team (IST), vulnerabilities identified by software vendors shall maintain their industry accepted (published) severity rating. Examples include, but are not limited to, CVSS or Microsoft Severity Rating.

Remediation and Reporting

Vulnerability Log

The IST shall maintain a vulnerability log that contains all known vulnerabilities.

Remediation and Response

Vulnerabilities shall be remediated in accordance with the Vulnerability Management Process.

Installation of security updates should be tested prior to deployment to production systems and applications where the capability exists. Additionally, updates should be coordinated and applied during an established maintenance window.

Remediation actions shall be completed in compliance with Change Management.

Reporting

The IST shall produce periodic reports and distribute to appropriate management resources.

Antivirus

Purpose and Scope

This policy section clearly defines the responsibilities and actions required to protect computing systems and networked resources against malicious software. All computing systems, whether managed by Office of Technology Services (OTS), Agency, or third party, that are capable of supporting anti-virus software, shall comply with this policy section.

Signature Updates

All computing systems with anti-virus software must be configured to receive daily signature and engine updates.

Software and Process Requirements

Anti-virus software must be centrally managed and configured to alert the appropriate OTS resources. OTS resources receiving alerts generated from anti-virus software shall follow the procedures outlined in Incident Management.

Anti-virus software logs shall be retained in accordance with record retention policies.

End-User Responsibilities

Users shall:

- Take every precaution to ensure malicious software is not introduced into State environments.
- Notify OTS End User Support Services of any actual or suspected malicious software and shall not attempt to remediate themselves.
- **Not** attempt to disable or uninstall anti-virus protection on any computing system.
- **Not** download personal anti-virus software, including evaluation software, public-domain software, or other unauthorized software, on computing systems.

Computing systems shall only contain authorized software as installed, provided, or approved by OTS.

Encryption

Purpose and Scope

In order to ensure Confidential and Restricted Data are adequately protected and compliant with regulatory requirements, it is imperative that only authorized data encryption methods shall be used. This policy section documents the standards for storing and transmitting Confidential and Restricted Data, whether managed by an Agency, the Office of Technology Services (OTS), or a third party. This section also provides policies for the management of encryption keys.

This section does not intend to conflict with any Federal, State, or local law for use of encryption technologies outside of the United States.

Encryption Standards

Confidential and Restricted Data that will traverse the internet, public or untrusted networks, or transmitted wirelessly shall be encrypted in accordance with Encryption Requirements. In addition, Confidential and Restricted Data stored on laptops and other portable devices, shall be encrypted in accordance with Encryption Requirements. In the event technical or operational limitations are identified and cannot be addressed, which prevent the required use of encryption for laptops and other mobile devices, the Agency shall complete the Exception Request process.

The use of proprietary data encryption methods for Confidential and Restricted Data protection is strictly prohibited.

Encryption Key Management

Encryption keys must be generated, accessed, distributed and stored in a controlled and secured manner as specifically required below.

Key Access

Access to encryption keys used to encrypt and decrypt Restricted Data must strictly comply with Access and Identity Management. The Chief Information Security Officer (CISO) is the Data Owner of encryption keys. The CISO shall perform periodic reviews of the users with access to encryption keys.

Split Knowledge and Dual Control

When required, a minimum of two encryption key users are required to perform any key action (such as key generation or loading the key). Additionally, no single user with encryption key access shall know or have access to all pieces of a data encryption key.

Key Generation

Creation of encryption keys must be accomplished using a random or pseudo-random number generation algorithm. Generating encryption keys must be accomplished by a minimum of two authorized users.

Key Storage

All encryption keys must be encrypted and stored in a secure location as determined by CISO. Key-encrypting keys must be stored separately from data-encrypting keys. Clear-text backups of encryption key components must be stored separately in tamper-evident storage in a secure location. Only users with access to encryption keys shall be authorized to retrieve key components from secure storage or distribute encryption keys.

Key Changes and Destruction

An encryption key change is the process of generating a new key, decrypting the current production data and re-encrypting the Confidential and Restricted Data with the new encryption key.

All data encryption keys must be changed when circumstances dictate a change by the Chief Information Security Officer (CISO) to maintain data encryption or key integrity. The following are circumstances that may dictate when an encryption key change is required:

- Regular Rotation: Keys shall be changed at least annually, where applicable as determined by the CISO.
- Incident Response: Any identified (actual or suspected) unauthorized access to or exposure of encryption keys, determined during the scope of actions performed in accordance with the Incident Management.
- Suspicious Activity: Activity related to the encryption key process which raises concern regarding the exposure of the existing encryption key.
- Resource Change: As deemed necessary by the CISO, a process shall begin to change encryption keys when a user with knowledge of the encryption keys ends employment or assumes a new job role that no longer requires access to an encryption process.
- Technical Requirement: Encryption keys shall be changed if the encryption key has become questionable due to a technical issue such as corruption or instability.

All data encryption key changes shall be documented as required in Encryption Requirements. Encryption keys no longer in service are to be disposed of in accordance with Data Sanitization.

Transmission of Confidential and Restricted Data

Confidential and Restricted Data must be encrypted when it is transmitted across public or untrusted networks, including but not limited to, email, or transmitted wirelessly. Encryption methods must be in implemented in strict compliance with Encryption Requirements.

Examples of acceptable encryption levels include:

- Transport Layer Security (TLS)
- Internet Protocol Security (IPSEC)

All wireless devices and networks in use at OTS and Agency facilities must be configured in accordance with Network Devices and Communication and Encryption Requirements.

Disk Encryption

Electronic media or mobile computing systems storing Confidential and Restricted Data, where feasible, shall be rendered unusable, unreadable, or indecipherable by disk encryption implemented in compliance with Encryption Requirements. Feasibility will be determined based on technical functionality, a risk analysis performed by the IST, the applicable operational OTS section, and the Data Owner.

Although the use of encryption may not be absolutely required in all instances, the intention of this policy is to require the use of encryption for all mobile devices and removable electronic media stores that potentially stores, processes, or used to access Confidential or Restricted Data.

End User Facing Devices and Technologies

Purpose and Scope

End User Facing Devices and Technologies refers to all computing systems, devices, applications, and interfaces, including remote access technologies (VPN or dial-in modem access), wireless technologies, removable electronic media (USB drives, CD drives, external hard-drive, etc.), mobile computing devices (laptops, smartphones, tablet computers, PDAs, etc.), and e-mail, internet and instant message programs, that store, process, or transmit data. This policy section sets forth the requirements and approval process for End User Facing Devices. End User Facing Devices that are not owned, leased, or managed by an Agency or Office of Technology Services (OTS) shall not be allowed to directly connect to the State's network unless prior approval is given by the Information Security Team (IST).

Approved Devices and Inventory

Any production, test, or pilot deployment of a new End User Facing Device or Technology shall be reviewed and approved by the IST prior to production implementation. The IST, working with the appropriate OTS operational sections, shall maintain a list of Approved End User Facing Technologies.

Additionally, all End User Facing Devices and Technologies must be inventoried as required by Information Asset Management and must be configured and managed as required by System Configuration.

Device Requirements

Authentication

All End User Facing Devices and Technologies shall be deployed and maintained with User authentication mechanisms, including usernames and passwords as required by Access and Identity Management.

Remote Access

All End User Facing Devices and Technologies with remote access to the State's networks shall be accessed via secure authentication and data encryption technologies which comply with the State's Password Requirements. Multi-factor authentication for privileged users or systems which require elevated security may be required in accordance with Access and Identity Management.

Wireless Access Points

The purchase and placement of any wireless access points within any Agency location shall be authorized by OTS and the IST prior to deployment. Additionally, all wireless access points shall be tracked by OTS Network Services using a wireless access point location tracking list.

Acceptable Use

Use of End User Facing Technologies is subject to End User Agreement.

Personally Owned Devices

When deemed necessary, Personally Owned Devices maybe utilized with prior approval by the Agency Section Director, Data Owner, and IST.

Storing Confidential or Restricted Data on Personally Owned Devices is strictly prohibited without the use of Encryption and prior approval of the IST.

Secure Software Development

Purpose and Scope

This policy section applies to all new custom software and updating of existing custom software developed by an Agency, the Office of Technology Services (OTS), or third party.

The Information Security Team (IST) will support the appropriate teams developing, maintaining, and participating in the SSDLC process for the development, testing, and deployment of custom software.

Secure Software Development Life Cycle (SSDLC)

Requirements Analysis

A risk assessment shall be conducted by reviewing the documented operational requirements for the planned software or update.

Design

Application components must be planned in a manner consistent with data and network security best practices.

Application Security Risk Assessment

The IST, in coordination with the development team, will conduct an Application Security Risk Assessment for each application prior to deployment. The Application Security Risk Assessment will document the key risk areas as defined in Risk Assessment Standards and Requirements.

Development

Developers must consider application security vulnerabilities (*e.g.*, memory bound issues, privilege and access bypass, input validation, etc.) as part of the development process.

Code Review

A second developer (Agency, OTS, or third party), other than the originating code author, must conduct code reviews of all new and changed software, specifically in an attempt to identify security issues. For web applications, code reviews must confirm that code is developed according to the Web-Based Applications requirements. Special care shall be given to web-based and external facing applications. System architects and developers who create or modify web-based and external facing applications shall receive training on secure coding practices and refresher training annually.

Quality Assurance Implementation

Implementation must not compromise security controls already in place, or introduce new security vulnerabilities.

Quality Assurance Testing

For new application development, in addition to standard testing, all security features of the application must be tested.

Documentation

All application features and implementation documentation should include direction on proper security configurations.

Production Implementation

Implementation should not compromise security controls already in place, or introduce new security vulnerabilities.

Production Testing

In addition to standard testing, relevant security features of the application shall be tested.

Maintenance

In addition to standard testing, all new security features of the application shall be tested.

Non-Production Environments

A Non-Production Environment is simply any environment that is not the actual production environment.

Examples of Non-Production Environments include, but are not limited to the following:

- Development
- Test (Quality Assurance or User Acceptance)
- Staging
- Pilot
- Beta
- Proof of Concept (PoC)

Separation of Environments and Duties

Non-Production Environments shall be separated from the Production application, system, and database.

Individuals in development or testing roles shall not have access to production systems, unless approved by the IST.

Access Controls

Non-Production environments with access to an Agency's production network(s) must have access controls pursuant to Access and Identity Management.

Any data, accounts, or access used for testing must be removed from the production software candidate prior to production implementation. In addition, all vendor default supplied application accounts, user IDs and passwords must be changed or disabled prior to production utilization or released to end users.

Confidential or Restricted Data

Confidential or Restricted Data shall not be used for Non-Production Environments without sufficiently de-identifying and sanitizing, such that it cannot be recovered (e.g., use of encryption with sufficient key management controls). De-identification or sanitization must be completed in a temporary Production environment prior to transferring Confidential or Restricted Data to a Non-Production Environment.

In instances where Confidential or Restricted Data absolutely must be used to support testing and development efforts and de-identification or sanitizing is not feasible, a Request for Exception shall be submitted and approved by Data Owner and the IST.

Production Environments

Production Environment management must include the necessary controls and processes to ensure proper separation of duties.

Code Promotion

Only authorized system administrators shall be responsible for any code promotion to a Production Environment.

Access Management

Individuals performing Software Development for an application shall not be granted any privileged (Read or Write) access to the corresponding Production application, system, or database. Under emergency situations, Software Development resources may assist in troubleshooting production applications through the use of an alternatively created ID or account in accordance with Access and Identity Management.

Software Utilizing Restricted Data

Displaying Restricted Data

To the extent it is practical, any software processing Restricted Data must be designed in a manner which masks, truncates, or sanitizes the displayed Restricted Data to a subset of the information for reference purposes (e.g. last four digits of social security number, last four digits of the credit card number) and limits the display of Restricted Data to only one record at a time.

If the full content of the Restricted Data must be displayed for the functionality of the software, approval must be provided by the Information Security Team (IST) during the Requirements Analysis Phase of the SSDLC.

If the full set or Restricted Data must be displayed or more than one record must be displayed is required for the functionality of the software, approval must be provided by the Data Owner and the IST during the Requirements Analysis Phase of the SSDLC.

Printing or Exporting Restricted Data

To the extent possible, any software processing Restricted Data must be designed in a manner which masks, truncates, or sanitizes the exported or printed Restricted Data to a subset of the information for reference purposes (e.g. last four digits of social security number, last four digits of the credit card number) and limits the Restricted Data exported from the application.

If exporting or printing full sets or Restricted Data is required for the functionality of the software, approval must be provided by the Data Owner and the IST during the Requirements Analysis Phase of the SSDLC.

Additional requirements for printing Restricted Data are located within Agency Physical Data Security.

Storing Restricted Data

To the extent possible, any software storing Restricted Data must be designed in a manner that the software encrypts the Restricted Data at the database field level in order to provide adequate data protection. The methods utilized, including encryption key management, must comply with Encryption.

If encrypting Restricted Data at the database field level is not technically possible or operationally feasible, approval must be provided by the Data Owner during the Requirements Analysis Phase of the SSDLC.

Web Applications

Any Web Application processing Restricted Data must be designed in a manner that ensures Restricted Data:

- Is never stored in an URL.
- Is never stored on the client.
    - Including Browser Cache or User Cookie.
- Is never accessible without proper authentication and authorization.

In instances that require Web Application to process Restricted Data in a manner that conflicts with the requirements within this policy section, approval must be provided by the Data Owner and the IST during the Requirements Analysis Phase of the SSDLC.

Passwords

Software requiring to store or utilize passwords must be designed, developed, and implemented in accordance with Password Requirements.

Incident Management

Purpose and Scope

The State of Louisiana recognizes the importance of establishing an Incident Management Program capable of timely actions and communications to ensure appropriate and consistent responses to each incident. This policy section clearly establishes the phases, actions, responsibilities, and documentation requirements for handling all incidents.

This section applies to any and all efforts related to the detection, action, documentation, and communication of an Incident.

Incident Management Program

All Incidents are handled in accordance with the following seven-phase Incident Management program:

- Preparation
- Identification and Classification
- Containment
- Eradication
- Recovery and Remediation
- Lessons Learned
- Continuous Program Evaluation

Preparation

To ensure all Incidents are identified and consistently managed, meaning all formal policies, plans, and procedures shall be developed, implemented, maintained and executed in a timely manner. To facilitate accurate and timely Incident Management, a pre-defined course of action shall be created that will be followed during the course of each Incident.

Additional Preparation requires, but is not limited to the following:

- The development and implementation of a formal Incident Response Plan.
- The creation and periodic evaluation of defined Incident Classifications.
- The assignment of an Incident Response Team (IRT) with specific roles and responsibilities, relevant administrative personnel, and committed technical or process subject-matter experts.
- The creation and periodic evaluation of specific communications channels.
- Procurement of the required supplies, tools, technologies, and facilities to support IRT processes and actions.

Identification and Classification

To facilitate the timely identification of Security Events, a strategic combination of technical and non-technical controls shall be employed to collect events from appropriate sources.

Event Types

The following Security Events are both technical and non-technical events that individuals should identify and report as potential Incidents.

- Theft, Loss, or Damage of Asset

  Examples: lost or stolen device, electronic media, or physical documents; deleted or missing log files, or unscheduled/unauthorized physical entry.

- Unauthorized Access

  Examples: Viewing PII or PHI without a need to know, operational requirement, or prior authorization; external source attempting to access internal resources.

- Evidence of Fraud

  Examples: False information within databases, logs, files, or physical records.

- Unauthorized Sharing or Exposure of Data

  Examples: Improper disposal of electronic media containing Confidential or Restricted Data.

- Unexpected or Abnormal System Behavior

  Examples: Unscheduled reboot, unexpected messages, abnormal or suspicious errors in system or application log files, or attempted connections to undocumented external systems.

- System Generated Alerts

  Examples: File integrity alerts, intrusion detection alerts, anti-virus software notifications, or physical security alarms.

- Policy violations

  Examples: Violation of End User Agreement, including sharing usernames and passwords.

Event Reporting

Any individual, regardless of assigned duties or job function, has a responsibility to report any suspected, potential, or actual Security Event. Once an individual becomes aware of a suspected, potential, or actual Security Event, the individual shall report the Security Event as outlined below.

Third parties shall report Security Events within the timeline and to the contact contained within the third party agreement.

Employees shall report Security Events to their supervisor.

End User Support Services, Agency Relationship Manager, or other OTS resource, upon identification or receiving notification of a Security Event, shall immediately notify the Information Security Team (IST).

Evidence Preservation

For Security Events involving a potentially compromised system or device, the user or system administrator, once aware, shall not tamper with, use, or take any other action, including login or turning it off, until advised by the Chief Information Security Officer (CISO), or designee, directly; as any action may indefinitely remove forensic evidence required to accurately assess the Security Event.

A Chain of Custody form shall be created, maintained, and directly attached to any evidence.

Event Evaluation

Upon receipt of a Security Event notification, the Chief Information Security Officer (CISO), or designee, will assess, evaluate for legitimacy, and make final determination if the Security Event is promoted to an Incident.

If the Security Event is declared an Incident, the Chief Information Officer (CIO) shall be notified and the Incident Response, Management, and remediation actions set forth in this policy shall be implemented.

If the Security Event is not declared an Incident, the CISO, or Information Security Team (IST) will forward to the appropriate resource for operational analysis and disposition.

Incident Classification

The CISO, or designee, shall assess the severity of the Incident and provide a classification level as provided in Incident Response Plan.

Incident Response Team (IRT) Assignments

Events determined to be Incidents must be assigned a dedicated incident handler and must be processed in accordance with the procedures defined in the Incident Response Plan.

Additional IRT positions are assigned as applicable by Incident.

Incidents involving the potential breach of Confidential or Restricted Data require Office of Human Capital Management (OSHCM) and the applicable Legal IRT member assignment.

Incident Report and Documentation

Upon the classification of an Incident, the assigned incident handler must initiate an incident report as outlined in the Incident Response Plan.

Incident Communication

Once an Incident has been classified, an incident handler has been assigned, and the incident report has been initiated, communication flow must begin.

Incident communication must follow the guidelines established in the Incident Response Plan.

The details of an evolving incident shall be communicated to as few people as possible without compromising the ability to successfully manage the incident.

Chain of Custody

A Chain of Custody must be established for all gathered evidence as required in the Incident Response Plan.

Evidence Collection

IRT shall collect, log, and retain evidence of the Incident based on severity.

Evidence collected by IRT shall include but is not limited to system logs, reports, emails, and helpdesk tickets containing details of the Incident, and first-hand accounts.

The IRT shall use forensic evidence collection and handling procedures, approved by the CISO, to determine the scope of the incident, the source of the Incident, and to determine the likelihood that Confidential or Restricted Data was compromised.

Containment

A strategy shall be employed, based on the results and details of the previous Identification and Classification phase that appropriately addresses both short-term and long-term containment. Additionally, during this phase, the IRT shall begin a root-cause analysis of the Incident prior to beginning the eradication phase**.**

Short-Term Containment

Based on the criticality of the affected system or source, and the likelihood of exploitation of the identified vulnerability, the IRT may work in accordance with Data Owners and identified Subject Matter Experts to achieve short-term containment.

Examples include, but are not limited to, taking backups, shutting down systems, denying network traffic, and system isolation.

The determination to remove a system from production use may be made by the IRT in conjunction with the affected Data Owners; however, the IRT maintains exclusive rights to remove an affected system from production depending on the identified or potential criticality of the Incident.

Long-Term Containment

After ensuring the identified Incident has been contained, the IRT shall work with Data Owners and Subject Matter Experts to devise a long-term strategy for containment.

Examples include, but are not limited to, cloning an infected system into a quarantined network for analysis and restoring the compromised system to production use.

The restoration of a system to production use must follow the Eradication phase set forth in this policy.

Root-Cause Analysis

Upon completion of Short-term Containment, the IRT will work in conjunction with relevant Subject Matter Experts to identify the root-cause of the incident.

Root-cause analysis should include but is not limited to, system or application vulnerabilities, system or application misconfigurations, network misconfigurations, breaches of physical security, or other non-technical scenarios.

The identified root-cause analysis must be included in the incident response report and must be specifically reviewed in the Eradication and Lessons Learned phases set forth in this policy.

Eradication

The IRT, in conjunction with system or application owners and relevant subject matter experts, shall work through a formal process to identify and eliminate all components that may have led to the root cause of the Incident prior to returning an affected system to production use.

Eradication actions may include, but are not limited to:

System and Application Patching

If available, relevant system and application patches must be applied prior to restoring a system to production use.

Resetting, Reconfiguring, or Removing User Accounts

Compromised or potentially compromised network, system, or application account passwords shall be disabled until able to be reset.

Re-Imaging Compromised Systems or Devices

If determined to be compromised at the machine-level, the IRT may require that a system be rebuilt to ensure that all vulnerabilities, unapproved software, or configuration are removed.

Re-imaging may include a completely new server, instance of the operating system, and application software.

Improving Network Defenses

The IRT may require that network controls be re-evaluated depending on the results of the incident investigation.

Additional controls may include, but are not limited to firewall rules, intrusion detection/prevention signatures, web application firewalls, web access filters, or host firewall rules.

Recovery and Remediation

Upon the completion of Containment and Eradication phases the IRT will evaluate the resulting security posture of the affected systems or resources prior to returning a system to production. The IRT may employ internal Subject Matter Experts or external parties to evaluate implemented remediation efforts. Where possible, the IRT shall implement additional monitoring controls of affected systems for an appropriate period of time after re-entry into production. Additionally, the Chief Information Security Officer (CISO), or designee, may periodically re-evaluate the security posture of the affected systems or resources.

Long-Term Remediation

Upon identification of the root-cause of the incident, the IRT and affected Data Owners must agree to a long-term resolution. Remediation actions which require further effort, such as the acquisition of new technology, reconfiguration of existing systems and networks, and additional logging, must be formally documented with reasonable timelines established. Such timelines may be dependent on the severity of the incident and the likelihood of re-exploitation. All incidents must be considered “open” until all members of the IRT and affected Data Owners agree that all identified corrective measures have been implemented.

In the unlikely event that Long-Term remediation actions cannot be agreed upon, the Chief Information Officer (CIO), consulting with the CISO and Data Owner, shall determine the actions required for Long-Term remediation.

Lessons Learned

Following the Remediation and Recovery phase, all members of the IRT, and any other affected/applicable parties will meet to review the results of the investigation to discuss the root cause of the Incident in accordance with the Incident Response Plan.

The IRT shall evaluate the effectiveness of this Incident Management policy section and recommend any appropriate changes to the CISO or ISGB.

Objectives of the Lessons Learned phase require, but are not limited to, identify what happened (in addition to the root cause), identify if the Incident could have been prevented with existing controls, and to identify opportunities to improve the security posture of the affected system or resource.

Continuous Program Evaluation

In order to ensure the Incident Management Program maintains the appropriate support, preparedness, and awareness, a commitment for Continuous Program Evaluation efforts are required as outlined below.

Testing and Training

At least once every 12 months, a mock incident will be initiated by the CISO without the prior knowledge of the IRT or other relevant personnel to evaluate the preparedness and efficiency of the response plan.

The Incident type and severity will be at the discretion of the CISO.

Independent of the unplanned mock-incident test, training regarding Incident response responsibilities shall be performed at least annually to prepare IRT members and other applicable resources for actual and test Incidents.

Recurring IRT Communication

The IRT shall remain informed of all currently open Incidents via the methods established in Incident Response Plan.

The IRT shall be notified of the status of Incidents that are currently being investigated.

The IRT shall also be notified of the status of currently pending incident remediation efforts.

Risk Management

The Chief Information Security Officer (CISO), in consultation with the Chief Information Officer (CIO), shall periodically evaluate risk areas for potential security risks.

To the extent necessary, the CISO shall assess the State's technical environments to identify risks and assess the ability to prevent, measure, and respond to incidents.

Where new potential risks are identified, the appropriate actions required to update Office of Risk Management (ORM) shall be taken.

All risk assessment activities required within this policy section shall be completed in adherence to Risk Management.

Data Center Security

Purpose and Scope

This policy section provides the policies for managing and monitoring the physical access of State Employees, third parties, and visitors to State owned, operated, or managed Data Center facilities.

ID Badgess

As a vital part of Data Center security, State ID badges with an individual's name, photo, and department shall be issued and maintained during the entire course of employment, assignment, or engagement. An ID badge shall serve as an electronic key to access a Data Center and other secured areas as needed.

ID Badge Display Requirements

Employees shall, at all times, clearly display their ID badges when present in Data Center facilities. Third parties and visitors shall, at all times, clearly display an ID badge or a visitor sticker.

ID Badge Creation

The Office of State Buildings (OSB) shall create Employee ID badges in a physically secure environment. Only designated personnel shall have access to the Employee ID badge creation system and the ability to create ID badges.

Additionally, each ID Badge created shall be assigned a Unique ID. Unique IDs shall be recorded along with the full name, Agency or company, and job role or position.

ID Badge Assignment

ID Badges shall be assigned in the following manner:

- New Employee ID Badge Administration

  The new Employee's supervisor shall complete a request for an ID Badge & security access and submit the request to OSB. Data Center Operations (DCO) grants physical access after receiving an approved authorization request from OSB. Employee ID Badges shall clearly identify the Employee name, Agency, and Office or Section. All ID badges must contain a photograph of the Employee.

- Third Party ID Badge Administration

  Upon request by an Employee, the Data Center receptionist or other individual designated by Data Center Operations (DCO) management, shall assign third parties a temporary ID badge.

  Third parties shall have no physical Data Center access privileges and shall be monitored or accompanied at all times by an Employee unless additional Data Center access was approved by the Director of Data Center Operations and the Information Security Team (IST). To obtain additional facility access for a third party, the requesting Employee must submit the request to Data Center Management.

  All third party ID badges or stickers must be surrendered at the conclusion of the third party's business with the State. The Employee responsible for the third party shall confirm that the third party ID badge or sticker is returned to the receptionist, other office designee, or properly disposed.

- Visitor ID Badges and Stickers

  Upon request by an Employee, the Data Center receptionist or other individual designated by DCO management, shall provide visitors with a visitor ID badge or sticker.

  Visitors shall have no physical facility access privileges and shall be monitored or accompanied at all times by an Employee.

  All visitor ID badges and stickers must be surrendered at the conclusion of the visit.

Changing ID Badge Access

All requests for a change in physical access level through the use of an ID badge must be submitted by the Employee's supervisor (Director of above) to Data Center Operations (DCO) management.

Revoking ID Badges

The Employee's direct supervisor is primarily responsible for collecting the assigned ID Badge from the State Employee and notifying DCO when the Employee is no longer employed by the State; DCO management shall disable all badge access for the departed Employee in a timely manner.

The Employee who initially requested the access for a third party's ID Badges shall be responsible for contacting DCO for badge deactivation at the end of their contracted time period or when engagements have completed. Badge access duration for third parties shall not extend past 12 months without an additional request for extension.

DCO shall monitor third party badge access to Data Centers by minimally reviewing access reports on a quarterly basis.

Lost or Stolen ID Badges

Individuals shall notify the OSB and DCO management in the event that their ID Badge is lost or stolen. DCO shall remove access to the lost or stolen ID Badge immediately as practical.

Facility Security

Visitor Logs

All third parties and visitors are required to enter through the primary entrance of the Data Center and check in with the Data Center receptionist upon their entrance unless the individual had previously been issued a State contractor ID badge. Third parties and visitors shall sign the visitor log or check-in using an electronic kiosk. The visitor log or kiosk must require the third party or visitor to provide his/her name and company (if applicable), time of entry and exit, date, and contact information.

All third parties and visitors to Data Centers must sign an additional Data Center visitor log prior to gaining access to the primary data hosting areas.

Visitor logs must be retained for minimum of seven years by DCO management and disposed of in accordance with Data Sanitization.

Facility Security

Security perimeters (*e.g.*, walls, card controlled entry gates, or manned reception desks) and controls (*e.g.*, guards, access badges, or security cameras) shall be used, to the extent practicable, to protect Data Center facilities from unauthorized access or vandalism.

External doors shall contain a locking mechanism to prevent unauthorized access and allow for the logging of the entry.

Doors to internal secure areas shall lock automatically, implement a door delay alarm, and be equipped with electronic locks (*e.g.*, keypad, card swipe), where practicable.

Doors and windows shall be locked when unattended and external protection should be considered for any windows, particularly windows at ground level.

Any repairs or modifications to the physical components of a Data Center which are related to security (e.g., hardware, walls, doors, and locks) shall be documented, retained for minimum of seven years by Data Center Operations Management, and disposed of in accordance with Data Sanitization.

Reception Area

Data Center facilities must control physical access to the building to process visitors and third parties.

Access to Data Center facilities from the reception areas is restricted to Employees and third parties that have been granted temporary access rights.

Internal directories or documentation indicating Data Center areas containing Confidential or Restricted Data shall not be readily accessible to the public facing reception area or any other public areas.

After Hours Security

To the extent practicable, Data Center facilities shall maintain electronic security measures to prevent unauthorized entries during non-working hours. Where possible, the electronic security measures should be able to identify each person who enters the premises after-hours, as well as the time of entry and exit. If an electronic security system is not practicable, the facility should maintain a log of persons to whom keys, security alarm codes, and access codes are granted.

System Security

Entry controls, including ID Badge access or security cameras, shall be used to limit and monitor physical access to Data Center systems that store, process, or transmit Confidential or Restricted Data.

Data Center Operations (DCO) shall ensure, when appropriate, that Data Center facilities segregate the State's data from data provided by other non-State entities.

Where applicable, facilities housing data processing activities shall give minimum indication of their purpose, with no obvious signs, outside or inside the building identifying the presence of information processing activities.

Agency Physical Data Security

Purpose and Scope

This policy section provides the additional policies for securing physical data owned, managed, or held in trust by the State. This policy section applies to all State Employees, third parties, and visitors to State owned, operated, or managed facilities.

Securing Confidential and Restricted Data

Printed Materials

Printed materials containing Confidential or Restricted Data should be secured when workforce members are away from the work space. Printers should be located in areas not easily accessible by the public. Printer controls shall be set so that pages will be printed face-down or with a cover sheet where technically possible.

Telephonic Disclosures

Prior to disclosing any Confidential or Restricted Data over the telephone, it is the obligation of the Employee to verify the identity of the person with whom they are speaking.

Employees shall refrain from discussing or otherwise communicating Confidential or Restricted Data in the presence of persons not entitled to access such data.

Voice Messages

Employees shall refrain from disclosing Confidential or Restricted Data in any Voice Message, if possible. In the event that Confidential or Restricted Data must be disclosed, Employees should leave a message containing only the minimum amount of Confidential or Restricted Data necessary for the purpose of the disclosure.

Facsimiles

- Outgoing Facsimiles

  Confidential or Restricted Data may be faxed to persons or entities that are lawfully or contractually entitled to receive the data. Individuals should verify the number to which facsimiles will be transmitted prior to transmission. A copy of the facsimile transmission verification sheet should be retained and maintained by the Agency. All facsimile cover sheets shall contain an Agency approved disclaimer informing the recipient that the transmission includes Confidential or Restricted Data.

- Incoming Facsimiles

  Agency fax machines shall be located in areas not accessible by the public. Where possible, fax machine must be set so that incoming pages will arrive face-down.

  Received facsimiles should only be initially read by the individual(s) to whom the transmission is directed such that only the designated recipient may ascertain any other person(s) with whom the transmission should be shared or directed.

Clean Desk

To the extent operationally possible, an Employee shall ensure all physical materials containing Confidential and Restricted Data are removed from a desk or common work area and adequately secured when items are not in use.

Dry-Erase Boards, Bulletin Boards

Dry-erase boards, bulletin boards, and similar modules on which Confidential or Restricted Data is written should not be placed in open areas or in locations that are easily visible or accessible to non-State employee personnel. s

Security of Data in Vehicles

Employees using vehicles to transport Confidential or Restricted Data shall exercise the utmost caution in order to safeguard the privacy of and access to such material. Confidential or Restricted Data should be stored inside the vehicle's trunk during transport, or in vehicles not having trunks, should be placed out of plain view. At no time should such materials be left on car seats or in unlocked vehicles. Confidential or Restricted Data shall not, to the extent possible, be stored in vehicles overnight.

Offsite Working Environment

Employees or contractors working offsite shall ensure appropriate physical safeguards are in place to protect Confidential and Restricted Data. When data is not being used, it shall be stored in locked filing cabinets, a sesparate home office with locking door, closets with locking doors, or other reasonable physical controls that prevent access by unauthorized individuals.

Audit Logging and Event Monitoring

Purpose and Scope

This policy section provides the policy for ensuring that procedures are in place for real time monitoring of access to Confidential and Restricted Data. All computing systems in production or intended for production use, whether managed by an Agency, The Office of Technology Services (OTS) or by third parties, must be built, deployed, and configured in accordance with the requirements of this section.

Event Logs

Agency computing systems, network devices, or third party systems connected directly to any State network shall be configured to generate automated event logs in accordance with the Audit Logging Standards and Requirements. The event logs shall minimally account for all user access to Confidential and Restricted Data.

Event Log Access and Retention

Event logs, audit tools, and audit trails shall be stored in a centralized location and only be accessible to authorized users in accordance with Access and Identity Management. Additionally, event logs are to be maintained in accordance with Agency record retention policies and disposed of in accordance with Data Sanitization.

Event Log Security

A method for change detection shall be implemented for Event Logs to ensure that the Information Security Team (IST) is notified when changes are made to existing event log data.

Event Log Reviews

Event logs shall be reviewed by the Information Security Team (IST) in accordance with the Audit Logging Standards and Requirements. In the event of an exception alert, the IST shall respond to the event pursuant to Incident Management.

Risk Management

Purpose and Scope

Risk Management is the ongoing process of assessing, identifying, documenting, prioritizing, responding, and monitoring potential or inherent risk associated with any device, system, application, network, service, third-party, data storage facility or information used to support or provide any operational or business process. Establishing a Risk Management framework is essential to maintaining and strengthening the security, reliability, resiliency, and recoverability of the State systems, services, and data.

This policy section further defines the responsibilities, methods, and actions that shall be taken to effectively manage risk.

Risk Ratings

Using the detailed steps in Risk Assessment Standards and Requirements, any identified risk shall be assigned one of the following:

Critical

A Critical Risk is a risk that is certain to occur and will have clear catastrophic or major impact to an Agency, individual, or the State as the result of loss of confidentiality, integrity, or availability due to absence of security controls.

- *Examples of Critical Risk*

  Include, but not limited to: unauthorized use or disclosure of Restricted Data, unintended modification or corruption of data or systems utilized by critical Agency processes, unrecoverable failure of a system, device, or control providing or supporting a critical public service.

High

A High Risk is a risk that is possible or expected to occur and will have clear moderate or major impact to an Agency, individual, or the State as the result of loss of confidentiality, integrity, or availability due to absence of security controls.

- *Examples of High Risk*

  Include, but not limited to: unauthorized disclosure of Confidential Data, limited unauthorized disclosure of Restricted Data, unintended modification or corruption of large file server or data source, unintended or unplanned interruption of services utilized to provide critical public services.

Moderate

A Moderate Risk is a risk that can be improbable or unlikely to occur and have a moderate or major impact, or certain and have minor or insignificant impact to an Agency, individual, or the State as the result of loss of confidentiality, integrity, or availability due to absence of security controls.

- *Examples of Moderate Risk*

  Include, but not limited to: unauthorized use, disclosure, or modification of Uncategorized Data, limited unauthorized disclosure of Confidential Data, unintentional modification or corruption of non-critical production devices, systems, or data sources; or unintended interruption in availability of a system, device, or control providing or supporting a critical public service.

Low

A Low Risk is a risk that signifies a risk that has limited impact or generally accepted risk to an Agency or the State as the result of loss of confidentiality, integrity, or availability.

- *Examples of Low Risk*

  Include, but not limited to: unauthorized use or disclosure of Uncategorized Data, workstation failure, unintentional modification or corruption of test or development devices, systems, or data sources.

Risk Assessments

All formal and informal information security or technical risk assessments shall be performed as outlined in Risk Assessment Standards and Requirements.

Responsibilities

Agencies shall:

- Ensure operational processes exist to ensure both formal and informal risk assessments are performed as specifically outlined in Risk Assessment Standards and Requirements.
- Ensure any alternate risk mitigation recommendations are thoroughly evaluated prior to Risk Acceptance.

The Information Security Team (IST) shall:

- In accordance with previously defined responsibilities, ensure risk is assessed in accordance with Risk Assessment Standards and Requirements.

The Chief Information Security Officer (CISO) shall:

- Ensure formal internal and external final risk assessment reports are reviewed by the Information Security Governance Board (ISGB) and OTS Executive Leadership, in addition to any affected Agency Leadership, Data Owner, or key stake holder.
- Initiate Risk Acceptance Forms when required.
- Retain record of all Risk Acceptance Forms.
- Inform ISGB of any accepted risk.

Risk Acceptance

A Risk Acceptance Form must be completed by the CISO, acknowledged by the CIO, and requires the additional approval of the affected Data Owner and the Agency's Executive Director in order to accept any identified risk for which mitigation, avoidance, or transference is not possible, preferred, or deemed unacceptable.

Training and Awareness

Purpose and Scope

In order to ensure all individuals are properly educated and aware of Information Security Policies, processes, procedures, and the requirements for data protection; the State of Louisiana must establish appropriate methods to provide Information Security Training and Awareness. This policy section clearly indicates the responsibilities and actions required to ensure Information Security Training and Awareness are properly provided to individuals before and during the course of their employment, contract, or engagement.

Responsibilities

Agencies shall establish operational processes to ensure Employees and partners receive initial and on-going training, including the capture and retention of the acknowledgement, in addition to supporting opportunities to improve awareness for the State's Information Security Policy, as outlined in this policy section.

New Employee Training

Upon hire, all Employees shall receive appropriate training on the policies and procedures regarding the privacy and security of data. Employee training shall include a review of the Information Security Policy and require the successful completion of a post-test.

Annual Employee Training

Each year, all Employees shall receive follow-up training on the policies and procedures regarding privacy and security, and shall successfully complete a post-test.

Third Party and Independent Contractor Training

Depending on the scope of work, the Information Security Team (IST) may require that certain third party employees and independent contractors complete privacy and security training, which must include the policy and procedures regarding privacy and security relevant to the current scope of work. In instances where third parties or independent contractors are required to complete Information Security Training, the third party or independent contractor shall provide the state with evidence of each successful individual completion of a post training test.

Remedial Training

In the event of a complaint, investigation, policy violation, or routine audit reveals that an Agency or any part thereof requires additional training, the Chief Information Security Officer (CISO) may require that all appropriate individuals complete remedial training, the receipt of which shall be conducted and documented in accordance with Office of Human Capital Management (OSHCM) Policy and processes or the partner's contractual agreements.

Specialized Training

When an Agency requires specialized applications or hardware to its operational processes, the Agency shall also provide the training and awareness for applicable staff, as deemed necessary by the IST.

Awareness Opportunities

As part of Statewide, Regional, Agency, or Office communications or meeting(s), the CISO or designated Information Security Officer (ISO) shall be authorized and allowed opportunity to utilize such opportunities to raise awareness of the State's Information Security Policy.

Training Records

Agencies shall use appropriate means to document and retain all training records for a minimum of 5 years. Additionally, training records shall be readily available to support any audit or review.

Third Party and Data Sharing Agreements

Purpose and Scope

This policy section sets forth the responsibilities and contractual requirements when third parties are utilized to provide goods or services to an Agency. This policy section applies to all third parties that store, process, or transmit Confidential and Restricted Data for an Agency, otherwise have access to such data, or require access to Agency systems.

This policy section also speaks to the Information Security requirements and considerations taken when executing a Data Sharing Agreement (DSA) between two Agencies exchanging Uncategorized, Confidential, or Restricted Data.

It is not the intent of this policy to needlessly increase the operational expense of any (current or potential) third party, but rather to ensure the controls and mechanisms required for data protection are implemented, managed, and monitored in order to prevent the loss or exposure of the State's Confidential or Restricted Data.

Due Diligence

Prior to contractually engaging any third party, the Information Security Team (IST) shall verify, through proper due diligence, that the third party has implemented reasonable measures to protect Confidential and Restricted Data from unauthorized access, acquisition, destruction, modification, and disclosure.

The IST may rely upon any industry accepted certification obtained by the third party within the previous 12 months as validation of effective security controls. In the event the third party does not have any independent representation of effective security controls, or the evidence provided is deemed inadequate by the Data Owner or Chief Information Security Officer (CISO), the third party shall be required to complete the IST's Third Party Information Security Questionnaire and make available the resources required for the IST the perform a review (of the third party) as outlined in Risk Assessment Standards and Requirements.

Any identified and unmitigated risk to Confidential and Restricted Data shall be documented and require a Risk Acceptance Form by the Data Owner, containing the Agency Executive Director's approval, prior to transferring data to the third party.

Note: In instances where the State or its Agencies have signed a contractual agreement with a third party prior to the initial publication date of the Information Security Policy, the third party shall not be held to the requirements stated within this policy section that were not previously contained or referenced within the executed agreement. However, the State and its Agencies shall ensure any new, renewed, or amended agreement directly comply with the processes and requirements for third parties contained within the Information Security Policy.

Prior to Exchange of Data

Access to the Agency's Confidential and Restricted Data **shall not** be provided until the third party has signed a contractual agreement minimally containing:

- End User Agreement
- Non-Disclosure and Confidentiality Requirements
- Breach Notification Requirements
- Responsible Parties and duration of agreement
- Acceptable destruction methods for media in accordance to Data Sanitization
- Information Asset Management requirements
- The State's right to audit compliance with the State's privacy and security requirements

Specific Restricted Data Requirements

Agencies shall ensure the actions required below are successfully completed prior to allowing access or disclosing Restricted Data to a third party or independent contractor.

Specific Restricted Data types have specific regulatory requirements as outlined:

- **Protected Health Information** (PHI)
  - Access to PHI **shall not** be granted until the third party has signed the Business Associate Agreement (BAA).
- **Federal Tax Information** (FTI)
  - Access to FTI **shall not** be granted until the Agency and designated Information Security Officer (ISO) has received written authorization from the IRS Office of Safeguards.
  - Ensure the third party contractual agreement contains verbiage within Safeguarding Federal Tax Information.
    - Any requested modifications to the verbiage within Safeguarding Federal Tax Information requires the review and approval of the assigned ISO and Data Owner.
- **Criminal Justice Information** (CJI)
  - Access to CJI **shall not** be granted until the processes, approvals, and agreements required in FBI's Criminal Justice Information Security Policy (CJIS) (section 5.1) have been successfully completed.
  - Once CJIS requirements are satisfied, an additional approval is required from the State's assigned CJIS ISO, prior to sharing any CJI with a third party.
- **Personally Identifiable Information** (PII)
  - If the third party services requires the sharing of PII, the third party shall sign a contractual agreement that contains specific requirements for the third party to verifiably implement, maintain, and monitor security controls to protect Confidential and Restricted Data from unauthorized access, acquisition, destruction, use, modification, and disclosure prior to access to the PII.

Providing Third Party Access

Remote Access Connections

All remote access connections between the State and third parties shall be secured in accordance with Network Devices and Communications and Access and Identity Management.

Allowing remote access to Restricted Data, or systems containing Restricted Data, to third party resources physically located outside of the U.S. is strictly prohibited.

Least Privileged Access Rights

Third parties shall be granted the minimum access required (least privilege), in accordance with Access and Identity Management. In tailoring the amount of access necessary to fulfill the third party's duties, the Information Security Team (IST) and the Data Owner responsible for the third party shall consider the following types of access:

- Physical access (e.g., physical facilities, filing cabinets, data center facilities)
- Logical access (e.g., to Agency systems and servers)
- Remote access (e.g., VPN)

Data Transfer

Any files containing Confidential or Restricted Data exchanged with a third party shall be encrypted with the recipient's public encryption key prior to secure transmission, in accordance with Encryption and Network Devices and Communications.

Maintenance and Support

VPNs, dial-in modems, systems and accounts used solely for the purpose of third party or vendor maintenance and support must remain disabled or disconnected until required and be disabled again directly after the success completion of the required task.

Third party accounts must be uniquely named to the individual user, or follow check in\out process approved by the IST. Third party accounts shall never be shared, even among the assigned individuals within the third party.

List of Third Parties and Review of Service-Level Agreements

Agencies, assisted by OTS, shall create and maintain a list of all third parties with whom Confidential or Restricted Data is shared.

Agencies shall conduct an audit of service-level agreements (SLAs) at least annually to confirm that third parties have satisfied their contractual requirements.

The State may employ or rely on an independent third party to satisfy such a review or audit.

Landlords

Each lease of office space or facility shall contain an agreement obligating the landlord and its representatives to maintain and respect the confidentiality of Confidential or Restricted Data maintained by the Agency and inspecting, duplicating, or disseminating Confidential or Restricted Data is strictly prohibited.

Agency to Agency Sharing

A Data Sharing Agreement (DSA) is required when Uncategorized, Confidential, or Restricted Data is shared between Agencies. The DSA is a formal agreement which delineates the responsibilities of the involved parties, including the role of the Office of Technology Services (OTS) in providing information technology services and data security on behalf of the executive branch agencies. At a minimum, the following elements shall be included in the agreement:

- Justification – Including the legal, business, or operational need for the data being shared;
- Authority – Identify the law, regulation, or other source authorizing the data share;
- Description – Provide a detailed description of the data, including the appropriate Data Classification level;
- Access or Exchange Method – Describe how the data will be accessed or exchanged;
- Custodians – Designate a Data Custodian for each principal party;
- Authorized User – Identify the individuals or groups authorized to access the data;
- Use – Describe how data will be utilized;
- Retention – Clearly specify any applicable record retention or Data Classification requirements;
- Confidentiality – Statement of any obligations by either party to maintain the appropriate level of confidentiality.

The DSA is acknowledged and made effective by the signatures of the Agency Executive Directors, or designee, of the agreement party agencies. In addition, the Chief Information Officer (CIO) acknowledges the agreement's confidentiality requirements on behalf of OTS.

Information Asset Management

Purpose and Scope

This policy section establishes the requirements for the planning, procurement, deployment, management, support, and handling of an Agency's Information Assets. Information Asset Management assists in confirming that the State's systems and devices are protected according to their Data Classification Level. All Information Assets owned, leased, or managed by an Agency, the Office of Technology Services (OTS), or third party, used to store, transmit, or process an Agency's information shall adhere to the requirements and responsibilities of this policy section.

Inventory Management

Asset Management Personnel

Personnel with Information Asset Management roles and responsibilities are responsible for tracking the Information Asset Lifecycle. These personnel should be documented as such, and trained periodically. These individuals may be from one or many operational areas, as appropriate depending on the type of Information Asset or the Agency's operational needs.

For example, the management of software and hardware assets may be handled by OTS, and the management of Employee assets may be handled by the Office of State Human Capital Management (OSHCM) or the Agency.

Asset Identification and Handling

All Agency Information Assets, owned or leased, shall be inventoried by their Data Classification Level, Data Owner, and assigned user. The inventory of all Information Assets shall be retained by the Agency or OTS on the Agency's behalf. The inventory shall be accurately maintained and reviewed annually to identify any missing or no longer utilized Information Assets. Agencies shall confirm, to the extent possible, that Information Assets are tagged with an approved identification tag and a unique number for tracking purposes.

System Identification for Business Continuity Management

In the event of a disaster, the inventory maintained by an Agency shall be utilized to identify all Information Assets, the last location, back-up information, licensing information, and Information Asset's value to support any operational impact analysis.

Third Party Contractual Agreements

When required, notice of Information Asset Management requirements are to be included in third party contracts. The agreement shall specify how and when the applicable Information Assets will be inventoried and include how Information Assets will be returned upon completion of the contract.

Information Asset Lifecycle

Planning and Procurement

Personnel with Information Asset management roles and responsibilities shall receive timely notifications of Information Assets changes, updates, or new acquisitions in order to ensure inventories are updated.

Deployment

Information Assets are to be deployed following the policies outlined in this Information Security Policy.

Management and Support

Information Assets are to be labeled, handled, supported, and returned following the policies outlined in this Information Security Policy. To the extent possible, the assigned user's supervisor or the assigned Data Owner shall provide the Office of State Human Capital Management (OSHCM) personnel a list of the Information Assets an Employee retains in his/her possession upon the Employee's departure, dismissal, or change in position. In addition, the user's supervisor and the Data Owner shall assist OSHCM with efforts to recoup information assets from former Employees.

Disposal

All Information Assets shall be disposed of in accordance with Data Sanitization.

Lost or Stolen

Upon becoming aware of a lost or stolen Information Asset, an individual must report the event to the Information Security Team (IST) or OTS End User Support Services, as required by Incident Management.

Data Sanitization

Purpose and Scope

This policy section clearly indicates the responsibilities and actions required to ensure data is properly removed prior to the release or disposal of equipment.

This section applies to any and all electronic media or devices subject to surplus, disposal, transfer, or otherwise permanently leaving the possession of an Agency or its agents.

Electronic media and devices shall be sanitized using approved equipment, techniques, and procedures as required by Data Sanitization Standards and Requirements.

This section does not apply to any device or electronic media seized, confiscated, or requested as evidence to support any administrative, legal, or lawful action.

Responsibilities

Agencies shall:

- Review and ensure compliance with current data or record retention policies and directives prior to taking any approved actions to overwrite or destroy data.
- Establish operational processes to ensure compliance with Data Sanitization Requirements.
- Utilize the assigned data classification level, as required by Data Classification and Handling, to determine the required sanitization method.
- Maintain sanitization log records, as defined in Data Sanitization Standards and Requirements, indefinitely.
- Report any violation of this policy directly to the Information Security Team (IST) immediately as practical.

Appendix Items

General Overview

The Information Security Policy Appendix is structured predominantly to both, improve the usability of the Information Security Policy, and ease the maintenance of updating technical specifications which are expected to change over time.

Appendix Requirements

Item Location

Depending on an Appendix Item's format, operational need, or the sensitivity of the information contained within, an Appendix Item may be stored and maintained in one of the following locations:

- Within the Information Security Policy directly;
- Within the OTS policy library located on the Division of Administration's public facing website; or
- Within the State's internal network utilizing a secure file repository.

The Chief Information Security Officer (CISO) shall ensure that following Appendix sections are updated with accurate file locations or links.

Updates to Items

Updates made to existing an Appendix Item's technical or procedural sections shall be logged and require written approval by the CISO prior to use or reference.

Adding or Removing Items

Adding or removing Appendix Items shall require the same process for Information Security Policy Changes and Amendments.

Request for Exception Form

Exception request forms must be completed by the Data Owner or Agency Leadership and must include the signature of the Agency's Executive Director prior to submission to the Chief Information Security Officer (CISO).

Completed forms are summited to the CISO or IST using the Contact Information provided within the Information Security Policy.

Please feel free to contact the Information Security Team (IST) with any questions or comments you have about the Exception Request process.

The Request for Exception Form is hosted as a separate file within the OTS policy library on the Division of Administration's public website.

End User Agreement

This appendix item will be hosted as a separate file within the OTS policy library on the Division of Administration's public website.

Password Requirements

Purpose

The purpose of this policy is to clearly inform all Agencies and third parties of the currently approved authentication methods in addition to the password policy required for all systems, domains, applications, and technical resources utilized by the State or its Agencies.

In the event technical limitations limit the ability to achieve the requirements within this Appendix section, a Policy Exception must be requested for the system or application in addition to a Risk Acceptance Form approved by the Data Owner and Agency Executive Director.

End User Account Password Requirements

All general end user accounts shall require passwords that meets or exceeds the below configurations, settings, or policies.

Policy Configuration

- Minimum Length - 8 characters
- Full Character Set - (alphanumeric and all special characters)
- Complex - By requiring 2 of the following 3:
    - Numeric character (0-9)
    - Special character (, !@#$%^&*()-_+{[=\|/:;}]<>)
    - Uppercase (A-Z)
- Maximum age - 90 days
- Minimum age - 1 day (24hrs)
    - Passwords set to force reset at next logon do not require the above mentioned minimum age.
- No previous password: 24 passwords
    - Meaning: a new password shall not be the same value of the User's previous 24 passwords

Account Lockout Policy shall be determined by Data Classification Levels

Accounts **with** access to Confidential or Restricted Data shall be:

- Locked or disabled and require administrative unlock upon 3 consecutive, unsuccessful login attempts in a 10-minute time period.

Accounts **without** access to Confidential or Restricted Data shall be:

- Temporarily locked out for 15 minutes upon 6 consecutive, unsuccessful login attempts in a 15-minute time period.

Privileged User Account Password Requirements

User accounts for privileged users shall require the more restrictive password configurations outlined below.

Policy Configuration

- Minimum Length - 15 characters
- Full Character Set - (alphanumeric and all special characters)
- Complex - By requiring 2 of the following 3:
    - Numeric character (0-9)
    - Special character (, !@#$%^&*()-_+{[=\|/:;}]<>)
    - Uppercase (A-Z)
- Maximum age - 90 days
- Minimum age - 1 day (24hrs)
    - Passwords set to force reset at next logon do not require the above mentioned minimum age.
- No previous password: 24 passwords
    - Meaning: new passwords shall not be the same value of the previous 24 passwords

Account Lockout Policy

- Locked or disabled and require administrative unlock upon 3 consecutive, unsuccessful login attempts in a 10-minute time period.

Service Account Password Requirements

Service or System accounts require the explicit password configurations as outlined below.

Policy Configuration

- Minimum Length - 24 characters
- Full Character Set - (alphanumeric and all special characters)
- Complex - Required to use 2 of the 3 following:
    - Numeric character (0-9)
    - Special character (, !@#$%^&*()-_+{[=\|/:;}]<>)
    - Uppercase (A-Z)
- Maximum age - Never Expire

Account Lockout Policy

- Locked or disabled and require administrative unlock upon 3 consecutive, unsuccessful login attempts in a 10-minute time period.

Additional Service Account Requirements

Once Service or System accounts have successfully been used to authenticate a service or application, all reasonable efforts shall be taken to restrict the service accounts from interactive logons.

Single Sign-On (SSO) Requirements

SSO for any system, service, website, portal, or application owned, managed, or utilized by an Agency shall be reviewed by the Information Security Team (IST) in addition to meeting the following requirements.

The following are approved methods and requirements for SSO.

SAML v2.0 Requirements

- Validate Message Confidentiality and Integrity
    - Utilize TLS v1.2 or a digitally signed message with a certified key in compliance with Encryption Requirements.
- Validate Protocol Usage
    - SAML Response Data Element **AuthnRequest (ID, SP)**
    - SAML Response Data Element **Response (ID, SP, IdP, {AA} K -1/IdP)**
    - SAML Response Data Element **AuthAssert (ID, C, IdP, SP)**
    - Always perform schema validation on the XML document
    - Securely validate the digital signature
- Validate Protocol Processing Rules
    - Validate **AuthnRequest** processing rules
    - Validate **Response** processing rules

Kerberos Requirements

- Kerberos is an approved authentication method for use both on and off domain or configured for SSO.
- The IST strongly endorses the use of Kerberos whenever when available.

NTLM Requirements

- NTLM v1 shall only be utilized when NTLMv2 or Kerberos is not available due to technical limitations.
- NTLM v2 is the recommended authentication protocol for domain SSO authentication.

OpenID & OAuth

- Due to the highly decentralized nature and the historically flawed model, both OpenID and OAuth shall not be used for any Agency process or application.

Password and Authentication Token Storage Requirement

All passwords, authentication tokens, certificates, and encryption keys shall be encrypted, in accordance with Encryption Requirements, when stored on any client, server, or when embedded within any application, code, or script.

Multi-Factor Authentication Requirements

Definition

The classic paradigm for authentication systems identifies three factors as the cornerstone of authentication:

- Something you know (for example, a password)
- Something you have (for example, an ID badge or a cryptographic key)
- Something you are (for example, a fingerprint or other biometric data)

Multi-factor authentication refers to the use of more than one of the factors listed above. The strength of authentication systems is largely determined by the number of factors incorporated by the system. Implementations that use two factors are considered to be stronger than those that use only one factor; systems that incorporate all three factors are stronger than systems that only incorporate two of the factors.

Approved Authentication Factors

All Multi-Factor authentication systems shall be subject to a formal review by the Information Security Team (IST). The following types of Multi-Factor authentication types are approved.

- Hardware Tokens
- Software Tokens
- Certificates
    - Must be non-exportable
    - Key must not be subject to memorization

Other Authentication Methods

Device or Application PIN Requirements

- PIN minimum length – 4 digits
- Minimum Age – N/A
- Maximum Age – 90 days

Session Management Requirements

All Session IDs (or Tokens) utilized to maintain the active authenticated state of an application or system user shall expire and reissue after a maximum of:

- 15 minutes

Any inactive authenticated user session of any externally accessible application or system shall be expired and require re-authentication after a maximum inactivity of:

- 15 minutes

Any active authenticated user session of any externally accessible application or system shall be expired and require re-authentication after a maximum active use of:

- 24 hours

Access Request Requirements

This appendix item will be hosted as a separate file within the OTS policy library on the Division of Administration's public website.

Change Management Process

The Information Security Team is currently working with each operational section of the Office of Technology Services (OTS) and Agencies to create and document a Change Management Process which can accommodate the State's consolidating IT environments.

Each operational section of OTS and Agency shall continue to utilize their currently documented Change Management Process in compliance with Change Management.

Once finalized, the CISO will include the new Change Management Process to this appendix item and will be hosted as a separate file within the OTS policy library on the Division of Administration's public website.

Request for Change Form

The Information Security Team is currently working with each operational section of the Office of Technology Services (OTS) to create and document a Change Management Process which can accommodate the State's consolidating IT environments.

Each operational section of OTS and Agency shall continue to utilize their currently documented Change Management Process in compliance with Change Management.

Once finalized, the CISO will include the new Request for Change Form to this appendix item and will be hosted as a separate file within the OTS policy library on the Division of Administration's public website.

Approved Network Services, Protocols, and Ports

The Office of Technology Services – Network Services, working with the Information Security Team (IST), shall create and maintain a list of approved network services, protocols, and ports that are maintained and operationally required by an Agency.

The list of approved network services, protocols, and ports shall be updated with any newly provisioned services, protocols, and ports. Once approved and changed per the Network Devices and Communications in accordance with Change Management.

The list of approved network services, protocols, and ports is to be reviewed on an annual basis to verify that insecure, unused or unauthorized services, protocols, and ports are not present in the State's environment.

Due to the potential risk associated and confidential nature of this content, access to this list shall be restricted and the list shall not be published or shared without prior approval from the CIO and CISO.

System Configuration Process

The Information Security Team is currently working with each operational section of the Office of Technology Services (OTS) to create and document a System Configuration Process which can accommodate the State's consolidating IT environments.

Each operational section of OTS and Agency shall continue to utilize their currently documented System Configuration Process in compliance with System Configuration.

Once finalized, the CISO will include the new System Configuration Process to this appendix item and will be hosted as a separate file within the OTS policy library on the Division of Administration's public website.

System Configuration Records

Configurations for all computing systems in production or intended for production use, whether managed by OTS, Agency, or third party, must be documented in accordance with these guidelines.

Purpose

Proper recording of system, application and network configuration components is required to maintain and up-to-date record of current configuration status information. An accurate configuration record will provide management with information including what and when changes have been made to a specific system. Such information can be useful for the system and network troubleshooting process and aid in the development of disaster recovery procedures.

All applicable configuration information shall be created and maintained or optionally entered into (or captured by) an approved configuration tracking system or service.

Record Requirements

The following list contains the configuration information where applicable to be recorded for each system:

- System Name – Name of the system based on the pre-determined naming convention
- Assigned Agency – Name of Agency being assigned
- Data Owner – if server, application, or database
- System Purpose – Why is this system being configured or re-configured
- Data Classification – if server hosting data or database
- Build Date – Date the engineer configured the system
- Build Engineer – Name of the engineer performing the system configuration
- Approved by – Who authorized or approved this build, if authorization was not pre-approved.
- IP address – If system will require a static IP address, the IP address of the system be configured
- Subnet Mask – If system required a static IP address, the subnet mask assigned to the system
- Default Gateway – If system will require a static IP address, the Default IP gateway assigned to the system
- Domain – the domain name assigned to the System.
- VLAN – is this system required to be on a special VLAN?
- DMZ – DMZ details, if applicable
- Operating System (OS) – Type of Operation System or firmware presently running on the system
- OS Version – The version of the operating system or firmware on the system
- Secure System Baseline applied? – Was the most current applicable secure baseline applied?
- Applications – any line-of-business applications that have been installed on the system.
- Version – the version number of all applicable line-of-business applications
- Date patched to – the date of the most recent patch update for applicable line-of-business applications.
- Patch Exceptions - any patches that may be applicable but were not installed and for what reason
- System/application Information Security requirements – did the system or application require any additional security configuration or hardened?
- Secure Exceptions – any applicable secure baseline configuration or setting that were not applied and for what reason
- Other Settings – any additional setting that are unique to the system.
- Comments – any additional information that may apply to the system or application not previously mentioned in the above fields.

Vulnerability Management Process

The Information Security Team is currently working with each operational section of the Office of Technology Services (OTS) to create and document a Vulnerability Management Process which accommodates the State's consolidating IT environments.

Each operational section of OTS and Agency shall continue to utilize their currently documented Change Management Process in compliance with Vulnerability Management.

Once finalized, the CISO will include the new Change Management Process to this appendix item and will be hosted as a separate file within the OTS policy library on the Division of Administration's public website.

Approved End User Facing Technologies

The Office of Technology Services – End User Computing, working with the Information Security Team (IST), shall create and maintain a list of Approved End User Facing Devices and Technologies that are maintained and operationally required by an Agency.

The list of Approved End User Facing Devices and Technologies shall be updated with any newly provisioned end user facing devices or technology, once approved and configured in compliance with the Information Security Policy.

The list of Approved End User Facing Devices and Technologies is to be reviewed on a bi-annual basis to verify that insecure, unused, or unauthorized devices or technologies are not present in the State's environment.

Due to the potential risks associated this content, this list will be maintained securely within the State's internal network (or system) in a manner that best suites the operational needs of the End User Computing section of OTS.

Encryption Requirements

Purpose

The purpose of this policy is to clearly inform an Agency or third party of authorized cryptographic algorithms, methods, configurations, and secure protocols necessary for adequate data protection. The requirements in this Information Security Policy Appendix section shall be referenced when data encryption methods are required for Agency systems, applications, workstations, mobile devices, file transfers, network connections, or digital signatures.

In the event technical or operational limitations impact the ability to achieve the requirements within this Appendix section, a Policy Exception must be requested for the system or application in addition to a Risk Acceptance Form approved by the Data Owner and Agency Executive Director.

Encryption Software

Encryption standards and algorithms require intensive analysis prior to approval in addition to continued examination in order to determine that the standard or algorithm provides adequate security. For this reason, the Information Security Team (IST) relies upon the National Institute of Standards and Technologies (NIST) for maintaining the currently approved encryption standards, algorithms, and corresponding key lengths.

Prior to production use of any software product or application (including any cryptographic library or module utilized during software development) used for data encryption, must have previously been submitted, tested, approved, and posted by NIST as a FIPS 140-2 compliant cryptographic module.

In addition to using a FIPS 140-2 compliant cryptographic module, all encryption software used in production environments shall adhere to the additional requirements within this Appendix section.

Please contact the IST with any questions about the requirements, use, or approval of encryption software.

Encryption Algorithms

Only currently approved encryption algorithms shall be used to provide confidentiality or protection for Confidential or Restricted Data.

Symmetric Key Algorithms

As provided in NIST sp800-57, the following symmetric key algorithms are approved:

- Triple DEA (TDEA)
    - 56-bit keys **only** (**not** preferred)
- Advanced Encryption Standard (AES)
    - 128-bit keys, (**not** preferred)
    - 192-bit keys, or (**not** preferred)
    - 256-bit keys. (**strongly preferred**)

Public Key Asymmetric Algorithms

As compliant with FIPS 140-2, the following asymmetric key algorithms are approved:

- RSA (1024 bit minimum)
- ECC (384 bit minimum)

Hash Functions

A hash function is used to take an input of arbitrary length and output a fixed-length value. The output from a hash function may be commonly referred to as a hash value, hash, message digest, and digital fingerprint. Using a well-designed hash function means it is not feasible to find a message that will produce a given hash value (pre-image resistance), nor is it feasible to find two messages that produce the same hash value (collision resistance).

As provided in FIPS 180, the following hash functions are approved:

- SHA-1,
- SHA-224,
- SHA-512/224,
- SHA-256,
- SHA-512/256,
- SHA-384, and
- SHA-512

Digital Signature Algorithms

Digital signature algorithms are used with hash functions to provide authentication, integrity, and non-repudiation.

As provided in FIPS 186, the following digital signature algorithms are approved:

- RSA (1024 bit minimum) with SHA-256
- DSA (1024 bit minimum) with SHA-256
- ECDSA (384 bit minimum) with SHA-256

Key Exchange

Key exchanges must use one of the following cryptographic protocols:

- Diffie-Hellman
- IKE
- Elliptic curve Diffie-Hellman (ECDH)

End points must be authenticated prior to the exchange or derivation of session keys.

Certificates and Key Authentication

All systems used for authentication (for example, RADIUS or TACACS) must have installed a valid certificate issued and signed by either the Agency's internal certificate authority (CA) or a publically trusted CA (provider).

Any system or applications using TLS must have a certificates signed by the Agency's internal certificate authority (CA), or a publically trusted CA.

Public keys used to establish trust must be authenticated prior to use. Examples of authentication include transmission via cryptographically signed message or manual verification of the public key hash.

Certificates issued to users, workstations, or servers for the purpose of authentication must not allow the certificate to be exported.

Encryption for End User Devices

Approved encryption software used to protect Confidential and Restricted Data on laptops, mobile devices, smart phones, workstations, and other end users devices that could potentially become lost or stolen shall be implemented in strict compliance with NIST sp800-111.

Encrypted Network Transmissions

Confidential and Restricted Data must be encrypted during transmission over the internet, public network, or otherwise un-trusted environment.

Restricted Data shall be encrypted even during transmission within an internal State, Agency, or authorized third party network; unless otherwise approved by the IST.

Agencies with an operational need for transmitting Confidential and Restricted Data shall only use the following approved protocols:

- TLS v1.2 (Transport Layer Security)
- IPsec (Internet Protocol Security)
    - IPsec requires the explicit use of Encapsulating Security Payload (ESP), the following are approved transform sets:
        - ESP-AES-256-MD5 esp-aes-256 esp-md5-hmac
        - ESP-AES-192-MD5 esp-aes-192 esp-md5-hmac
        - ESP-AES-128-SHA esp-aes esp-sha-hmac
        - ESP-AES-192-SHA esp-aes-192 esp-sha-hmac
        - ESP-AES-128-MD5 esp-aes esp-md5-hmac
        - ESP-AES-256-SHA esp-aes-256 esp-sha-hmac

Encrypted Wireless Networks

All wireless networks in use within State facilities must be protected by encryption. Under no circumstances should the encryption be configured to be less than 256 bits in strength.

- Wireless networks used by Employees or Third Parties to access to internal systems shall be configured to specifically use Protected Extensible Authentication Protocol over TLS v1.2 (PEAP-TLS).
- Wireless networks used by Employees or Third Parties with no access to any internal systems must be configured with WPA2 using AES with a Pre-Shared Key (PSK) of no less than 24 characters.
- Wireless networks, used by guests, visitors, or general public must strictly prohibit the access of any internal system and requires users to complete registration process prior to providing connectivity.
    - In instances where guest or general public wireless access is needed to support an event scheduled for less than 48hrs, user registration is not required unless requested by the Agency assigned event coordinator.

Restricted Data File Transfers

File transfers to third parties that contain or may contain Restricted Data, shall be encryption at file level (at rest) prior to being sent over an encrypted.

Continuous Review of Encryption Standards

Due to the inherent depreciation of encryption standards, as well as the on-going focus to improve encryption technologies, the Information Security Team (IST), in conjunction with OTS operational sections, shall continuously review the acceptable encryption guidelines and requirements to ensure the State's use of encryption maintain compliance with regulatory requirements and Restricted Data is adequately protected.

Incident Response Plan

This appendix item will be hosted as a separate file within the OTS policy library on the Division of Administration's public website.

Risk Assessment Standards and Requirements

The Chief Information Security Officer (CISO) is currently working with each operational section of the Office of Technology Services (OTS) and Agencies to finalize the Risk Assessment Standards and Requirements which accommodates the State's consolidating IT environments.

Once finalized, the CISO will communicate and publish the Risk Assessment Standards and Requirements to this appendix item and host as a separate file within the OTS policy library on the Division of Administration's public website.

Third Party Information Security Questionnaire

The Third Party Information Security Questionnaire appendix item will be hosted as a separate file within the OTS policy library on the Division of Administration's public website.

Risk Acceptance Form

A Risk Acceptance Form is primarily initiated by the Chief Information Security Officer (CISO) and submitted to the Agency or operational area for acknowledgement and acceptance. However, any individual who believes a Risk Acceptance Form should be initiated due to a recent increase in risk, may contact the CISO or Information Security Team (IST) using the Contact Information provided within the Information Security Policy.

Note: The CISO shall report all Risk Acceptance Forms, pending or accepted, directly to the Information Security Governance Board (ISGB), as required by the State's Information Security Program.

The Risk Acceptance Form is hosted as a separate file within the OTS policy library on the Division of Administration's public website.

Audit Logging Standards and Requirements

Purpose

The purpose of this policy is to clearly inform all Agencies, third parties, and operational sections within the Office of Technology Services (OTS) of the audit logging requirements for all computing systems, network devices, servers, applications, and databases in production or intended for production use, whether managed by an Agency, OTS, or third party.

General Logging Requirements

Any log generated by a system, application, database, etc. should be configured to produce unfiltered logs in as much detail as possible.

The following fields of information are required for all audit logs or system events:

- Timestamp
- Date
- Username (if applicable)
- Action Result
    - Success
    - Failure
- Source - Client Information
    - Hostname (if applicable)
    - IP Address
    - MAC Address
    - Port
- Destination - Client Information
    - Hostname (if applicable)
    - IP Address
    - MAC Address
    - Port
- Protocol
- Reason Code or Event Type
- Message Details

Operating System and Network Device Logging Requirements

In addition to the previously listed General Logging Requirements, Operating Systems shall be configured to produce audit logs for the following event types:

- Log Clearing or Deletion
- Actions performed by OS components
    - Startups and Shutdowns
    - Service starts, stops, creation, deletion
    - System Changes
    - Script or Command execution details
    - Errors (with error codes)
- Account Information
    - Authentication and Authorizations
        - Logons
        - Logoffs
        - Password resets or changes
    - Account Changes
    - Account Creation
- Policy Changes
- Account Changes
- Account Creation
- Permission Changes
- When required by Information Security Team File Access\Auditing for:
    - Update\Write
    - Read
    - Delete
    - Traverse

Application Logging Requirements

In addition to the both General Logging Requirements and Operating System Requirements, Applications shall be capable of generating and configured to produce the following event types (as relevant to the use, functionality, or scope of the application):

- Log Clearing, Deletion, or Purging
- Client Requests and Server Response
    - URLs
    - Status Code

- User Account Information
    - Authentication and Authorizations
        - Logons
        - Logoffs
        - Password resets or changes
    - Account Changes
    - Account Creation
- Operational
    - Service level Starts and Stops
    - Application Failures
    - Policy or Configuration Changes
    - Content Updates
    - Critical Errors
    - File or Message Transfer
- End User Actions
    - Access to any screen or menu containing Confidential or Restricted Data
    - Initiated Reports (to include query executed) containing Confidential or Restricted Data

Database Logging Requirements

In addition to the General Logging Requirements, Operating System Requirements, and Applications Logging, Databases shall be capable and configured to produce the following event types:

- Account Information
    - Authentication and Authorizations
        - Logons
        - Logoffs
        - Password resets or changes
    - Account Changes
    - Account Creation
- Operational Actions
    - Startup and Shutdown
    - Configuration Changes
    - Errors
    - Log Cleared
- Transactions (to include query string)
    - User generated

- Stored procedures or Scripts
- Scheduled Jobs or Tasks

Custom Application Logging Requirements

In addition to the General Logging Requirements, Operating System Requirements, and Applications Logging, and Databases Logging Requirements, Custom Application shall be required to be developed and tested to ensure creation of the following event types:

- Client Requests and Server Response
  - URLs
  - Status Code
- Account Information
  - Authentication and Authorizations
    - Logons
    - Logoffs
    - Password resets or changes
  - Account Changes
  - Account Creation
- Operational Actions
  - Startup and Shutdown
  - Application Failures
  - Configuration Changes
  - Updates
  - Errors
  - Log Cleared
- End User Actions
  - Access to any screen or menu containing Confidential or Restricted Data
  - Initiated Reports (to include query executed) containing Confidential or Restricted Data
  - File uploads
  - Searches (including strings)

Additional Requirements

Syslog Protocol Requirements

- Reliable Log Delivery
  - TCP Support
- Transmission Confidentiality Protection
  - TLS Support
- Transmission Integrity Protection and Authentication
  - Supports MD5 or SHA-1

Log Collection and Event Forwarding

- Security tools may be required to connect to log storage locations, including data bases, or flat file storage locations for log collection and processing.
  - In some situations, security tools may delete original log files / entries after collection and processing are complete.
- When required by the CISO, Agency, or Data Owner, Event Logs shall be forward to a central location for secure storage and monitoring.

Data Sanitization Standards and Requirements

The Office of Technology Services' previously approved and published Data Sanitization Standards and Requirements shall continue to be used and temporarily serve as this appendix item.

The Chief Information Security Officer (CISO) will update the OTS Data Sanitization Standards and Requirements and formatting as an official Information Security Appendix Item within 90 days and host in the OTS policy library on the Division of Administration's public website.

Safeguarding Federal Tax Information

Purpose

This document clearly outlines the contract language required in a Third Party Agreement prior to sharing Federal Tax Information (FTI).

The details must be directly included, without modification, in any Third Party Agreement prior to an Agency sharing Federal Tax Information.

Safeguarding Contract Language

CONTRACT LANGUAGE FOR GENERAL SERVICES

I. PERFORMANCE

In performance of this contract, the Contractor agrees to comply with and assume responsibility for compliance by his or her employees with the following requirements:

(1) All work will be performed under the supervision of the contractor or the contractor's responsible employees.

(2) Any Federal tax returns or return information (hereafter referred to as returns or return information) made available shall be used only for the purpose of carrying out the provisions of this contract. Information contained in such material shall be treated as confidential and shall not be divulged or made known in any manner to any person except as may be necessary in the performance of this contract. Inspection by or disclosure to anyone other than an officer or employee of the contractor is prohibited.

(3) All returns and return information will be accounted for upon receipt and properly stored before, during, and after processing. In addition, all related output and products will be given the same level of protection as required for the source material.

(4) No work involving returns and return information furnished under this contract will be subcontracted without prior written approval of the IRS.

(5) The contractor will maintain a list of employees authorized access. Such list will be provided to the agency and, upon request, to the IRS reviewing office.

(6) The agency will have the right to void the contract if the contractor fails to provide the safeguards described above.

(7) (Include any additional safeguards that may be appropriate.)

II. CRIMINAL/CIVIL SANCTIONS

(1) Each officer or employee of any person to whom returns or return information is or may be disclosed shall be notified in writing by such person that returns or return information disclosed to such officer or employee can be used only for a purpose and to the extent authorized herein, and that further disclosure of any such returns or return information for a purpose or to an extent unauthorized herein constitutes a felony punishable upon conviction by a fine of as much as $5,000 or imprisonment for as long as five years, or both, together with the costs of prosecution. Such person shall also notify each such officer and employee that any such unauthorized future disclosure of returns or return information may also result in an award of civil damages against the officer or employee in an amount not less than $1,000 with respect to each instance of unauthorized disclosure. These penalties are prescribed by IRCs 7213 and 7431 and set forth at 26 CFR 301.6103(n)-1.

(2) Each officer or employee of any person to whom returns or return information is or may be disclosed shall be notified in writing by such person that any return or return information made available in any format shall be used only for the purpose of carrying out the provisions of this contract. Information contained in such material shall be treated as confidential and shall not be divulged or made known in any manner to any person except as may be necessary in the performance of this contract. Inspection by or disclosure to anyone without an official need-to-know constitutes a criminal misdemeanor punishable upon conviction by a fine of as much as $1,000.00 or imprisonment for as long as 1 year, or both, together with the costs of prosecution. Such person shall also notify each such officer and employee that any such unauthorized inspection or disclosure of returns or return information may also result in an award of civil damages against the officer or employee [United States for Federal employees] in an amount equal to the sum of the greater of $1,000.00 for each act of unauthorized inspection or disclosure with respect to which such defendant is found liable or the sum of the actual damages sustained by the plaintiff as a result of such unauthorized inspection or disclosure plus in the case of a willful inspection or disclosure which is the result of gross negligence, punitive damages, plus the costs of the action. The penalties are prescribed by IRCs 7213A and 7431.

(3) Additionally, it is incumbent upon the contractor to inform its officers and employees of the penalties for improper disclosure imposed by the Privacy Act of 1974, 5 U.S.C. 552a. Specifically, 5 U.S.C. 552a(i)(1), which is made applicable to contractors by 5 U.S.C. 552a(m)(1), provides that any officer or employee of a contractor, who by virtue of his/her employment or official position, has possession of or access to agency records which contain individually identifiable information, the disclosure of which is prohibited by the Privacy Act or regulations established thereunder, and who knowing that disclosure of the specific material is so prohibited, willfully discloses the material in any manner to any person or agency not entitled to receive it, shall be guilty of a misdemeanor and fined not more than $5,000.

(4) Granting a contractor access to FTI must be preceded by certifying that each individual understands the agency's security policy and procedures for safeguarding IRS information. Contractors must maintain their authorization to access FTI through annual recertification. The initial certification and recertification must be documented and placed in the agency's files for review. As part of the certification and at least annually afterwards, contractors must be advised of the provisions of IRCs 7431, 7213, and 7213A (see Exhibit 4, Sanctions for Unauthorized Disclosure, and Exhibit 5, Civil Damages for Unauthorized Disclosure). The training provided before the initial certification and annually thereafter must also cover the incident response policy and procedure for reporting unauthorized disclosures and data breaches. (See Section) For both the initial certification and the annual certification, the contractor must sign, either with ink or electronic signature, a confidentiality statement certifying their understanding of the security requirements.

III. INSPECTION

The IRS and the Agency shall have the right to send its officers and employees into the offices and plants of the contractor for inspection of the facilities and operations provided for the performance of any work under this contract. On the basis of such inspection, specific measures may be required in cases where the contractor is found to be noncompliant with contract safeguards.

CONTRACT LANGUAGE FOR TECHNOLOGY SERVICES

I. PERFORMANCE

In performance of this contract, the contractor agrees to comply with and assume responsibility for compliance by his or her employees with the following requirements:

(1) All work will be done under the supervision of the contractor or the contractor's employees.

(2) Any return or return information made available in any format shall be used only for the purpose of carrying out the provisions of this contract. Information contained in such material will be treated as confidential and will not be divulged or made known in any manner to any person except as may be necessary in the performance of this contract. Disclosure to anyone other than an officer or employee of the contractor will be prohibited.

(3) All returns and return information will be accounted for upon receipt and properly stored before, during, and after processing. In addition, all related output will be given the same level of protection as required for the source material.

(4) The contractor certifies that the data processed during the performance of this contract will be completely purged from all data storage components of his or her computer facility, and no output will be retained by the contractor at the time the work is completed. If immediate purging of all data storage components is not possible, the contractor certifies that any IRS data remaining in any storage component will be safeguarded to prevent unauthorized disclosures.

(5) Any spoilage or any intermediate hard copy printout that may result during the processing of IRS data will be given to the agency or his or her designee. When this is not possible, the contractor will be responsible for the destruction of the spoilage or any intermediate hard copy printouts, and will provide the agency or his or her designee with a statement containing the date of destruction, description of material destroyed, and the method used.

(6) All computer systems receiving, processing, storing or transmitting FTI must meet the requirements defined in IRS Publication 1075. To meet functional and assurance requirements, the security features of the environment must provide for the managerial, operational, and technical controls. All security features must be available and activated to protect against unauthorized use of and access to Federal Tax Information.

(7) No work involving Federal Tax Information furnished under this contract will be subcontracted without prior written approval of the IRS.

(8) The contractor will maintain a list of employees authorized access. Such list will be provided to the agency and, upon request, to the IRS reviewing office.

(9) The agency will have the right to void the contract if the contractor fails to provide the safeguards described above.

(10) (Include any additional safeguards that may be appropriate.)

II. CRIMINAL/CIVIL SANCTIONS

(1) Each officer or employee of any person to whom returns or return information is or may be disclosed will be notified in writing by such person that returns or return information disclosed to such officer or employee can be used only for a purpose and to the extent authorized herein, and that further disclosure of any such returns or return information for a purpose or to an extent unauthorized herein constitutes a felony punishable upon conviction by a fine of as much as $5,000 or imprisonment for as long as 5 years, or both, together with the costs of prosecution. Such person shall also notify each such officer and employee that any such unauthorized further disclosure of returns or return information may also result in an award of civil damages against the officer or employee in an amount not less than $1,000 with respect to each instance of unauthorized disclosure. These penalties are prescribed by IRCs 7213 and 7431 and set forth at 26 CFR 301.6103(n)-1.

(2) Each officer or employee of any person to whom returns or return information is or may be disclosed shall be notified in writing by such person that any return or return information made available in any format shall be used only for the purpose of carrying out the provisions of this contract. Information contained in such material shall be treated as confidential and shall not be divulged or made known in any manner to any person except as may be necessary in the performance of the contract. Inspection by or disclosure to anyone without an official need-to-know constitutes a criminal misdemeanor punishable upon conviction by a fine of as much as $1,000 or imprisonment for as long as 1 year, or both, together with the costs of prosecution. Such person shall also notify each such officer and employee that any such unauthorized inspection or disclosure of returns or return information may also result in an award of civil damages against the officer or employee [United States for Federal employees] in an amount equal to the sum of the greater of $1,000 for each act of unauthorized inspection or disclosure with respect to which such defendant is found liable or the sum of the actual damages sustained by the plaintiff as a result of such unauthorized inspection or disclosure plus in the case of a willful inspection or disclosure which is the result of gross negligence, punitive damages, plus the costs of the action. These penalties are prescribed by IRC 7213A and 7431.

(3) Additionally, it is incumbent upon the contractor to inform its officers and employees of the penalties for improper disclosure imposed by the Privacy Act of 1974, 5 U.S.C. 552a. Specifically, 5 U.S.C. 552a(i)(1), which is made applicable to contractors by 5 U.S.C. 552a(m)(1), provides that any officer or employee of a contractor, who by virtue of his/her employment or official position, has possession of or access to agency records which contain individually identifiable information, the disclosure of which is prohibited by the Privacy Act or regulations established thereunder, and who knowing that disclosure of the specific material is prohibited, willfully discloses the material in any manner to any person or agency not entitled to receive it, shall be guilty of a misdemeanor and fined not more than $5,000.

(4) Granting a contractor access to FTI must be preceded by certifying that each individual understands the agency's security policy and procedures for safeguarding IRS information. Contractors must maintain their authorization to access FTI through annual recertification. The initial certification and recertification must be documented and placed in the agency's files for review. As part of the certification and at least annually afterwards, contractors must be advised of the provisions of IRCs 7431, 7213, and 7213A (see Exhibit 4, Sanctions for Unauthorized Disclosure, and Exhibit 5, Civil Damages for Unauthorized Disclosure). The training provided before the initial certification and annually thereafter must also cover the incident response policy and procedure for reporting unauthorized disclosures and data breaches. (See Section 10) For both the initial certification and the annual certification, the contractor must sign, either with ink or electronic signature, a confidentiality statement certifying their understanding of the security requirements.

III. INSPECTION

The IRS and the Agency shall have the right to send its officers and employees into the offices and plants of the contractor for inspection of the facilities and operations provided for the performance of any work under this contract. On the basis of such inspection, specific measures may be required in cases where the contractor is found to be noncompliant with contract safeguards.

Chain of Custody

The Chain of Custody appendix item will be hosted as a separate file within the OTS policy library on the Division of Administration's public website.