

OFFICE OF THE STATE AUDITOR
INFORMATION SECURITY
POLICIES AND PROCEDURES

I ACKNOWLEDGE RECEIPT OF THE AGENCY INFORMATION SECURITY
POLICY AND PROCEDURE'S MANUAL VIA THE OFFICE OF THE STATE AUDITOR
INTRANET.

Signature

Printed name

Date

CHAPTER I - ACCESS CONTROL

Reference

Section

A - Access Management	I-A
B - Network Access Management	I-B
C - Identity Management	I-C
D - Authentication	I-D
E - Emergency Access	I-E
F - Password Policy	I-F
G - Password Administration	I-G

CHAPTER II - ASSET MANAGEMENT

Section

A – Asset Identification	II-A
--------------------------	------

CHAPTER III - BUSINESS CONTINUITY MANAGERMENTS

Section

A – Contingency Planning	III-A
B – Disaster Recovery and Contingency Strategies	III-B
C – Data Backups	III-C

CHAPTER IV - DATA PROTECTION AND PRIVACY

Section

A – Data Classification	IV-A
B – Data Proposal	IV-B
C – Data Protection	IV-C
D – Privacy	IV-D

CHAPTER V - HUMAN RESOURCE (HR) AND SECURITY AWARENESS

Section

A – Human Resource Compliance	V-A
B – Security Awareness Training	V-B

STATE AUDITOR'S OFFICE INFORMATION SECURITY POLICY

Issued Date: 6/22/16

CHAPTER VI - IT COMPLIANCE

Reference

Section

A – Audit and Compliance Requirements	VI-A
B – Information System Audit Considerations	VI-B
C – Information Security Continuous Monitoring	VI-C

CHAPTER VII - IT RISK STRATEGY

Section

A – Security Performance and Metrics	VII-A
B – Third Party Risk Management	VII-B

CHAPTER VIII - INFORMATION SYSTEMS ACQUISITIONS, DEVELOPMENT, AND MAINTENANCE

Section

A – Change Management	VIII-A
B – Configuration Management	VIII-B
C – System Development and Maintenance	VIII-C
D – Release Management	VIII-D

CHAPTER IX – GOVERNANCE

Section

A – Information Security Program Planning	IX-A
B – Security Organization (Roles and Responsibilities)	IX-B
C – Policy Management (Plan of Action)	IX-C
D – Information Security Controls Deployment	IX-D

CHAPTER X - MOBILE SECURITY

Section

A – Mobile Security	X-A
B – Portable Computing Devices	X-B

CHAPTER XI - PHYSICAL & ENVIRONMENTAL SECURITY

Section	<u>Reference</u>
A – Physical Access and Security	XI-A
B – Environmental Security	XI-B
C – Disposal of Equipment	XI-C

CHAPTER XII- RISK MANAGEMENT

Section	
A – Risk Management	XII-A
B – Risk Mitigation	XII-B

CHAPTER XIII - THREAT AND VULNERABILITY MANAGEMENT

Section	
A – Vulnerability Assessment	XIII-A
B – Incident Management	XIII-B
C – Patch Management	XIII-C

OFFICE OF THE STATE AUDITOR INFORMATION SECURITY POLICY

I. ACCESS CONTROL

A. Access Management

Purpose:

The purpose of the Access Management section is to establish processes to control access and use of the Office of the State Auditor (OSA) information resources. Access management incorporates role based access controls (RBAC), privileged user access, access definitions, roles, and profiles.

Policy:

1. Access Control Policy and Procedures

- The OSA maintains written procedures to facilitate the implementation of the Access Control Policy and associated Access Controls.

2. Account Management

- The OSA primarily uses individual accounts.
- The OSA identifies authorized users of information systems and specifies access rights.
- The OSA approves access requests prior to provisioning user accounts.
- The OSA removes or disables default user accounts and, if user accounts cannot be removed or disabled, they are renamed.
- Access is granted based upon the principles of need-to-know, least-privilege, and separation of duties. Access not explicitly permitted is denied by default.
- The OSA approves requests by staff auditors to access SCEIS statewide agency information for the purpose of performing agency audits.

Procedure:

The Administration Department contracts with the Department of Technology Operations (DTO) to provide new employee account access to the OSA information systems.

The Administration Department notifies DTO via Help Desk to add a new user and defines the access rights.

I. ACCESS CONTROL (CONTINUED)

Procedure (Continued):

The Administration Department notifies DTO via Help Desk to remove or deactivate access rights when users are terminated, transferred, or access rights requirements change.

The Administration Department maintains a record of users, and their access rights. The record of users is reconciled with the monthly statement from DTO.

The Administration Department approves access rights for users before requesting DTO to implement the access rights.

The Administration Department notifies DTO via Help Desk to activate or deactivate access rights for staff auditors to SCEIS Statewide agency information.

- Privileged accounts (e.g., system / network administrators having root level access, database administrators) are only allowed upon approval by the State Auditor or his delegate. The approval is only granted to a limited number of individuals with the requisite skill, experience, business need, and documented reason based on role requirements.
- Privileged accounts are controlled, monitored, and reported on a periodic basis.

Procedure:

Upon approval by the State Auditor, the Administration Department notifies DTO via Help Desk to add a privileged user.

The Administration Department monitors privileged accounts and reports the status to the State Auditor at least every 180 days.

- Information data owners conduct periodic reviews to ensure the following:
 - Access levels remain appropriate, based upon approvals;
 - Terminated employees do not have active accounts; and
 - There are no duplicate user identifiers.

Procedure:

The Administration Department in consultation with information data owners reviews information system accounts at least every one-hundred eighty (180) days and documents the results.

The Administration Department reconciles list of users with the monthly statement from DTO.

- The OSA approves requests access from CPA firms to access SCEIS to perform the OSA agency annual audit, the Comprehensive Annual Financial Report, and the Statewide Single Audit.

I. ACCESS CONTROL (CONTINUED)

3. Access Enforcement

- The OSA allows only authorized users to access information systems.
- The OSA uses encryption as an access control mechanism as required by Federal, State or other laws or regulations.

Procedure:

The Administration Department contracts with DTO to encrypt notebook computers that contain OSA information.

The Administration Department contracts with DTO to restrict access to OSA information systems to users authorized by OSA.

The Administration Department notifies DTO via Help Desk to activate or deactivate access rights to CPA firms to SCEIS agency information for a specified period of time.

4. Information Flow Enforcement

- For Restricted data, the OSA uses security attributes on information source and destination objects as a basis for flow control.

Procedure:

The Administration Department contracts with DTO to establish file structure and privileges to control access to restricted data.

5. Separation of Duties

- The OSA maintains “separation of duties” through assigned access authorizations, including but not limited to:
 - Audit functions are not performed by security personnel responsible for administering information system access;
 - Division of critical business and information system management responsibilities;
 - Division of information system testing and production functions between different individuals or groups; and
 - Using an independent entity to conduct information security testing of information systems.

Procedure:

The Administration Department is responsible for and approves all information system functions and contracts with independent entities for auditing and testing of the information systems.

I. ACCESS CONTROL (CONTINUED)

6. Least Privilege

The OSA ensures that only authorized individuals have access to the OSA data / information and that such access is strictly controlled, audited in accordance with the concepts of “need-to-know, least-privilege, and separation of duties”.

Procedure:

The Administration Department contracts with DTO to:

- ***Disable file system access not explicitly required for system, application, and administrator responsibilities;***
- ***Provide minimal physical and system access to the contractors and ensure information security policy adherence by all contractors;***
- ***Restrict use of database management to authorized database administrators;***
- ***Grant access to authorized users approved by the Administration Department based on their required job duties; and***
- ***Disable all system and removable media boot access unless explicitly authorized by the CIO; if authorized, boot access shall be password protected.***

7. Unsuccessful Login Attempts

- The OSA limits unsuccessful logon attempts during a pre-defined time period.

Procedure:

The Administration Department contracts with DTO to limit the number of unsuccessful logon attempts within an established time period.

The Administration Department contracts with DTO to automatically lock user accounts after the maximum number of logon attempts is reached. The Administration Department establishes an account lock time period commensurate with the classification of data hosted, processed or transferred by the information system.

I. ACCESS CONTROL (CONTINUED)

8. System Use Notification

- The OSA displays a warning on computer displays before granting system access.
- The OSA implements warning banners that comply with Federal, State or other laws of regulations associated with the type of data handled by the OSA.

Procedure:

The Administration Department contracts with DTO to display warning banners that comply with Federal, State or other laws of regulations. DTO provides the following or similar warning before granting access to the information system:

“This computer system is the property of South Carolina State Government and may be accessed only by authorized users. Unauthorized use of this system is strictly prohibited and may be subject to criminal prosecution. This computer may be monitored for any activity or communication on the system and any information stored within the system may be retrieved. By accessing and using this computer, you are consenting to such monitoring and information retrieval for law enforcement and other purposes. Users should have no expectation of privacy as to any communication on or information stored within the system, including information stored locally on the hard drive or other media in use with this unit (e.g., floppy disks, PDAs and other hand-held peripheral, CD-ROMs, etc.)”

9. Session Lock

The OSA times out sessions or requires a re-authentication process after (30) minutes of inactivity.

Procedure:

The Administration Department contracts with DTO to time-out sessions or require a re-authentication process after (30) minutes of inactivity.

I. ACCESS CONTROL (CONTINUED)

B. Network Access Management

Purpose:

The purpose of the network access management section is to establish procedures to control and monitor access and use of the network infrastructure. These are necessary to preserve the integrity, availability and confidentiality of OSA information.

Policy:

1. Remote Access

- The OSA restricts the allowed methods for remote access to the network and information systems.
- The OSA utilizes automated mechanisms to enable management to monitor and control remote connections into networks and information systems.
- Virtual Private Network (VPN) or equivalent encryption technology is used to establish remote connections with the OSA networks and information systems.
- Employees of the OSA access the OSA information system remotely via an approved two-factor authentication (2FA) technology.
- The OSA maintains formal procedures for authorized individuals to access its information systems from external systems, such as access allowed from an alternate work site.

Procedure:

The Administration Department contracts with DTO to provide remote access to the network and information systems only through Virtual Private Network using two-factor authentication and encryption. DTO provides monitoring and control of remote connections.

2. Boundary Protection

- Networks where information deemed critical by the OSA is stored or processed are physically or logically segregated from publicly available networks.

I. ACCESS CONTROL (CONTINUED)

- The OSA networks and information systems are not accessible from public networks except under secured and managed interfaces.
- The OSA limits network access points to a minimum to enable effective monitoring of inbound and outbound communications and network traffic.

Procedure:

The Administration Department contracts with DTO to physically and logically segregate OSA data from publicly available networks except under secured and managed interfaces provided by DTO

C. Identity Management

Purpose:

The purpose of the identity management section is to establish a standardized method to create and maintain verifiable user identifiers, and enable decisions about the levels of access to be given to each individual and/or groups.

Policy:

1. Identification and Authentication

- The OSA maintains unique system identifiers (User IDs) assigned to each user.
- The OSA does not reuse user identifiers until all previous access authorizations are removed from the system, including all file accesses for that identifier.
- The OSA approves, documents, and designates a responsible party for each of these accounts.

Procedure:

The Administration Department identifies and approves each authorized user. The Administration Department contracts with DTO to assign a unique User ID by using first name initial and last name of employee.

I. ACCESS CONTROL (CONTINUED)

D. Authentication

Purpose:

The purpose of the authentication section is to establish the authentication methods utilized by the OSA for authenticating, external / remote access connections, VPN access, administrative function access, vendor access and remote access to sensitive information.

Policy:

1. Authenticator Management

- The OSA uses multifactor authentication to substantiate the claimed identity of a user.

2. Unsuccessful Logon Attempts

- The OSA records successful and failed authentication attempts.

Procedure:

The Administration Department contracts with DTO to monitor authentication attempts using multifactor authentication.

3. Session Lock

- The OSA defines a maximum number of invalid logon attempts commensurate to the criticality of network or information systems.
- The OSA disables user access upon reaching the maximum number of invalid access attempts.
- Network and information systems sessions remain locked for a predetermined time or until the user reestablishes access through an established authentication procedure.

Procedure:

The Administration Department contracts with DTO to enforce a maximum number of logon attempts and to lock sessions until the user reestablishes authenticated access.

I. ACCESS CONTROL (CONTINUED)

E. Emergency Access

Purpose:

The purpose of the emergency access section is to establish conditions under which emergency access is granted, outlines rules to determine who is eligible to obtain emergency access and the authorized personnel entitled to grant access.

Policy:

1. Account Management

- The OSA provides access to required information systems on an emergency basis.
- The emergency procedures ensure that:
 - Only identified and authorized personnel are allowed access to live systems and data;
 - All emergency actions are documented in detail; and
 - Emergency action is reported to management and reviewed in an orderly manner.
- The OSA automatically terminates emergency accounts within twenty-four (24) hours and temporary accounts with a fixed duration not to exceed three-hundred sixty-five (365) days.

Procedure:

The Administration Department contracts with DTO to provide emergency access to authorized personnel as needed during emergency situations. DTO will automatically terminate emergency accounts within twenty-four (24) hours and temporary accounts with a fixed duration not to exceed three-hundred sixty-five (365) days.

I. ACCESS CONTROL (CONTINUED)

F. Password Policy

Purpose:

The purpose of the password section is to establish uniform and enterprise-wide practices to create, manage and maintain passwords to ensure expected level of access security. The policy outlines requirements for creation of strong passwords, protection of those passwords, and password change frequency.

Policy:

1. Account Management

- The OSA maintains a process for password-based authentication to include the following:
 - Automatically force users to change user account passwords every ninety (90) days.
 - Enforce password minimum lifetime of one (1) day;
 - Prohibit the use of dictionary names or words as passwords;
 - Enforce password complexity consisting of at least eight (8) alphanumeric (i.e., upper- and lowercase letters, and numbers) and/or special characters;
 - Enforce a minimum number of characters to be changed when new passwords are created;
 - Encrypt passwords in storage and during transmission;
 - Prohibit password reuse for six (6) generations prior to reuse;
 - For FTI: Change/refresh authenticators every 90 days, at a minimum, for a standard user account, every 60 days, at a minimum, for privileged users.
- The OSA users shall not share passwords with others under any circumstance.
- The OSA shall not allow users to use common words or based on personal information as passwords (e.g., username, social security number, children's names, pets' names, hobbies, anniversary dates, etc.).
- The OSA shall suspend user accounts after a specified number of days of inactivity.

I. ACCESS CONTROL (CONTINUED)

- The OSA shall change passwords immediately if there is reason to believe a password has been compromised or disclosed to someone other than the authorized user.

Procedure:

The Administration Department contracts with DTO to enforce a password-based authentication process to comply with the above OSA policy

G. Password Administration

Purpose:

The purpose of the password administration section is to ensure that the allocation of passwords is controlled through a formal management process.

Policy:

1. Access Agreements

- The OSA information system users shall sign an acknowledgement to evidence understanding of authentication policies, including the OSA policy to keep passwords confidential.
- The OSA requires that employees sign acknowledgement prior to allowing access to network and information systems.

Procedure:

During orientation with a new employee the Administration Department will review authentication policies and the new employee will sign acknowledgement that he/she understands and will comply with the policy.

2. Identification and Authentication

- The OSA shall verify the identity of a user prior to providing a new, replacement or temporary password.

Procedure:

- ***The Administration Department will verify the identity of a user prior to authorizing a new, replacement or temporary password through DTO.***

I. ACCESS CONTROL (CONTINUED)

3. Authenticator Management

- First-time passwords shall be set to a unique value per user and changed immediately after first use.
- The OSA shall provide temporary passwords to users in a secure manner; the use of third parties or unprotected (i.e., clear text) electronic mail messages shall be prohibited.
- The OSA shall not allow default passwords for network and remote applications.

Procedure:

The Administration Department contracts with DTO to provide password management in compliance with the above policy.

4. Authenticator Feedback

- The OSA shall obscure feedback of authentication information during the authentication process to protect the information from possible exploitation/use by unauthorized individuals.

Procedure:

The Administration Department contracts with DTO to provide an authentication process in compliance with the above policy.

OFFICE OF THE STATE AUDITOR INFORMATION SECURITY POLICY

II. ASSET MANAGEMENT

A. Asset Identification

Purpose:

The purpose of asset identification is to ensure that those responsible for acquiring, recording, inventorying, maintaining, and disposing of Information Technology (IT) assets (both capital and non-capital) understand and adhere to the rules, regulations, and procedures governing such assets. Based on this information, the Office of the State Auditor (OSA) provides appropriate levels of protection.

Policy:

1. Asset Management Policy and Procedures

- The Administration Department assumes responsibility for the asset acquisition, distribution, disposition, physical inventory, storage, and accounting entries of all OSA assets.
- Roles and responsibilities are assigned by the Administration Department by position within the SCEIS system.
- The OSA asset management applies to information technology assets recorded in the South Carolina Enterprise Information Systems (SCEIS).
- These assets are classified as capital and non-capital assets. Capital assets are assets with a unit cost or market value of \$5,000 or more and non-capital assets are assets with a unit cost or market value of \$1,000 or more but less than \$5,000.
- Physical inventory of all assets is performed annually.
- Disposition of assets is done on an as needs basis.

Procedures:

Assets are acquired at the request of the Director of Administration (DOA). Once the request is made the purchasing officer conducts a search of the Materials Management Office (MMO) state contract website for state contract pricing. If no state contract exists then suppliers of this product would be contacted for pricing based on the SC State Procurement Code. Once a supplier is chosen the asset is classified as capital or non-capital and a purchase order for the asset is issued to the vendor.

II. ASSET MANAGEMENT (CONTINUED)

Procedures (Continued):

Upon receipt of the asset by the purchasing officer an internal property decal is placed on the asset by the serial number. The asset is then placed in the IT storage area for use or distribution.

The Administration Department creates and verifies roles within the SCEIS system for each position as filled or vacated. When a state agency auditor position is filled a separate request is made to the Technology Division help desk to add statewide auditor function roles for the purpose of performing audits of state agencies. If a position is vacated then the roles are terminated and a separate help desk request is made to terminate statewide access roles.

The Administration Department issues a laptop computer to each new auditor during the new hire orientation on their first day of employment. The laptop is identified by the internal OSA property decal and is associated with a corresponding SCEIS number. The employee signs that he/she has received the equipment along with a copy of section XIII-A through section XIII-E of the agency policy and procedures manual.

In addition to the SCEIS assets module tracking system a separate spreadsheet is maintained as assets are re-assigned. A separate signature sheet is used for release and return of assets. An annual physical inventory is performed for location verification and classification of assets.

The DOA determines when an asset should be disposed of. Once the decision is made the DOA makes a request to the DTO help desk to sanitize the equipment and ensure all computers or any property that may contain sensitive information is sanitized in accordance with Section 2.7 of the South Carolina Hardware Sanitization Policy dated August 2006. A turn in document (TID) is completed by the Administration Department and forwarded to the Division of General Services Surplus Property along with an original signed certification of sanitization. A representative from Surplus Property screens the equipment to determine if it can be resold or junked. If the equipment is deemed junk it is the responsibility of the (SAO) to dispose of the equipment properly. Surplus Property makes arrangements for the other equipment to be picked up and sold.

OFFICE OF THE STATE AUDITOR INFORMATION SECURITY POLICY

III. BUSINESS CONTINUITY MANAGEMENT

A. Contingency Planning

Purpose

The purpose of the contingency planning section is to establish procedures and processes to maintain continuity of critical business operations during or post an incident. This section includes implementation of controls to identify and reduce risks, to limit the impact of damaging incidents, and to ensure the timely resumption of critical business operations.

Policy

1. Contingency Planning Policy and Procedures

- The Office of the State Auditor (OSA) establishes a formal, documented contingency planning policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance.
- The OSA establishes formal, documented procedures to facilitate the implementation of the contingency planning policy and associated contingency planning controls.
- The OSA establishes a formal process for annual contingency planning policy and procedure review and update.

2. Contingency Plan

- The OSA conducts a Business Impact Analysis (BIA) to identify functions, processes, and applications that are critical to the OSA and determine a point in time (i.e. recovery time objective (RTO)) when the impact of an interruption or disruption becomes unacceptable to the OSA.
- The OSA utilizes the BIA results to determine potential impacts resulting from the interruption or disruption of critical business functions, processes, and applications.
- The OSA assigns contingency roles and responsibilities to key individuals from all business functions.
- The OSA establishes procedures to maintain continuity of critical business functions despite critical information system disruption, breach, or failure.

III. BUSINESS CONTINUITY MANAGEMENT

A. Contingency Planning (Continued)

2. Contingency Plan (Continued)

- The OSA documents a Business Continuity Plan (BCP) that addresses documented recovery strategies designed to enable the OSA to respond to potential disruptions and recover its critical business functions within a predetermined RTO following a disruption.
- The OSA establishes a process to ensure that the BCP is reviewed and approved by senior management.
- The OSA distributes copies of the BCP to key personnel responsible for the recovery of the critical business functions and other relevant personnel and partners with contingency roles, as determined by the OSA.
- The OSA establishes and implements procedures to review the BCP at planned intervals and at least on an annual basis.
- The OSA establishes a process to update the contingency plan, including BIA, when changes to the organization, information system, or environment of operation occurred.

3. Contingency Training

- The OSA provides training to personnel with assigned contingency roles and responsibilities.
- The OSA establishes a process for identifying and delivering training requirements (i.e., frequency) to and from the relevant participants and evaluating the effectiveness of its delivery.
- The OSA incorporates simulated events and lessons learned into contingency training to facilitate effective response by personnel with contingency roles when responding to disruption.

4. Contingency Plan Testing

- The OSA tests the BCP at least annually to determine the effectiveness of the plan and the OSA's readiness to execute the plan.
- The OSA reviews the BCP test results, record lessons learned and perform corrective actions as needed.

III. BUSINESS CONTINUITY MANAGEMENT

A. Contingency Planning (Continued)

5. Criticality Analysis

- The OSA employs standard testing methods, ranging from walk-through and tabletop exercises to more elaborate parallel/full interrupt simulations, to determine the effectiveness of the plan and to identify potential weaknesses in the plans.
- The OSA establishes procedures to enable continuation of critical business operations while operating in emergency mode.

B. Disaster Recovery and Contingency Strategies

Purpose:

The purpose of the disaster recovery and contingency strategies section is to establish procedures to facilitate the recovery and restoration of critical business functions in a timely manner by ensuring availability of requisite resources – work location, equipment and technology.

Policy:

1. Disaster Recovery Plan

- The OSA develops a Disaster Recovery Plan (DRP) that addresses scope, roles, responsibilities, and coordination among organizational entities for reallocating information systems operations to an alternate location.
- The OSA establishes recovery time objectives for the BIA identified critical information systems.
- The OSA establishes and documents procedures to fully restore critical information systems, post an incident, without deterioration of the security safeguards originally planned and implemented.
- The OSA assigns disaster recovery roles and responsibilities to key individuals.
- The OSA establishes a process to ensure that the DRP is reviewed and approved by senior management.
- The OSA distributes copies of the DRP to key personnel responsible for the recovery of the critical information systems and other relevant personnel and partners with contingency roles, as determined by the OSA.

III. BUSINESS CONTINUITY MANAGEMENT

B. Disaster Recovery and Contingency Strategies (Continued)

1. Disaster Recovery Plan (Continued)

- The OSA establishes and implements procedures to review the DRP at planned intervals and at least on an annual basis.
- The OSA establishes a process to update the DRP when changes to the organization or environment of operation occurred.

2. Alternate Site

- The OSA through contract with Department of Technology Operations (DTO) identifies and establishes processes to relocate to an alternate site to facilitate the resumption of information system operations for business-critical functions within the defined recovery objectives (RTO and Recovery Point Objective (RPO) when the primary site is unavailable due to disruption.
- The OSA through contract with DTO ensures that equipment and supplies required to resume operations at the alternate processing site are available.
- The OSA ensures contracts are in place with third parties and suppliers to support delivery to the site within the defined time period for transfer/ resumption of critical business operations.
- The OSA through contract with DTO ensures that the alternate processing site provides information security safeguards similar to that of the primary site.
- The OSA through contract with DTO identifies potential accessibility problems to the alternate site in the event of an area-wide disruption or disaster.

3. Telecommunications Services

- The OSA through contract with DTO establishes primary and alternate telecommunication service agreements with priority-of-service provisions in accordance with organizational availability requirements (including RTOs), quality of service and access;
- The OSA through contract with DTO establishes alternate telecommunications services to facilitate the resumption of information system operations for critical business functions within the defined recovery objectives when the primary telecommunications capabilities are unavailable.

III. BUSINESS CONTINUITY MANAGEMENT

B. Disaster Recovery and Contingency Strategies (Continued)

3. Telecommunications Services (Continued)

- The OSA through contract with DTO requires primary and alternate telecommunication service providers to have contingency plans.

4. Information System Recovery and Reconstitution

- The OSA through contract with DTO establishes documented procedures to restore and recover critical business activities from the temporary measures adopted to support normal business requirements after an incident.
- The OSA through contract with DTO implements procedures for the recovery and reconstitution of the information system to a known state after a disruption, compromise, or failure.
- The OSA through contract with DTO provides the capability to restore information system components within defined restoration time periods from configuration-controlled and integrity-protected information representing a known, operational state for the components (for e.g. reimaging methods).
- The OSA through contract with DTO establishes measures to protect backup and restoration hardware, firmware, and software.

C. Data Backup

Purpose:

The purpose of the Data Backup section is to establish procedures and processes to create and maintain information system data backup for easy storage and retrieval process in order to support the disaster recovery process.

Policy:

1. Data Backup and Storage Policy

- The OSA through contract with DTO develops, maintains and documents a Data Backup and Storage Policy that addresses the adequate procedures to storage data and thus ensures the recovery of electronic information in the event of failure.
- The OSA through contract with DTO identifies and applies security requirements for protecting data backups based on the different types of data (sensitive, confidential, public) handled by the entity.

III. BUSINESS CONTINUITY MANAGEMENT

C. Data Backups (Continued)

2. Alternate Storage Site

- The OSA through contract with DTO identifies an alternate storage site that is separated from the primary site so as not to be susceptible to same hazards to storage and recover information system backup information.
- The OSA through contract with DTO establishes necessary agreements with the site/ location owner to ensure that data storage and retrieval processes are not hindered during or post an incident.
- The OSA through contract with DTO ensures that the alternate storage site provides information security safeguards similar to that of the primary storage site.
- The OSA through contract with DTO identifies potential accessibility problems to the alternate storage site in the event of a disruption or disaster.
- The OSA through contract with DTO identifies secure transfer methods when transporting backup media off-site.
- The OSA through contract with DTO establishes and maintains an authorization list to retrieve backups from the off-site location.
- The OSA through contract with DTO reviews on an annual basis the security of the off-site location to ensure data is unexposed to unauthorized disclosure or modification while in storage.

3. Information System Backup

- The OSA through contract with DTO establishes a process to perform data backups of user-level and system-level information at a defined frequency consistent with the established RTOs and RPOs.
- The OSA through contract with DTO establishes a process to perform data backups of information system security documentation at a defined frequency consistent with RTOs and RPOs.
- The OSA through contract with DTO establishes safeguards and controls to protect the confidentiality, integrity, and availability of backup information at storage locations.

III. BUSINESS CONTINUITY MANAGEMENT

C. Data Backups (Continued)

3. Information System Backup (Continued)

- The OSA identifies encryption/secure methods in storage of backup data to transportable media (i.e., tapes, CD Rooms, etc.)
- The OSA enforces dual authorization (“two-person control”) for the deletion or destruction of sensitive data.

Dual authorization (“two-person control”) will require the signatures of the Director of Administration and the Information Security Liaison prior to deletion or destruction of sensitive data.

Contingency Training

The OSA Department of Administration is responsible for training its personnel to respond in a timely manner to a natural disaster. Training is conducted through the IT Information Security Policy which details the process of recovering the OSA Information System. The Contingency Training is conducted once a year to provide policies and procedures for recovery of OSA information system.

Business Impact Analysis

Function:

The function of the Office of the State Auditor (OSA) is to serve as a deterrent to fiscal mismanagement, fraud, and misuse of assets by state agencies and providers of Medicaid services and to provide audit coverage of those entities as required by law or regulation. The OSA Information System is a collection of computers, printers, server, faxes, scanners and telephone system that staff use to collect, filter, process, create and distribute data.

Processes:

1. OSA maintains all working files for state and Medicaid audits as well as personnel files on the OSA server.
2. SCEIS access is granted using the OSA server.
3. The OSA website is maintained and updated through the OSA information system.
4. The OSA telephone system is a part of the OSA Information System. Updates and additions are performed through Spirit Communications.

Applications:

1. Information system applications (SCEIS, Spirit Communications website, FileZilla and Seniors, etc.) are critical to the functions of OSA.

The recovery time objective is as soon as possible. Duration of service disruption will depend on severity and type of disaster encountered. The OSA Information System can be accessed outside of the OSA physical address through use of laptops and cell phones through secure wireless connections.

The OSA Administration Department maintains a spreadsheet which contains an inventory of all OSA hardware (laptops, desktops, servers, monitors, copiers, printers, wireless connectivity, scanners and fax machine) and software that can be used to assess losses in the event of natural disaster.

Business Continuity Plan

In the event of a disruption in service due to a natural disaster, the Office of the State Auditor (OSA) located at 1401 Main Street, Suite 1200, Columbia, South Carolina contacts the Department of Technology Operations (DTO) to recover its computer system in a timely manner.

The recovery strategy is as follows:

1. a. Contact Bob Turnmire of DTO at 803-513-7533 or bob.turnmire@admin.sc.gov when there is a disruption or interruption to the computer system. In the event Bob Turnmire is unavailable, contact the DTO Help Desk 803-896-0001, Opt. 4.
- b. In the event DTO is also affected, the OSA audit staff can continue to work in paper form offsite.
2. Information System applications (SCEIS, Spirit Communications, FileZilla and Seniors, etc.) are critical to the functions of the OSA. The priority of DTO is to ensure the computer system is restored in a timely manner and is functioning properly. Disruption of service time is dictated by nature of the natural disaster.
3. The OSA computer system is backed up by DTO. In the event of a natural disaster impacting the information system, OSA would contact DTO to request a system back-up be restored. If DTO is also affected by the natural disaster, OSA would be forced to wait until DTO has service.
4. The OSA procedure for business continuity is communicated through the IT Policy and Procedures Manual. The OSA staff would be notified through cell phones of any disruption of service due to a natural disaster. A reasonable time of disruption of service is 48 hours.

Disaster Recovery Plan

In the event of a natural disaster, the Office of the State Auditor (OSA) located at 1401 Main Street, Suite 1200, Columbia, South Carolina contacts the Department of Technology Operations (DTO) to recover its computer system in a timely manner when a disruption of the system occurs.

The OSA computer system is backed up by DTO. In the event of a natural disaster, OSA would contact DTO to request a system back-up be restored. If DTO is also affected from the natural disaster, OSA will be forced to wait until DTO has service.

The OSA staff will be notified through cell phones of disruption of service due to a natural disaster.

The primary recovery process is the OSA working files for state and Medicaid audits and personnel files which are kept on the OSA server. SCEIS access, the OSA website and the telephone system are also vital to the recovery process. The recovery time objective is as soon as possible depending on severity and type of disaster encountered.

The OSA Information system requires hardware, software, data and connectivity. If the OSA is without components of the information system, work can be performed in paper form from offsite.

The OSA information system applications (SCEIS, Spirit Communications, FileZilla and Seniors, etc.) are critical to the functions of the OSA. Copies of software should be available for re-installation on laptops and desktops in case of natural disaster. The priority of DTO is to ensure the computer system is restored in a timely manner and is functioning properly. Disruption of service time is dictated by nature of the natural disaster.

OFFICE OF THE STATE AUDITOR INFORMATION SECURITY POLICY

IV. DATA PROTECTION AND PRIVACY

A. Data Classification

Purpose:

The purpose of the data classification section is to define the different categories for the Office of the State Auditor (OSA) information assets regardless of form whether it is electronic, hard copy, or intellectual property.

Policy:

1. Security Categorization

- The OSA categorizes data in accordance with applicable federal and State laws, Executive Orders, directive, regulations, and information security guidance. The OSA data is classified into one of the following categories:
 1. Public: Information intended or required for sharing publicly. Examples of public information include information provided on government website, and reports meant for public distribution. Unauthorized disclosure, alteration or destruction of Public data would result in minimum to no risk to the State.
 2. Internal Use: Information that is used in daily operations of the OSA. Examples of internal use information include the OSA hierarchy structure, internal procedures, and internal communications. Unauthorized disclosure, alteration or destruction of Internal Use data would result in little risk to the State.
 3. Confidential: Confidential information refers to sensitive information in custody of the OSA. Examples of confidential information include credit card information, information security plan, system configuration standards, or information exempt from Freedom of Information Act (FOIA). Unauthorized disclosure, alteration or destruction of confidential data would result in considerable risk to the State.
 4. Restricted: Restricted information is highly sensitive information in custody or owned by the OSA and/or data which is protected by Federal or State laws and regulations. Examples of restricted information may include, but are not limited to, Federal Tax Information (FTI) and health information protected by the Health Insurance Portability and Accountability Act (HIPAA). Unauthorized disclosure, alteration or destruction of Restricted data results in considerable risk to the State including statutory penalties.

OSA INFORMATION SECURITY POLICY

IV. DATA PROTECTION AND PRIVACY (CONTINUED)

- Users who encounter information that is improperly labeled, according to the data classification descriptions above, consults with the owner of the information and/or the OSA Department of Administration to determine the appropriate data classification.
- If multiple data fields with different classifications have been combined, the highest classification of information included will determine the classification of the entire set.

B. Data Disposal

Purpose:

The purpose of the data disposal section is to define the controls that will be followed for disposal of data both in digital and non-digital formats.

Policy:

1. Media Sanitization

- The OSA through contract with DTO sanitizes electronic media prior to disposal, release for reuse and release outside of the OSA based on applicable regulatory requirements.
- The OSA through contract with DTO employs sanitization mechanisms with the strength and integrity commensurate with the security category or classification of the information.
- The OSA tracks media sanitization and disposal process, wherein such actions are tracked, documented, and verified.
- Media sanitization documentation includes a record of the media sanitized, when, how media was sanitized, and the final disposition of the media. The record of action taken is maintained in a written or electronic format.

OSA INFORMATION SECURITY POLICY

IV. DATA PROTECTION AND PRIVACY (CONTINUED)

- The OSA sanitizes electronic media containing Federal Tax Information and does not make it available for reuse by other offices or released for destruction without first being subject to electromagnetic erasing.
- Approved processes like physical destruction or digital degaussing are performed on devices, before they are disposed.
- The OSA destroys hard copy media containing internal-use, confidential or restricted information using approved methods prior to disposal.
- The OSA Department of Administration monitors the destruction of hard copy media, as required to ensure and verify compliance with policy.

C. Data Protection

Purpose:

The purpose of the encryption section is to define the controls that need to be in-place to protect confidential and restricted data.

Policy:

1. System and Communications Protection Policy and Procedures

- The OSA employees follow the OSA's acceptable use policies when transmitting data. The OSA contracts with DTO to provide remote access to the information systems.

2. Cryptographic Key Establishment and Management

- The OSA through contract with DTO maintains mechanisms to ensure availability of information in the event of the loss of cryptographic keys by users.
- The OSA through contract with DTO implemented mechanisms to ensure the confidentiality of private keys.
- The OSA through contract with DTO maintains appropriate controls to physically and logically safeguard the key-generating equipment from construction through receipt, installation, operation, and removal from service.

OSA INFORMATION SECURITY POLICY

IV. DATA PROTECTION AND PRIVACY (CONTINUED)

3. Cryptographic Protection

- For Restricted or data protected by Federal or State laws or regulations: The OSA through contract with DTO uses Federal Information Processing Standards (FIPS)-140 validated (e.g., Advanced Encryption Standards (AES), Triple Data Encryption Algorithm (TDEA), Diffie-Hellman, RSA, Rivest Cipher 5 (RC5)) technology for encrypting confidential data.
- The OSA through contract with DTO implements all encryption mechanisms to comply with this policy and support a minimum of, but not limited to the industry standard, AES 128-bit encryption.
- The OSA does not use any proprietary encryption algorithms for any purpose, unless approved by OSA's Department of Administration.

4. Transmission Confidentiality and Integrity

- Confidential or restricted information transmitted as an email message is encrypted based on DTO encryption policy.
- Any confidential or restricted information transmitted through a public network to and from vendors, customers, or entities doing business with OSA must be encrypted or transmitted through a tunnel encrypted by approved technologies such as virtual private networks (VPN).

OSA INFORMATION SECURITY POLICY

IV. DATA PROTECTION AND PRIVACY (CONTINUED)

D. Privacy

Purpose:

The purpose of the privacy section is to set forth policies the OSA uses when information systems or applications will gather Personal Identifiable Information (PII) and/or when webpages are available openly to the public.

Policy:

1. Privacy Impact Assessment

- The OSA conducts a Privacy Impact Assessment (PIA) on information systems that will handle Personal Identifiable Information (PII).
- The OSA publishes privacy policies on the OSA websites used by the public.
- The OSA updates PIAs when a system change creates new privacy risks (e.g., when functions applied to existing information collection change anonymous information into information in identifiable form).
- PIAs includes:
 - a. What information is to be collected (e.g., nature and source);
 - b. Why information is being collected (e.g., to determine eligibility)
 - c. Intended use of information (e.g., to verify existing data);
 - d. With whom the information will be shared;
 - e. What opportunities individuals have to decline to provide information;
 - f. How the information will be secured;
- The PIA document is reviewed by the OSA Department of Administration.
- Each employee of the OSA is to provide a confidentiality agreement defining the responsibilities of the OSA's employees and business partners (e.g., contractors, vendors) in maintaining the privacy of electronic information.

OSA INFORMATION SECURITY POLICY

IV. DATA PROTECTION AND PRIVACY (CONTINUED)

D. Privacy

Procedure:

The OSA will conduct a Privacy Impact Assessment (PIA) on systems involving Personal Identification Information (PII). The PIA will be reviewed by the Department of Administration designee. The PIA Assessment document is kept internally prior to completion by the OSA staff member. The OSA Privacy and Security policy will be available on the OSA website. During orientation with a new employee the Administration Department will review the confidentiality agreement defining the responsibilities of maintaining the privacy of electronic information. The new employee will sign acknowledgement that he/she understands and will comply with the policy.

OFFICE OF THE STATE AUDITOR INFORMATION SECURITY POLICY

V. HUMAN RESOURCE (HR) AND SECURITY AWARENESS

A. Human Resource Compliance

Purpose:

The purpose of human resource (HR) compliance is to define security roles and responsibilities for employees, contractors and third party users.

Policy:

1. Personnel Security Policy and Procedures

- The Office of the State Auditor (OSA) defines security roles and responsibilities of employees and documents in accordance with the organization's information security policy. **(See Section I – Access Control)**

2. Personnel Screening and Third-Party Personnel Security

- The OSA conducts background verification checks on all candidates for employment, which are carried out in accordance with relevant laws.

3. Personnel Termination and Transfer

- Upon termination/transfer of employment for employees, termination of engagement for non-employees, or immediately upon request, personnel returns to the OSA all agency documents (and all copies thereof) and other agency property and materials in their possession or control.

4. Access Agreements

- As part of their information security obligation, employees, contractors and third party users shall agree and sign an acceptable use policy, which shall state responsibilities for information security.

V. HUMAN RESOURCE (HR) AND SECURITY AWARENESS

B. Security Awareness Training

Purpose:

The purpose of security and awareness training is to define the information security training requirements for the OSA employees, contractors and third party users.

Policy:

1. Security Awareness Training and Information Security Workforce

- The OSA management requires employees, contractors and third party users to apply security in accordance with established policies and procedures of the organization.

2. Role-Based Security Training

- The OSA imparts appropriate awareness training and regular updates in organizational policies and procedures to all employees of the organization and to, contractors and third party users, as relevant for their job function.
 - Training must be accompanied by an assessment procedure based on the cyber security training content presented in order to determine comprehension of key cyber security concepts and procedures.
- User access to the OSA information assets and systems will only be authorized for those users whose cyber security awareness training is current (e.g., having passed the most recent required training stage).

3. Testing, Training, and Monitoring

- The OSA appoints a cyber-security awareness training coordinator to manage training content, schedules and user training completion status.
- The OSA cyber security training coordinator, along with the agency CISO or security manager reviews training content from the Division of Technology on an annual basis to ensure that it aligns with State of South Carolina policies.

OFFICE OF THE STATE AUDITOR INFORMATION SECURITY POLICY

VI. IT COMPLIANCE

A. Audit and Compliance Requirements

Purpose:

The purpose of the Audit and Compliance section is to establish controls and processes to help ensure compliance with information security policies and standards at State agencies and institutions.

Policy:

1. Compliance with legal and contractual requirements

- The Office of the State Auditor (OSA) through contract with the Division of Technology Operations (DTO) identifies and documents its obligations to applicable State, federal and other third party laws and regulations in relation to information security.

2. Compliance with security policies and standards

- At least annually, the OSA performs reviews or audits of users' and systems' compliance with security policies, standards, and procedures, and initiate corrective actions where necessary.
- Results from compliance reviews or audits shall be documented, and reported to the Office of the State Auditor leadership.

3. Audit and Accountability Policy and Procedures

- The OSA through contract with DTO establishes a formal, documented audit and accountability policy and associated audit and accountability procedures.
- The OSA through contract with DTO implements a process to review and update the audit and accountability policy and associated procedures at least annually.

OFFICE OF THE STATE AUDITOR INFORMATION SECURITY POLICY

VI. IT COMPLIANCE (CONTINUED)

B. Information System Audit Considerations

Purpose:

The purpose of the IS Audit Considerations section is to establish controls and processes to maximize the effectiveness of and to minimize interference to/from the information systems audit process.

Policy:

1. Information systems audit controls

- The OSA through contract with DTO implements audit procedures to help ensure that activities involving reviews or audits of operational systems are carefully planned to minimize the risk of disruptions to business processes.

2. Protection of information systems audit tools

- The OSA through contract with DTO implements security controls to help prevent unauthorized access and/or access abuse of audit tools.

3. Audit Events

- The OSA determines the type of events that are to be audited within information systems.
- The OSA through contract with DTO reviews and updates the list of audited events annually.
- The OSA leadership ensures coordination between the audit function, information security function, and business functions to facilitate the identification of auditable events.

4. Content of Audit Records

- The OSA information systems through contract with DTO is enabled to generate audit records containing details to help establish what type of event occurred, when and where the event occurred, the source and outcome of the event, and the identity of any individuals or subjects associated with the event.

OFFICE OF THE STATE AUDITOR INFORMATION SECURITY POLICY

VI. IT COMPLIANCE (CONTINUED)

B. Information System Audit Considerations (Continued)

5. Audit Records Review and Reporting

- The OSA analyzes information system audit records periodically.
- The OSA reports findings of audit records reviews to information security personnel and Office of the State Auditor leadership.
- The OSA performs correlation and analysis of information generated by security assessments and monitoring.

6. Audit Storage Capacity

- The OSA through contract with DTO allocates sufficient audit storage capacity to help ensure compliance with audit logs retention requirements from State, federal, and other applicable third party laws and regulations.
- The OSA implements provisions for information systems to off-load audit records at regular intervals onto a different system or media than the system being audited.

C. Information Security Continuous Monitoring

Purpose:

The purpose of the Information Security Continuous Monitoring policy is to establish controls that will provide State agencies and institutions the effective monitoring and response capabilities in relation to compliance issues and incidents.

Policy:

1. Continuous Monitoring

- The OSA through contract with DTO monitors the security controls on an ongoing basis.
- The OSA assessment teams are independent from operational or business functions, or hired third parties.

OFFICE OF THE STATE AUDITOR INFORMATION SECURITY POLICY

VI. IT COMPLIANCE (CONTINUED)

C. Information Security Continuous Monitoring (Continued)

2. Plan of Action and Milestones

- The OSA develops a plan of action and milestones to document planned remedial actions to correct weaknesses or deficiencies identified as result of internal/external risk assessments, security reviews, and/or audits.
- The OSA updates its plan of action and milestones at least on a yearly basis, and also based on the findings from continuous security monitoring activities.

OFFICE OF THE STATE AUDITOR INFORMATION SECURITY POLICY

VII. IT RISK STRATEGY

A. Security Performance and Metrics

Purpose:

The purpose of the Security Performance and Metrics section is to establish controls to assess the performance of the security program and its components.

Policy:

1. Information Security Measures of Performance

- The Office of the State Auditor (OSA) develops, monitors, and reports on performance metrics to demonstrate progress in adoption of security controls, and associated policies and procedures, and effectiveness of the information security program.
- The OSA-defined performance measures are able to support the determination of information system security posture, demonstrate compliance with requirements, and identify areas of improvement.

Procedure:

OSA conducts an annual assessment of its Information Security Policies to assess the performance of the security program.

2. Manageability of Metrics

- The OSA ensures that the metrics/measures that are collected are meaningful, yield impact and outcome findings, and provide stakeholders with the time necessary to use the results to address performance gaps.

3. Data Management Concerns

- The OSA standardizes the data collection methods and data repositories used for metrics data collection and reporting to ascertain the validity and quality of data.

B. Third Party Risk Management

Purpose:

The purpose of the Third Party Risk Management section is to establish the controls to safeguard Office of the State Auditor information and information processing facilities that are accessed, processed, communicated to, or managed by third parties.

Policy:

1. External Information System Services

- The OSA establishes a policy and associated processes to enforce that third parties comply with information security requirements and employ defined security controls in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance.
- The OSA implements processes, methods, and techniques to monitor security control compliance by third parties on an ongoing basis.

2. Risk Assessment

- The OSA establishes a process to conduct risk assessments on third party service providers, and document the risk assessment results.
- The OSA implements controls to help ensure that risk assessments are updated in case of major changes in scope of services or contractual changes with third parties.

3. System Interconnections

- The OSA authorizes connections from the OSA information systems to third party information systems by entering into Interconnection Security Agreements.
- For each third party interface, The OSA documents the interface characteristics, security requirements, and the nature of the information communicated.

4. Use of External Information Systems

- The OSA establishes terms and conditions for trust relationships established with other entities owning, operating, and/or maintaining external information systems.
- Terms and conditions established by Office of the State Auditor should control:
 - Access to the OSA information systems from third party information systems; and
 - Controls for processing, storing, or transmit of Office of the State Auditor data using third party information systems.
- The OSA reviews and updates third party security agreements on an annual basis, or as defined in the contract.

5. Information Sharing with Third Parties

- The OSA shares personally identifiable information (PII) with third parties only for the authorized purposes identified in the Privacy Act and/or described in its notice(s), as well as State laws and Interconnection Security Agreements.
- The OSA, where appropriate, enters into Memoranda of Understanding, Memoranda of Agreement, Letters of Intent, Computer Matching Agreements, or similar agreements, with third parties that specifically describe the types of sensitive data covered (e.g., PII) and specifically enumerate the purposes for which the data may be used.
- The OSA monitors, audits, and trains its staff on the authorized sharing of sensitive data with third parties and on the consequences of unauthorized use or sharing of such data.
- The OSA evaluates any proposed new instances of sharing sensitive data with third parties to assess whether the sharing is authorized and whether additional or new public notice is required.

Procedure:

The OSA does not allow access to its server through third parties. Therefore, there is no need for a third-party risk management assessment.

OFFICE OF THE STATE AUDITOR INFORMATION SECURITY POLICY

VIII. INFORMATION SYSTEMS ACQUISITIONS, DEVELOPMENT, AND MAINTENANCE

A. Change Management

Purpose:

The purpose of the change management section is to ensure all changes are assessed, approved, implemented and reviewed in a controlled manner to production and applicable non-production environments with minimal impact and risk.

Policy:

1. Configuration Change Control

- The Office of the State Auditor (OSA) contracts with DTO to manage changes to information systems in order to minimize the likelihood of disruption, unauthorized alterations and errors. The implementation of changes is controlled through the use of a change control process. The following recommendations are followed for the change control process:
 - All requests for change are handled in a structured way that determines the impact on the operational system and its functionality;
 - All changes to production environments, including emergency maintenance and patches, are formally managed in a controlled manner;
 - All changes are categorized, prioritized and authorized by the Administration Department;
 - Post-implementation reviews are performed to ensure production changes are operating as intended;
 - All changes to the production environment are thoroughly and adequately tested;
 - Emergency changes that do not follow the established change process are defined, tested and authorized by the Administration Department; and
 - Information systems are reviewed and tested after major changes to operating systems.

VIII. INFORMATION SYSTEMS ACQUISITIONS, DEVELOPMENT, AND MAINTENANCE (CONTINUED)

B. Configuration Management

Purpose:

The purpose of the configuration management section is to establish procedures for the compliance with minimally acceptable system configuration requirements. In addition, this section helps ensure the OSA through contract with DTO establishes processes to identify and implement secure configurations, control configuration changes, and monitor security controls to validate adherence with approved configurations.

Policy:

1. Baseline Configuration

- DTO develops, reviews, and formally approves baseline configurations (most secure state) for critical information systems and infrastructure components.
- DTO develops a process to manage changes to baseline configurations, including identification, review, security impact analysis, test, and approval prior to implementation of changes.
- DTO establishes a central repository of all baseline configurations and shall implement access restrictions to prevent unauthorized changes.
- DTO retains older versions of baseline configurations to be able to support rollback.
- DTO reviews and updates baseline configurations periodically, and/or as an integral part of information system component installations or upgrades.

2. Configuration Management Plan

- DTO assigns responsibilities for developing and managing the configuration management process to personnel that are not directly involved in system development activities.

VIII. INFORMATION SYSTEMS ACQUISITIONS, DEVELOPMENT, AND MAINTENANCE (CONTINUED)

C. System Development and Maintenance

Purpose:

The purpose of the system development and maintenance section is to define requirements for system security planning and to improve protection of Office of the State Auditor information system resources.

Policy:

1. System Security Plan

- The OSA through contract with DTO prepares system security plans and documentation for critical enterprise information systems or systems under development.
- The System security plans provide an overview of the security requirements of the system and describe the controls in place for meeting the requirements through all stages of the systems development life cycle.
- When the system is modified in a manner that affects security, system documentation shall be updated accordingly.

2. Vulnerability Scanning

- The DTO performs a vulnerability assessment on all enterprise information systems undergoing significant changes, before the systems are moved into production.
- The DTO performs periodic vulnerability assessments on production enterprise information systems and takes appropriate measures to address the risks associated with any identified vulnerabilities.
- Vulnerability notifications from vendors and other appropriate sources are monitored and assessed for all information systems and applications.

3. System and Services Acquisition Policy and Procedures

- The OSA follows procedures consistent with State procurement standards as defined by the Division of Information Security and the Information Technology Management Office.

VIII. INFORMATION SYSTEMS ACQUISITIONS, DEVELOPMENT, AND MAINTENANCE (CONTINUED)

3. System and Services Acquisition Policy and Procedures (Continued)

- The OSA ensures that the State's interests are protected and enforced in all IT procurement contracts.

4. System Development Life Cycle

- The OSA implements appropriate security controls at all stages of the information system life cycle.

5. External Information System Services

- The OSA supervises and monitors outsourced software development to validate Office of the State Auditor security requirements.

6. Developer Security Testing and Evaluation

- The OSA establishes separate development, testing, and production environments.
- The OSA does not use production data for testing purposes unless the data has been obfuscated, sanitized, or declassified. If production data must be temporarily used in these environments, appropriate security controls, including management approval, procedures to remove/delete data after completion of tests, and documentation of activities, are implemented.

7. Flaw Remediation

- The OSA designs appropriate controls into information systems, including user developed applications to ensure correct processing.
- The OSA through contract with DTO ensures that software patches are applied when they function to remove or reduce security weaknesses.

8. Security Alerts, Advisories, and Directives

- The OSA through contract with DTO collects information system security alerts, advisories, and directives on patches on an ongoing basis and implements these security directives in accordance with established time frames.

VIII. INFORMATION SYSTEMS ACQUISITIONS, DEVELOPMENT, AND MAINTENANCE (CONTINUED)

8. Security Alerts, Advisories, and Directives (Continued)

- DTO monitors vulnerabilities and vendors' releases of patches and fixes.

9. Software, Firmware, and Information Integrity

- The OSA through contract with DTO ensures that any decision to upgrade to a new release shall take into account the business requirements for the change, and the security of the release (e.g., the introduction of new security functionality or the number and severity of security problems affecting this version).
- DTO tests critical operating system (OS) changes and updates in the test environment to ensure there is no adverse impact on organizational operations or security.

10. Information Input Validation

- The OSA incorporates controls into information systems to check the validity of information inputs and information outputs.
- The OSA incorporates processing validation checks into information systems to detect processing errors, inadvertent or deliberate processing actions (e.g., accidental deletions).

11. Session Authenticity

- The OSA through contract with DTO identifies the appropriate controls to ensure session authenticity, protecting message integrity in applications and protecting information transmission to and from information systems.

VIII. INFORMATION SYSTEMS ACQUISITIONS, DEVELOPMENT, AND MAINTENANCE (CONTINUED)

D. Release Management

Purpose:

The purpose of the release management section is to define the appropriate release activities during an implementation or upgrade of information systems.

Policy:

1. Allocation of Resources

- The OSA through contract with DTO ensures that production-ready release packages have been deployed using the release management lifecycle (i.e., plan, prepare, build and test, pilot, and deploy).
- DTO determines as part of the release planning process:
 - Resources required to deploy the release;
 - Pass/fail criteria;
 - Build and test plans prior to implementation;
 - Pilot and deployment plans; and
 - Develop requirements for the release.

2. Information System Documentation

- DTO documents the set of tools and processes used to manage the IT release lifecycle, and the prioritization of the release;
- DTO validates the release design against the requirements, and identify the risks and potential issues.

3. Security Engineering Principles

- DTO implements standardization and enforces operational controls through the use of change requests for deploying releases into production.

OSA INFORMATION SECURITY POLICY

IX. GOVERNANCE

A. Information Security Program Planning

Purpose:

The purpose of this section is to establish the principles to regulate how the Office of the State Auditor (OSA) provides an appropriate level of governance controls over Information Security related activities.

Policy:

1. Information Security Plan

The Office of the State Auditor (OSA) develops and communicates an information security plan that underlines security requirements, the security management controls, and common controls in place for meeting those requirements.

- The OSA's security plan identifies and assigns security program roles, responsibilities and management commitment, and ensures coordination among the agency's business units, as well as compliance with the security plan.
- The OSA ensures coordination among the business units responsible for the different aspects of information security (i.e., technical, physical, personnel, etc.)
- The OSA ensures that the security plan is approved by senior management.
- The OSA reviews the information security plan at least on an annual basis.
- The OSA updates the security plan to address changes and problems identified during plan implementation or security control assessments.
- The OSA protects the information security plan from unauthorized disclosure and modification.

2. Information Security Resources

- The OSA considers resources needed to implement and maintain the information security plan in capital planning and investment requests.

3. Plan of Action and Milestones Process

- The OSA implements a process for ensuring that plans of action and milestones for the security program and associated information systems are developed and maintained.

IX. GOVERNANCE (CONTINUED)

3. Plan of Action and Milestones Process

- The OSA reviews plans of action and milestones for consistency with the agency's risk management strategy and priorities for risk response actions.

The OSA Department of Administration communicates with Division of Technology Operations (DTO) on an annual basis to identify deficiencies related to security controls.

4. Information Security Measures of Performance

- The OSA develops, monitors and reports on the results of information security measures of performance, as directed or guided by the SC DIS and SC EPO.

The OSA conducts annual assessment of Information Security Policies to assess the performance of the security program

B. Security Organization (Roles and Responsibilities)

Purpose:

The purpose of this section is to establish key principles based on which the OSA's Security Organization shall be established.

Policy:

1. Information Security Authority

- The OSA agency's chief executive ensures that OSA's senior officials are given the necessary authority to secure the operations and assets under their control.

2. Information Security Liaison

- The OSA appoints an information security liaison with the mission and resources to: coordinate, develop, implement, and maintain an information security plan.

3. Information Security Workforce

- The OSA through contract with DTO establishes an information security workforce and professional development program appropriately sized to the OSA's information security needs.

IX. GOVERNANCE (CONTINUED)

4. Role-based Security Training

- The OSA provides role-based security training to personnel with assigned security roles and responsibilities.

C. Policy Management (Plan of Action)

Purpose:

The purpose of this section is to establish key principles based on which the OSA's security procedures shall be developed.

Policy:

1. Procedure Development

- The OSA adopts a risk-based approach to identify State and agency-specific information security objectives, and develops information security procedures in alignment with the identified security objectives.
- The OSA allocates the appropriate subject matter experts to the development of State and agency-specific information security procedures.
- The OSA approaches independent external (third party) specialists to assist in the development of information security policies in cases where it is established that the required skills do not exist within the agency and are not available within any other state government agency.
- The OSA works in collaboration with other states, Federal government, and external special interest groups in cases where procedures directly or indirectly affect interfacing activities with them.
- Information security procedures that are developed contains the following information, as appropriate:
 - Revision history
 - Introduction
 - Preface
 - Ownership, roles, and responsibilities
 - Purpose
 - Policy statements
 - Policy supplement
 - Guidance
 - Definitions

IX. GOVERNANCE (CONTINUED)

1. Procedure Development (Continued)

- Scenarios which cannot be effectively addressed within the constraints of the agency's security procedures, should be identified as exceptions:
 - Exceptions shall be evaluated in the context of potential risk to the agency as a whole;
 - Exceptions that create significant risks without adequate compensating controls shall not be approved; and
 - Exceptions shall be consistently evaluated in accordance with the agency's risk acceptance practice.
- The OSA reviews each draft procedure with stakeholders who shall be impacted by the procedure, to ensure that the procedure is enforceable and effective.
- The OSA identifies gaps within the procedures that are not enforceable and effective, shall document the gaps, and shall assign the appropriate resources to remediate the gaps.
- The OSA develops and implements a communication plan to disseminate new procedures or changes to existing procedures.
- The OSA reviews procedures on an annual basis to ensure that procedures are up-to-date and aligned with the State's risk posture.

2. Procedure Review and Approval

- A procedure governance committee shall be established for the purpose of review and approval of procedures.
- Procedure exemptions shall be explicitly approved by the procedure governing committee.
- Procedure approval history shall be documented in detail.

3. Procedure Implementation

- The OSA implements mechanisms to help ensure that information security procedures will be available to OSA's personnel on a continuous basis and whenever required.
- The OSA requires employees to review and acknowledge understanding of information security procedures prior to allowing access to sensitive data or information systems.

The OSA communicates the Information Security Policies and Procedures to the OSA staff through the OSA Intranet.

IX. GOVERNANCE (CONTINUED)

D. Information Security Controls Deployment

Purpose:

The purpose of this section is to establish key principles for deployment of information security controls.

Policy:

1. Controls Deployment

- The OSA adopts a risk-based approach to prioritize deployment of controls.
- The OSA allocates the appropriate subject matter experts to the deployment of State and agency-specific information security controls.
- The OSA approaches independent external (third party) specialists to assist in the deployment of information security controls in cases where it is established that the required skills do not exist within the agency and are not available within any other state government agency.
- Controls which cannot be deployed due to the OSA's resource or other constraints must be reported to the office of the State Chief Information Security Officer.
- The OSA reviews each control with stakeholders who shall be impacted, to ensure that the control is enforceable and effective.
- The OSA identifies gaps within the controls that are not enforceable and effective, documents the gaps, and assigns the appropriate resources to remediate the gaps.
- The OSA develops and implements a communication plan to disseminate new controls or changes to existing controls.
- The OSA reviews controls on an annual basis to ensure that they are up-to-date and aligned with the State's risk posture.

OFFICE OF THE STATE AUDITOR INFORMATION SECURITY POLICY

X. MOBILE SECURITY

A. Mobile Security

Purpose:

The purpose of the mobile security section is to describe the minimum security policy for mobile devices used to access State data, including usage restrictions, configuration management, device authentication, and implementation of mandatory security software.

Policy:

State business requirements may, on occasion, justify storing confidential data on mobile computing devices. It is the responsibility of the Office of the State Auditor (OSA) to recognize the associated risks and take the necessary steps to protect and secure their mobile computing devices.

1. Device Identification

- The OSA only allows portable media devices when these are assigned and identified to an individual owner.
- The OSA only allows the use of portable media devices that allow sanitization.
- The OSA uses mobile devices that have the ability to be remotely wiped/erased.

2. Access Control for Mobile Devices

- The OSA through contract with the Division of Technology (DTO) develops usage restrictions, configuration requirements, connection requirements, and implementation guidance for organization-controlled mobile devices.
- The OSA develops a list of approved mobile devices. Only approved mobile devices shall be allowed to access the OSA's network and information systems.
- The OSA develops and applies adequate asset management procedures to all mobile devices.
- The OSA utilizes the approved encryption standard for mobile devices.

X. MOBILE SECURITY (CONTINUED)

2. Access Control for Mobile Devices (Continued)

- The OSA through contract with DTO implements controls to centrally manage the installation of standardized operating system, applications and patches on mobile devices.
- The OSA through contract with DTO removes sensitive and confidential information from the mobile device before it is disposed.
- The OSA deploys administrative and technical controls to mitigate risks associated with lost or stolen mobile devices.
- In order to reduce risks associated with vulnerabilities in mobile devices, the OSA implements:
 - Controls for testing vendor recommended patches, hot-fixes or service packs before such changes are approved installation; and
 - A process to keep system hardware, operating system and applications up-to-date with the approved system updates.
- The OSA through contract with DTO disables all mobile device options and applications that are not in use or required by users' duties.
- The OSA protects all mobile devices with password or Personal Identification Number (PIN).
- The OSA through contract with DTO ensures all mobile devices have timeout/locking features.
- The OSA through contract with DTO develops controls for the protection of data storage on mobile devices including removable media.
- The OSA through contract with DTO protects the storage and transmission of information on portable and mobile information devices through scanning the devices for malicious code, virus protection software. Before a mobile device is connected to an OSA's network, it shall be scanned for viruses. If mobile device is used for transitional storage (e.g., copying data between systems), the data shall be securely deleted from the mobile device immediately upon completion.
- The OSA develops a process for users to notify designated personnel when mobile devices are lost or stolen. The process shall include remote wiping / erasing of mobile devices.

X. MOBILE SECURITY (CONTINUED)

3. Access Agreements

- The OSA ensures that individuals requiring access to information or information systems sign appropriate access agreements prior to being granted access.
- The physical security of these devices shall be the responsibility of the employee to whom the device has been assigned. Devices shall be kept in the employee's physical presence whenever possible. Whenever a device is being stored, it shall be stored in a secure place, preferably out of-sight.

B. Portable Computing Devices

Purpose:

The purpose of the Portable Computing Devices security section is to establish security mechanisms to protect both portable computing devices, such as laptops, and the information they contain.

Policy:

1. Access Control for Mobile Devices

- The OSA through contract with DTO employs whole disk encryption to protect the confidentiality and integrity of information stored on computing devices, including laptops.
- The OSA through contract with DTO configures computing devices operating system (OS) so that only approved services are enabled and/or installed.
- The OSA through contract with DTO implements a configuration management process that includes flaw remediation such as installing most current stable security patches, critical security updates and hot fixes for the relevant OS.
- The OSA through contract with DTO implements tools to automatically update virus definition files on laptops and other portable computing devices susceptible to viruses.
- The OSA through contract with DTO installs firewall software on laptops and implements mechanisms that prevent users from making firewall configuration changes.
- Unauthorized software is not installed on laptops and/or other portable computing devices. Approval through contract with DTO is obtained for the installation of any software that may be required for business use.

X. MOBILE SECURITY (CONTINUED)

B. Portable Computing Devices (Continued)

1. Access Control for Mobile Devices (Continued)

- The OSA places asset tags on portable computing devices.
- The OSA disables Peer-to-Peer wireless connections, otherwise known as “Ad-Hoc Connections”, on all portable computing devices, including laptops.

OFFICE OF THE STATE AUDITOR INFORMATION SECURITY POLICY

XI. PHYSICAL & ENVIRONMENTAL SECURITY

A. Physical Access and Security

Purpose:

The purpose of the Physical Access and Security section is to prevent unauthorized physical access to the Office of the State Auditor (OSA) information assets in order to protect them from damage, interruption, misuse, destruction and/ or theft.

Policy:

1. Physical and Environmental Protection Policy and Procedures

- The OSA contracts with DTO to provide physical and environmental protection of OSA electronic information assets.

2. Physical Access Authorizations

- The OSA contracts with DTO to control authorization for physical access to OSA electronic information assets.

3. Physical Access Control

- The OSA contracts with DTO to control physical access to OSA electronic information assets.

4. Access Control for Transmission Medium

- The OSA contracts with DTO to control physical access to information system distribution and transmission lines within the data center(s) using physical access control devices (e.g., keycard or keys).

5. Access Control for Output Devices

- The OSA Department of Administration places output devices in secured areas and in locations that can be monitored by authorized personnel, and allow access to authorized individuals only.
- The OSA Department of Administration controls physical access to information system output devices (e.g., printers, copiers, scanners, facsimile machines) to prevent unauthorized individuals from obtaining sensitive data.

OFFICE OF THE STATE AUDITOR INFORMATION SECURITY POLICY

XI. PHYSICAL & ENVIRONMENTAL SECURITY (CONTINUED)

A. Physical Access and Security (Continued)

6. Monitoring Physical Access

- The OSA contracts with DTO to review physical access logs at a defined frequency and upon occurrence of security incidents.

7. Visitor Access Records

- The OSA contracts with DTO to maintain visitor access records to the data center(s) and/or sensitive facilities for a minimum of 1 year

8. Delivery and Removal

- The OSA contracts with DTO to establish processes to authorize, monitor, and control items entering and exiting the data center(s) and maintain records of those items.

B. Environmental Security

Purpose:

The purpose of the Environmental Security section is to protect the OSA information assets from damage, destruction and/ or interruption due to environmental factors such as fire, humidity, water, power outage, etc.

Policy:

The OSA contracts with DTO to provide environmental security for OSA electronic information assets.

OFFICE OF THE STATE AUDITOR INFORMATION SECURITY POLICY

XI. PHYSICAL & ENVIRONMENTAL SECURITY (CONTINUED)

C. Disposal of Equipment

Purpose:

The purpose of the Disposal of Equipment section is to define the controls that are followed for disposal of information system equipment which contains the OSA information.

Policy:

1. Media Sanitization:

- The OSA contracts with DTO for disposal of digital media and data storage devices.
- The OSA through contract with DTO employs sanitization mechanisms with the strength and integrity commensurate with classification of data to be sanitized.
- The OSA contracts with DTO for cleansing and disposal of computers, hard drives, and fax/printer/scanner devices.
- The OSA tracks the sanitization of devices prior to disposal.

OFFICE OF THE STATE AUDITOR INFORMATION SECURITY POLICY

XII. RISK MANAGEMENT

A. Risk Management

Purpose:

The purpose of the risk management section is to define the controls that are implemented by the Office of the State Auditor to identify and assess information security risks and to take steps to reduce risk to an acceptable level.

Risk management typically consists of the following:

- Risk Assessment: A risk assessment is the first process of risk management, and is used to determine the extent of the potential threat and the risk associated with IT security.
- Risk Mitigation: Risk mitigation involves prioritizing, evaluating, and implementing the appropriate risk-reducing controls for the risks identified during the risk assessment process.

Policy:

1. Risk Management Strategy

- The Office of the State Auditor defined a schedule for an on-going risk assessment and risk mitigation process.
- The Office of the State Auditor reviewed and evaluated risk based on the system categorization level and/or data classification of their systems.

B. Risk Assessment

Purpose:

The purpose of the risk assessment section is to define a process to identify and manage IT security risks and ensure ongoing compliance with applicable State laws and regulations.

Policy:

1. Risk Assessment

- The Office of the State Auditor established a risk assessment framework based on applicable State and federal laws, regulation, and industry standards (e.g., NIST 800-30). This assessment framework shall clearly define accountability, roles and responsibilities.

OFFICE OF THE STATE AUDITOR INFORMATION SECURITY POLICY

XII. RISK MANAGEMENT (CONTINUED)

2. Security Assessment

- The Office of the State Auditor annually conducts a formal assessment of the IT security processes and controls to determine the appropriateness of the design and implementation of controls, and the extent to which the controls are operating as intended and producing the desired outcome with respect to meeting the security requirements for their systems (e.g., NIST SP 800-115).
- The Office of the State Auditor ensures that risk assessments identify, quantify, and prioritize risks against criteria for risk acceptance and objectives relevant to the Office of the State Auditor.

3. Plan of Action and Milestones

- The Office of the State Auditor develops and periodically updates a Plan of Action & Milestones (POAM) document that shall identify any deficiencies related to internal security controls. The POAM shall identify planned, implemented, and evaluated remedial actions to correct deficiencies noted during annual assessments.
- The Office of the State Auditor develops and periodically updates a Corrective Action Plan (CAP) to identify activities planned or completed to correct deficiencies identified during the security assessment review. Both the POAM and the CAP shall address implementation of security controls to reduce or eliminate known risks in the Office of the State Auditor systems.

The OSA Department of Administration will communicate with DTO annually to identify any deficiencies related to internal security controls. If deficiencies are noted, a Plan of Action and Milestones along with a Corrective Action Plan will be implemented/

4. Security Authorization

- The Office of the State Auditor establishes a process and assigns a senior-level executive or manager to determine whether or not risks can be accepted, and for each of the risks identified following the risk assessment, the designated personnel within the Office of the State Auditor shall make a decision regarding risk treatment.

5. Continuous Monitoring

- The Office of the State Auditor continuously monitors the security controls within its information systems to ensure that the controls are operating as intended.

OFFICE OF THE STATE AUDITOR INFORMATION SECURITY POLICY

XII. RISK MANAGEMENT (CONTINUED)

C. Risk Mitigation

Purpose:

The purpose of the risk mitigation section is to support mitigation of risks identified and to define the level of risk that is acceptable to the Office of the State Auditor where risks are accepted knowingly and objectively.

Policy:

1. Continuous Monitoring

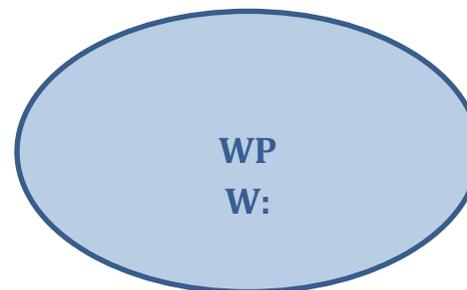
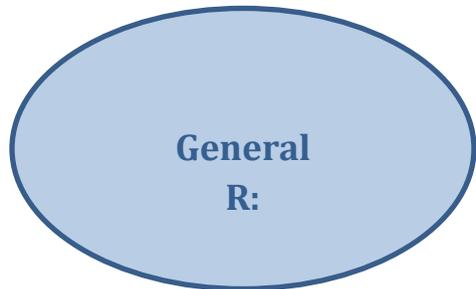
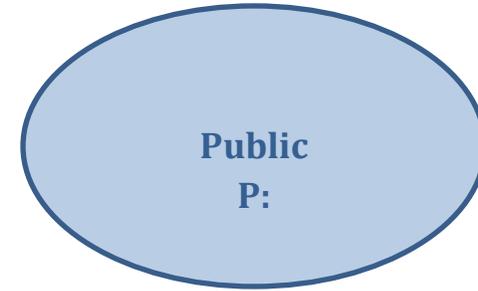
- The Office of the State Auditor establishes and implements controls to ensure risks are reduced to an acceptable level based on security requirements and once threats have been identified and decisions for the management of risks have been made.
- The Office of the State Auditor determines and documents the acceptable level for risk for various threats based on the business requirements and the impact of the potential risk to the Office of the State Auditor.

Risk Assessment

Agency:	SC Office of the State Auditor
Official System Name:	Office of the State Auditor
System Acronym:	OSA
System Business Owner:	Norma Jean Dawkins
System Technical Owner	Norma Jean Dawkins
System Security Owner:	Tracy Brice
System Location Full Address:	1401 Main Street, Suite 1200, Columbia, SC 29201
Contract Number, Contractor names, phone numbers and emails, if applicable	
Function and purpose of the system	The OSA Information System functions as a collection of computers, printers, server, faxes, scanners and telephone system that staff use to collect, filter, process, create and distribute data.
General functional requirements	To complete audit reports of state and Medicaid engagements as well as administrative functions.
Business process, applications and services supported	OSA maintains all working files for state and Medicaid audits as well as personnel files on the OSA server. SCEIS access is granted using the OSA server. The OSA website is maintained and updated through the OSA information system. The OSA telephone system is a part of the OSA Information System. Updates and additions are performed through Spirit Communications. Applications (SCEIS, Spirit Communications website, FileZilla and Seniors, etc.) are critical to the functions of OSA.
System components	Windows 7 Professional
Environmental factors	Loss of power due to electrical outings, natural disaster, etc.
Network diagram with system boundaries (attach)	Attached
General Information flow	The OSA contracts with DTO to maintain its server.
Technical and business users (list)	OSA Staff

The Office of the State Auditor

Server Diagram



OSA Information Systems Risks

Risk No.	Vulnerability	Threat	Risk of Compromise	Risk Summary
1	Patches to correct flaws in application software not installed.	Computer crime Malicious use System compromise unauthorized access	Confidentiality and integrity of OSA data.	Exploitation of flaws in application software could result in compromise of confidentiality and integrity of OSA data.
2	Patches to correct flaws in operating system software not installed.	Computer crime Malicious use	Confidentiality and integrity of OSA data.	Exploitation of flaws in operating system software could result in compromise of confidentiality and integrity of OSA data.
3	Remote access to server console not properly monitored.	System compromise Unauthorized access	Confidentiality and integrity of corporate data.	Remote access currently set to... Restrictive. If these controls are not in place, unauthorized access could result in compromise of confidentiality and integrity of OSA data.
4	Loss of firewall protection.	Computer crime Malicious use System compromise Unauthorized use	Confidentiality and integrity of corporate data.	This system sits at DTO; failure of this firewall can result in increasing the likelihood of other risks being exploited.
5	Internal access to server.	Computer crime Malicious use Unauthorized use	Confidentiality and integrity of corporate data	Loss or theft of data from server could result in compromise of confidentiality and integrity of OSA data.
6	Hardware Issues/Equipment Failure or loss	System Unavailable	Inability to access the system.	Loss of hardware or equipment would result in the entire system or some portion of the system being unavailable.
7	Single Point of Failure	System Unavailable	Inability to access the system.	Loss of any portion of the system would result in the entire system or some portion of the system being unavailable.
8	Poor Systems Administration Practices External to OSA	Computer crime, Malicious use, System compromise, Unauthorized access	Confidentiality and integrity of corporate data.	Poor administration practices could result in compromise of the system and expose OSA data to a risk of loss of availability, confidentiality or integrity.
9	Key Person Dependency	System Unavailable	Inability to adequately support the application.	Loss of key person could result in system downtime if a software issue occurred, or the inability to enhance or maintain this system's functionality.
10	Loss of Critical Documentation, Data or	Computer crime, Malicious use, System	Confidentiality and integrity of corporate data.	Loss of documentation, software or data could result in data compromise and temporary disruption in service, or inability

	Software	compromise, Unauthorized access		to restore services which have been lost.
11	Clear Text Transmission of Critical Data	Computer crime, Malicious use, System compromise, Unauthorized access	Confidentiality and integrity of corporate data.	Capture of clear text data could result in identity theft and /or system access control issues.
12	Data Disclosure	Computer crime, Malicious use, System compromise, Unauthorized access	Confidentiality and integrity of corporate data.	Disclosure of sensitive personal information could result in identity theft and/or system access control issues.
13	Inadequate Customer Practices	Computer crime, Malicious use, System compromise, Unauthorized access	Confidentiality and integrity of corporate data.	Data corruption or loss, or implementation of applications with errors could result from improper or incomplete testing of system or application changes
14	Inadequate Database Support	Computer crime, Malicious use, System compromise, Unauthorized access	Confidentiality and integrity of corporate data, inability to access and recover corporate data.	Data corruption or loss could result from improper or incomplete testing of system changes or system management /monitoring.
15	Inadequate Applications Support	Computer crime, Malicious use, System compromise, Unauthorized access	Inability to adequately support the application.	Data corruption or loss could result from improper or incomplete testing of the application changes.
16	Software Issues from Vendor	Computer crime, Malicious use, System compromise, Unauthorized access	Confidentiality and integrity of corporate data and ability to provide service to the campus.	Software issues caused by the vendor could lead to data corruption or mission critical system disruption or dysfunction.
17	Poor Password Practices	Computer crime, Malicious use, System compromise, Unauthorized access	Confidentiality and integrity of corporate data.	Poor password practices could allow improper system access which could result in data theft, data corruption, application system alteration or disruption.
18	System Compromise	Computer crime, Malicious use, Unauthorized access	Confidentiality and integrity of corporate data.	Compromise system could result in data theft, data corruption, application system alteration or disruption.

19	Lack of Sufficient Operational Policies	Computer crime, Malicious use, System compromise, Unauthorized access	Confidentiality and integrity of corporate data.	Lack of or the improper execution of sufficient operational polices could result in data theft, data corruption, application system alteration or disruption.
20	Poor Physical Security	Computer crime, Malicious use, System compromise, Unauthorized access	Confidentiality and integrity of corporate data.	Poor physical security could allow personal access to staff workstations or Computer Center assets which could result in data theft, data corruption, application system alteration or disruption.
21	Functional Lockout	System unavailability	Inability to access the system.	The inability of staff to access the computing infrastructure or applications could result in the inability to access the system.
22	Environmental Issues	Loss AC or power	Inability to access the system	Environmental issues could result in the inability to access and maintain server hardware.
23	Natural Disaster	Hurricanes, floods, and other weather phenomenon.	Inability to access the system.	Natural disasters could interrupt power to the Computer Center and make it impossible for staff to support the server environment thus disabling access to OSA Information Systems.

Signatures

Submitted by: _____
 Risk Assessment Manager

Date: _____

Reviewed by: _____
 Director of Administration

Date: _____

Approved by: _____
 State Auditor

Date: _____

OSA INFORMATION SECURITY POLICY

XIII. THREAT AND VULNERABILITY MANAGEMENT

A. Vulnerability Assessment

Purpose:

The purpose of the Vulnerability Assessment policy is to establish controls and processes to help identify vulnerabilities within the Office of the State Auditor (OSA) technology infrastructure and information system components which could be exploited by attackers to gain unauthorized access, disrupt business operations, and steal or leak sensitive data.

Policy:

1. Vulnerability Scanning

- The OSA through third party vending with the Supply Chain Information Sharing and Analysis (SCISAC) implements processes to scan for vulnerabilities in information systems and hosted applications at least annually and when new vulnerabilities potentially affecting the information systems / applications are reported.
- The OSA through SCISAC implements a process to control privileged access to vulnerability scanning tools and vulnerability reports.
- The OSA through SCISAC analyzes vulnerability scan reports and results from security control assessments.
- The OSA through SCISAC remediates identified vulnerabilities in accordance with the OSA assessment of risk.

Procedure:

SCISAC uses a vulnerability scanner to assess the OSA information system for weaknesses or vulnerabilities. The OSA is contacted by the Security Operations Center (SOC) of SCISAC once a weakness or vulnerability is detected.

The SCISAC controls access to the vulnerability scanning tools and the resulting reports.

2. Penetration Testing

- The OSA through SCISAC conducts penetration testing exercises on an annual basis.

OSA INFORMATION SECURITY POLICY

XIII. THREAT AND VULNERABILITY MANAGEMENT (CONTINUED)

B. Incident Management

Purpose:

The purpose of the Incident Management policy is to establish controls and processes that provide the OSA information system effective monitoring capability and responsiveness against security threats and incidents. Design and implementation of an incident management framework can secure the information system against known vulnerabilities and threats.

Policy:

1. Incident Response Policy and Procedures

- The OSA through SCISAC develops, documents, and publishes an incident response policy that addresses scope, roles, and responsibilities, internal coordination efforts, and compliance.
- The OSA through SCISAC establishes formal, documented procedures to facilitate the implementation of the incident response policy and associated incident response controls.
- The OSA reviews and updates the incident response policy and procedures on an annual basis.

Procedure:

When a security incident is confirmed by the SOC, SOC sends an email notification to the OSA IT Security Officer, the State Auditor and the Director of Administration. The notification includes preliminary response measures recommended by SOC, which are assigned based on the initial assessment of the incident's severity. The response measures are classified by a tier system numbered 1-5 with 1 being the most severe. The Department of Technology Operation (DTO) is also notified of the incident from SOC. DTO is responsible for looking at the workstation to ensure no further IT Security is compromised and then notifies SOC of its findings.

OSA INFORMATION SECURITY POLICY

XIII. THREAT AND VULNERABILITY MANAGEMENT (CONTINUED)

2. Incident Response Plan

- The OSA develops an incident response plan to:
 - establish a roadmap for implementing incident response capabilities;
 - identifies and documents the requirements of the organization, including mission, size, structure, and functions;
 - define the types of information security incidents to be reported;
 - establish metrics to help ensure incident response capabilities remain effective; and
 - Define resources, such as technology and personnel, required to effectively support incident response capabilities.
- The OSA reviews and updates the incident response plan on an annual basis.

Procedure:

The SOC of SCIASC notifies the OSA of an incident once vulnerability has been detected.

The OSA implements the Division of Information Security's Information Security Response Plan.

Vulnerabilities and weaknesses to the OSA Information System are reported to the OSA and DTO.

SCIASC through SOC ensures that capabilities remain effective through vulnerability scanning and penetration testing.

3. Incident Handling

- The OSA through SCISAC implements formal processes to handle security incidents, including preparation, detection and analysis, containment, eradication, and recovery.
- The OSA through SCISAC implements dynamic response capabilities/tools such as intrusion detection, intrusion prevention systems, and firewalls, among others, to effectively respond to security incidents.

Procedure:

Once the OSA receives notification from SOC of an incident, based on the tier system number, the computer hardware is handled according to the guidelines of the Division of Information Security's Information Security Incident Response Plan. The SOC notifies the OSA of their findings from an incident. The OSA reviews and documents all findings.

OSA INFORMATION SECURITY POLICY

XIII. THREAT AND VULNERABILITY MANAGEMENT (CONTINUED)

4. Incident Monitoring and Reporting

- The OSA through SCISAC establishes a process and tools to maintain detailed records of information security incidents that occur in external (e.g., boundary systems) and internal information systems.
- The OSA implements a policy to require personnel to report suspected information security incidents to the incident response team and/or OSA leadership.

Procedure:

Employees of the OSA are required to report suspected information security incidents to the IT Security Officer.

5. Information System Monitoring

- The OSA through contract with DTO monitors information systems to detect attacks and/or signs of potential attacks, including unauthorized network local or remote connections.
- The OSA through contract with DTO deploys monitoring devices strategically within information technology environment to collect information security events and associated information.
- The OSA through contract with DTO protects information obtained from intrusion-monitoring tools from unauthorized access, modification, and deletion.
- The OSA through contract with DTO monitors inbound and outbound communications traffic to/from the information system for unusual or unauthorized activities or conditions.
- The OSA through contract with DTO heightens the level of information system monitoring activity whenever there is an indication of increased risk to the OSA operations, individuals and assets.

6 Incident Response Training

- The OSA provides incident response training within one (1) month of personnel assuming incident response roles or responsibilities.
- The OSA provides training to incident response personnel upon significant changes to information systems and/or changes to the incident response plan.

OSA INFORMATION SECURITY POLICY

XIII. THREAT AND VULNERABILITY MANAGEMENT (CONTINUED)

7. Incident Response Testing

- The OSA through contract with DTO establishes a formal process to test incident response capabilities on a yearly basis to determine the incident response effectiveness and adequacy.
- The OSA through contract with DTO documents the incident response test results and update incident response processes as applicable.

8. Malicious Code Protection

- The OSA through contract with DTO employs malicious code protection mechanisms at information system entry and exit points to detect and eradicate malicious code.
- The OSA through contract with DTO implements a process to help ensure malicious code protection mechanisms are updated whenever new releases are available.
- The OSA through contract with DTO configures malicious code protection mechanisms to perform periodic scans at defined time intervals.
- The OSA through contract with DTO blocks malicious code and sends an alert to information system/networks administrator and initiate action(s) in response to malicious code detection.

OSA INFORMATION SECURITY POLICY

XIII. THREAT AND VULNERABILITY MANAGEMENT (CONTINUED)

C. Patch Management

Purpose:

The purpose of the Patch Management policy is to identify controls and processes that will provide appropriate protection against threats that could adversely affect the security of the information system or data entrusted on the information system. Effective implementation of these controls will create a consistently configured environment that is secure against known vulnerabilities in operating system and application software.

Policy:

1. Flaw Remediation

- The OSA through contract with DTO develops and implements a process to identify, report, and correct information system flaws.
- The OSA through contract with DTO establishes a formal process to test software and firmware updates related to flaw remediation for effectiveness and identification of potential impact prior to implementation.
- The OSA through contract with DTO installs latest stable versions of applicable security software and firmware updates.
- The OSA through contract with DTO establishes a patch cycle that guides the normal application of patches and updates to systems.
- The OSA establishes a process of patch testing to verify the source and integrity of the patch and ensure testing in a production mirrored environment for a smooth and predictable patch roll out.

Procedure:

Patch Management is handled through contract with DTO.