.

:

Enterprise Information Security Policy

State of Tennessee
Department of Finance and Administration
Strategic Technology Solutions
Information Security Program

Document Version 2.5 – August 2, 2021

Table of Contents

1. EXECUTIVE SUMMARY

The main purpose of this document is to define the information security policy of the State of Tennessee along with the organization and framework/structure required to communicate, implement, and support this policy. Information is an asset, which like any other asset owned by the State of Tennessee, has significant value to the stakeholders of the State. Information security is a critical component that is required to enable and ensure the confidentiality, integrity and availability of data, network and processing resources required for the State of Tennessee to perform its business and operational practices. This policy document has been created to establish and uphold the minimum requirements that are necessary to protect Information Technology (IT) resources (assets) against unavailability, unauthorized or unintentional access, modification, destruction, or disclosure as set forth by the Information Systems Council (ISC) of the State of Tennessee.

The scope of this document is intended to cover any information asset owned, leased, or controlled by, or operated on behalf of the State of Tennessee. The methodologies and practices of external entities that require access to the State of Tennessee's IT resources may be impacted and could be included in this scope. This document seeks to protect:

- All desktop computing systems, servers, data storage devices, communication systems, firewalls, routers, switches, and mobile devices (computing platforms) owned by the State of Tennessee where lawfully permitted.
- All computing platforms, operating system software, middleware, or application software under the control of third parties that connect in any way to the State of Tennessee's enterprise computing or telecommunications network.
- All data, information, knowledge, documents, presentations, databases, or other information resource stored on the State of Tennessee's computing platforms and/or transferred by the State's enterprise network.
- All data, information, knowledge, documents, presentations, databases, or other information resource stored on contractor computing platforms and/or transferred over contractor network infrastructure.

This document applies to all full- and part-time employees of the State of Tennessee, all third parties, outsourced employees or vendors who work on State premises or remotely connect their computing platforms to the State of Tennessee's computing platforms and any cloud provider storing, processing, or transmitting State data.

By establishing the appropriate policy framework and utilizing a documented policy development process that includes all stakeholders, the State envisions maximum voluntary compliance. The policy development and implementation process includes an impact analysis, input from Agency IT professionals and approval by the Chief Information Security Officer (CISO) and Policy Review Committee within Strategic Technology Solutions (STS), Department of Finance and Administration.

All IT resources and any information system owned by the State of Tennessee should be protected from unauthorized disclosure, use, modification or destruction in a manner commensurate with their value, sensitivity and criticality to the business and operation of the State government and those they serve. Access to information technology assets will be granted using the principle of least privilege which restricts the access privileges of authorized individuals to the minimum necessary to perform their role.

All approved policies will support the guidelines established by the Information Systems Council of the State of Tennessee.

2. INTRODUCTION

The Information Security Challenge

IT solutions are driven by the demands of our daily business activities. The ability to procure efficient communication, IT resources and technologies that support business processes at a low cost is a foundational component of successful IT programs. Cloud technologies and offerings continue to grow, and this integration moves quickly to align itself with the "just in time" requirements of the business. Given the growth demands of the business along with the associated time sensitive integration strategies, we are presented with new risks at every turn. Organizations will frequently take risks in order to meet those time sensitive business requirements, sometimes bypassing existing processes to meet time demands of the customers whom they serve. As the State expands its use of cloud technologies, it is incumbent upon the State to ensure the State data that is hosted or processed in cloud environments or is transmitted across cloud infrastructure receives protection similar to what is provided by the STS managed data centers and infrastructure. This practice, also known as risk management, is a component of any successful business. Modern enterprises will implement risk management and/or information security programs to mitigate these risks.

The State of Tennessee has recognized the need to evaluate risk and has established information security programs. One of the main goals of any successful information security program is to protect the organization's revenues, resources, and reputation. This is accomplished through several means. Some examples are implementing risk management methodologies, security architectures, control frameworks and security policy.

Security policies are a foundational component of any successful security program. The Enterprise Information Security Policy for the State of Tennessee is based on the International Standards Organization (ISO) 27000 series standard framework. This policy is designed to comply with applicable statutes and regulations; however, if there is a conflict, applicable statutes and regulations will take precedence. This policy defines the minimum requirements for providing a secure operational environment.

Scope (2.1)

The scope of this document is intended to cover any information asset owned, leased or controlled by the State of Tennessee and the methodologies and practices of the State of Tennessee as well as external entities that require access to the State of Tennessee's IT resources. This document seeks to protect:

- All desktop computing systems, servers, data storage devices, communication systems, firewalls, routers, switches and mobile devices (computing platforms) controlled by or operated on behalf of the State of Tennessee where lawfully permitted.
- All computing platforms, operating system software, middleware or application software under the control of the State of Tennessee, or by third parties, operated on behalf of the State of Tennessee that connect in any way to the State's enterprise computing or telecommunications network or any State Cloud Tennant.
- All data, information, knowledge, documents, presentations, databases or other information resource stored on the State of Tennessee's computing platforms and/or transferred by the State's enterprise network.
- All data, information, knowledge, documents, presentations, databases or other information resource stored on contractor computing platforms and/or transferred over contractor network infrastructure.

All full- and part-time employees of the State of Tennessee, all third parties, outsourced employees, or vendors who work on state premises or remotely connect their computing platforms to the State of Tennessee's computing platforms and any cloud provider storing, processing or transmitting State data should adhere to the policies and requirements set forth in this document.

Authority (2.2)

The ISC authorized the Department of Finance and Administration, STS to establish and enforce enterprise policies and standards related to information security. These policies and standards include, but are not limited to, network and Internet access, any computing platform attached to the State's enterprise network and any wired or wireless technology attached to the State's enterprise network. STS is responsible and authorized by the ISC to perform audits on any device that attaches to the State of Tennessee's enterprise network.

References:

Tennessee Code Annotated, Section 4-3-5501, et seq., effective May 10, 1994 [Acts 1994, ch. 992, § 2; 1995, ch. 305, § 66] 1994
ISC Information Resource Policies, Policy 1.00 (Data Security)
ISC Information Resource Policies, Policy 5.00 (Information Systems Management and System Development Life Cycle)
ISC Information Resource Policies, Policy 9.00 (Disaster Recovery)
ISC Information Resource Policies, Policy 13.00 (Network Infrastructure Support and Maintenance)

Exceptions (2.3)

All exceptions to any security policy will be reviewed, evaluated and processed by a member of the CISO's staff. Some exceptions may also require signature of agency head to acknowledge and/or accept associated risks.

Review (2.4)

Review of this document takes place within the STS Policy Review Committee sessions and will occur on an annual (within every three hundred and sixty-five (365) days) basis at a minimum. Document review can also be requested by sending a request to the CISO.

The official policy document and supporting documentation will be published on the STS intranet site located at:

https://www.teamtn.gov/sts/policies-and-procedures.html

Document Format (2.5)

This document generally follows the International Standards Organization 27000 series standard framework for information technology security management. Each section starts with a high-level security control category followed by the control objective. Policy statements follow the objectives.

The MINIMUM COMPLIANCE REQUIREMENTS category contains the minimum requirements for compliance criteria that are global and apply to all systems or platforms across the entire enterprise.

X. Section Name

Control Category (x.x)
Objective Statement

Policy Name (x.x.x)
Policy Statement

Sub-Policy Name (x.x.x.x)
Sub-Policy Statement

MINIMUM COMPLIANCE REQUIREMENTS:

Policy Maintenance (2.6)
All policies will be maintained in accordance with the STS policy process documentation.

3. INFORMATION SECURITY

Management Direction for Information Security (3.1)

Objective: To provide management direction and support for information security in accordance with agency business requirements and relevant state and federal statute and regulations for the State of Tennessee's computing environments.

Information Security (3.1.1)

STS Information Security Management will initiate, control and communicate an enterprise information security architecture that includes, but is not limited to, a policy framework, an organizational and communication framework and a security technology framework.

Agency Policies for Information Security (3.1.2)

Agencies should develop and communicate agency specific policy documents as required by agency or regulatory requirements provided the minimum requirements set forth in this document are met.

4. OPERATIONS SECURITY

Operational Procedures and Responsibilities (4.1)

Objective: To protect critical State information resource assets, including hardware, software and data from unauthorized use, misuse, or destruction to ensure correct and proper operations.

Documented Operating Procedures (4.1.1)

All agencies of the State of Tennessee and vendors or outsourced employees acting on behalf of the State should identify, document and maintain standard security operating procedures and configurations for their respective operating environments and ensure the documentation is available to all users who need it.

Change Management (4.1.2)

Changes to information processing facilities and systems should be controlled and monitored for security compliance. Formal management responsibilities and procedures should exist to ensure satisfactory control of all changes to equipment, software, applications, configurations and/or procedures that affect the State of Tennessee's operational environment. All documentation generated by the change control policies and procedures should be retained as evidence of compliance.

Change Control Procedures (4.1.2.1)

Change control procedures should include authorization, risk assessment, logging, auditability, and roll back procedures.

Capacity Management (4.1.3)

The use of IT resources should be monitored and tuned so that projections of future capacity requirements can be made.

Separation of Development, Testing and Operational Environments (4.1.4)

Development and testing environments should be segregated from production environments in order to reduce the risks of unauthorized access or changes to the production environment. Data classified as confidential must be protected from unauthorized disclosure, use, modification or destruction and should not be used in development or test environments.

Protection from Malware (4.2)

Objective: Prevent the automated propagation of malicious code and contamination of environments attached to the enterprise network.

Malicious Software Control (4.2.1)

All computing platforms that are attached to the State's enterprise technology infrastructure or operated on behalf of the State should be protected from intentional or unintentional exposure to malicious software. Malicious software includes, but is not limited to, software viruses, worms, Trojan horses, logic bombs and rootkits. Compromised systems should be removed from the operational environment. All computing platforms that are attached to the State's enterprise technology infrastructure will participate in the State's enterprise antivirus program if antivirus signatures are available for the computing platforms. STS Security Management reserves the right to seize any compromised system for forensic analysis.

Backup (4.3)

Objective: To prevent loss of data and to ensure data availability.

Data Backup (4.3.1)

Backup copies of data, software and system images should be taken and tested regularly in accordance with established procedures. A copy of the backup data should be stored off-site according to applicable regulatory requirements and State policy. Results of restore tests should be furnished to data owners with recommendations for any remedial steps found. Data owners should approve any remedial plans and timelines for implementing those remediation steps within a reasonable period not to exceed three months. Following remediation, the restore testing should be repeated and results documented to ensure that those steps mitigated all identified issues.

Logging and Monitoring (4.4)

Objective: To record events and generate evidence.

Event Logging (4.4.1)

All systems should be configured to support security event logging, recording user activities, exceptions, faults and information security events. System administrators should monitor and report inappropriate access to the STS Customer Care Center. Critical systems should be configured to support automated logging to a facility that protects the integrity of the logs. Logging levels and monitored elements will be configured in accordance with federal and state statute and regulatory requirements.

Availability and Performance Monitoring (4.4.2)

Critical systems should be configured to support State approved automated monitoring of system availability and performance.

Protection of Log Information (4.4.3)

Logging facilities and log information should be protected against tampering and unauthorized access.

Administrator and Logs (4.4.4)

System administrator activities should be logged and the logs protected and regularly reviewed.

Clock Synchronization (4.4.5)

Approved State of Tennessee managed enterprise network time servers should be the only State devices permitted to synchronize with external time services. All State provided or managed systems will synchronize time with approved State of Tennessee managed enterprise network time servers. All non-State provided or managed systems storing, processing or transmitting State data should be synchronized to State approved time synchronization services.

Control of Operational Software (4.5)

Objective: To ensure the integrity of operational systems.

Installation of Software on Operational Systems (4.5.1)

Only software that has been licensed and approved as a State standard software product or that has been approved as an exception through the State's architecture standards approval process should be installed on devices covered by the software's license agreement.

Patch Management (4.5.1.1)

All applications and processing devices that are attached to the State's enterprise technology infrastructure will have critical security related application, operating system, and/or security related patches made available by the software or hardware vendor applied within 90 calendar days or sooner if an acceptable date can be agreed upon by all affected parties. Emergency patches and updates will be applied as soon as possible following successful validation and testing.

Patch schedule:

- 14 days for critical patches addressing known exploits
- 30 days for high patches addressing known exploits
- 90 days for critical patches
- 90 days for high patches

Software Maintenance (4.5.1.2)

Servers and workstation computing devices should have defined maintenance windows within every 90 days.

Appliances should have established review and maintenance cycles for software updates.

Software Development Code (4.5.1.3)

Software development code cannot be installed on production systems (i.e. non-compiled software programming code).

Review of Application and Operating System Changes (4.5.1.4)

Applications and operating systems should be reviewed and tested to ensure that there is no adverse impact on operations or security when a change has been performed on the operating system. (e.g. patch).

Technical and Vulnerability Management (4.6)
Objective: To prevent the exploitation of technical vulnerabilities.

Management of Technical Vulnerabilities (4.6.1)

Information about technical vulnerabilities on information systems and supporting infrastructure should be obtained in a timely fashion, evaluated for exposure and risk to the State and appropriate measures implemented to address the associated risk.

Restrictions on Software Installation (4.6.2)

Users should not install software that has not been approved by STS and their agency.

Information Systems Audit Considerations (4.7)
Objective: To minimize the impact of audit activities on operational systems.

Information Systems Audit Controls (4.7.1)

Audit requirements and activities involving verification of operational systems should be carefully planned and agreed upon in advance to minimize disruptions to business processes.

5. ACCESS CONTROL

Business Requirements of Access Control (5.1)

Objective: To limit access to information and information processing facilities.

Access Control (5.1.1)

All access rules and requirements to access the State of Tennessee's IT resources should be developed, documented, and maintained by their respective resource owners. Access to the State of Tennessee's IT resources will be granted consistent with the concept of least privilege. All information processing systems owned by or operated on behalf of the State of Tennessee should have an appropriate role-based access control system that ensures only legitimate users and/or systems have access to IT resources that they are explicitly authorized to use.

Access to Networks and Network Services (5.1.2)

All access and connectivity to the State of Tennessee's enterprise network or networks operated on behalf of the State should be granted consistent with the concept of least privilege. Users will only be provided with access to the network and network resources that they have been specifically authorized to use.

Remote Access (5.1.2.1)

All users who are accessing the State's internal network should access those resources through a State approved multifactor Virtual Private Network (VPN) solution. All users who access State data on networks operated on behalf of the State should use secure connection methods. Remote desktop protocol (RDP) and VPN connections are prohibited from personally owned devices.

Information Security Roles and Responsibilities (5.1.3)

All information security responsibilities should be defined and assigned by the access granting authority.

Segregation of Duties (5.1.4)

Where appropriate, conflicting duties and areas of responsibility should be segregated and assigned to different individuals to reduce opportunities for unauthorized or unintentional modification or misuse of the State's assets.

User Access Management (5.2)

Objective: To ensure authorized user access and to prevent unauthorized access to systems and services.

User Registration and De-Registration (5.2.1)

A formal user registration and de-registration process should be implemented to enable assignment of access rights and to adjust those rights as the user's role changes.

User Access Provisioning (5.2.2)

User access to IT resources should be authorized and provisioned according to the Agency's employee provisioning process.

User Account Naming (5.2.2.1)

All State user accounts will follow a State approved standardized naming convention.

Management of Privileged Access Rights (5.2.3)

Users should have the least privileges required to perform their roles as identified and approved by their management. The allocation and use of privileged access rights should be restricted and controlled.

Management of Secret Authentication of Information Users (5.2.4)

The allocation of secret authentication information should be controlled through a formal management process.

Review of User Access Rights (5.2.5)

A user's access rights should be reviewed, validated and updated for appropriate access by their section supervisor on a regular basis or whenever the user's access requirements change (e.g. hire, promotion, demotion, and transfers within and between agencies).

Removal or Adjustment of Access Rights (5.2.6)

All access rights for employees and external entities to information and information processing facilities should be revoked upon termination of their employment, contract, agreement or change of agency by the close of business on the user's last working day or within 24 hours of notification of the user's death, determination of job abandonment or retroactive notification of resignation or retirement.

In the event the user is retiring and returning as a 120 Day Appointment within 45 days of the last working day, the user's account is exempt from the revocation requirement stated above.

Procedures for emergency removal of access rights should be in place.

User Responsibilities (5.3)

Objective: To make users accountable for safeguarding their authentication information.

Use of Secret Authentication Information (5.3.1)

Users should follow State policy in the use of secret authentication information.

System and Application Access Control (5.4)

Objective: To prevent unauthorized access to systems and applications.

Information Access Restriction (5.4.1)

Access to information and application system function should be restricted in accordance with the defined access control policy.

Secure Log-on Procedures (5.4.2)

Where required by the access control policy, access to systems and application should be controlled by a secure log-on procedure. At a minimum, user access to protected IT resources requires the utilization of User Identification (User ID) and password that uniquely identifies the user. Sharing access credentials intended to authenticate and authorize a single user between any two or more individuals is prohibited.

System Administrator Access (5.4.2.1)

All systems administrators or users with elevated privileges using administrative tools or protocols to access servers located in State managed data processing facilities or facilities

operated on behalf of the State must use a multifactor VPN solution to obtain access.

Logon Banner (5.4.2.2)

All systems and devices owned and operated by or on behalf of the State of Tennessee must display the State approved logon banner before the user is able to log in.

Service Account Use (5.4.2.3)

Service accounts should be unique to each application and/or system and should only be used to authenticate systems and/or applications to specific services.

System/Application Account Use (5.4.2.4)

System/application accounts are created upon installation of an application and may have a predetermined User ID. Privileged User access to system accounts must be approved and documented. A system/application account differs from a service account in that individuals may know the password to the system/application account. This account must be elevated to from a lesser account, e.g. using the run as administrator function in Windows or using sudo in Linux.

An example of this type of account is the default administrative account required by the application.

System Administrator Account Use (5.4.2.5)

System Administrator accounts have elevated privileges and should only be used when elevated privileges are required. Administrative accounts are used to administer operating systems and applications.

Password Management System (5.4.3)

Password management systems, such as Active Directory services, should be interactive and should ensure quality passwords.

Use of Privileged Utility Programs (5.4.4)

The use of utility programs that might be capable of overriding system and application controls should be restricted and tightly controlled.

Access Control to Program Source Code (5.4.5)

Access to program source code should be restricted to authorized users.

Default Configurations (5.4.6)

All applications and processing devices that are attached to the State's enterprise technology infrastructure should be deployed with modified configurations including, but not limited to, default accounts, and/or installation paths to minimize the use of default settings to gain unauthorized use, modification or destruction.

MINIMUM REQUIREMENTS:

Password Management (5.4.3)

- All user and system administrator passwords must contain a minimum of eight (8) characters.
- All service account and system/application account passwords must contain a minimum of fifteen (15) characters, and these passwords may be non-expiring.
- All passwords must include a character from each of the following four categories.
    - Uppercase characters of European languages (A through Z, with diacritic marks, Greek and Cyrillic characters)
    - Lowercase characters of European languages (a through z, sharp-s, with diacritic marks, Greek and Cyrillic characters)
    - Base 10 digits (0 through 9)
    - Non-alphanumeric characters: ~!@#$%^&*_-+=`|\(){}[]:;"'<>,.?/, including any Unicode character that is categorized as an alphabetic character but is not uppercase or lowercase. This includes Unicode characters from Asian languages.
- Temporary or default passwords assigned by system administrators or dictated by the operating system must be changed immediately after initial login.
- Passwords must be changed every 90 days or less from the last change. Shared system administrator passwords must be changed when an individual who has access to the passwords leaves.
- All systems that support password history will be configured to remember a password history of 4 at a minimum.

- All passwords should be hashed and salted.
- User ID's will be revoked after five (5) consecutive attempts to login with an invalid password.
- All service account and system/application account passwords must be changed when an individual who has had access to the passwords is terminated or accepts a role where knowledge of those passwords is no longer required.
- Service and system/application accounts should be approved for use and documented in the area where the account is being used.

6. ASSET MANAGEMENT

Responsibility for Assets (6.1)

Objective: To identify organizational assets and define appropriate protection responsibilities.

Inventory of Assets (6.1.1)

Assets associated with information and information processing facilities should be identified and an inventory of these assets should be created and maintained in order to protect the assets in accordance with Department of Finance and Administration Policy 32 Maintaining Control Over Items That Are Not Capitalized.

Ownership of Assets (6.1.2)

All information resource assets listed in the asset inventory should have an assigned owner or entity who will ensure the assets are protected in a manner consistent with their value, sensitivity and criticality to the business and operation of the State's government and those it serves or as specified by any superseding state or federal statute or regulation**.**

Acceptable Use of Assets (6.1.3)

Rules for the acceptable use of information and assets associated with information and information processing facilities should be identified, documented, implemented and communicated to the employees and outsourced employees who have access to those assets.

Return of Assets (6.1.4)

All employees and outsourced employees must return all state assets in their possession upon termination of their employment or contract**.**

Asset Identification (6.1.5)

All state hardware assets will be named in accordance with the State approved standardized naming convention.

Data Classification (6.2)

Objective: To ensure the data used and managed by the State receives an appropriate level of protection commensurate with the value, importance and criticality of the data to the State.

Classification of Data (6.2.1)

Data assets owned and/or managed by the State of Tennessee should be classified according to the definition of "Personal Information" or "Confidential Records" as specified by applicable state and/or federal statute or regulations to indicate the need, priorities and degree of protection it will receive. At a minimum, data will be classified as Public or Confidential.

Labelling of Data (6.2.2)

An appropriate set of procedures for labeling data assets owned and/or managed by the State of Tennessee should be developed and implemented in accordance with the State's data classification scheme.

Handling and Use of Data (6.2.3)

Procedures for handling data assets should be developed and implemented in accordance with the data classification scheme adopted by the State.

Public Data Classification and Control (6.2.3.1)

Data classified as public should be protected from unauthorized modification or destruction.

Confidential Data Classification and Control (6.2.3.2)

Data classified as confidential must be protected from unauthorized disclosure, use, modification or destruction and cannot be used in development or test environments or publicly disclosed. Controls should be applied to data in a manner consistent with its value, sensitivity and criticality to the business and operation of state government. Data classified as confidential must be encrypted at rest and during transmission in accordance with applicable state or federal statute or regulatory requirements.

Confidential Data on Personally Owned Devices (6.2.3.3)

Confidential data should not be stored on personally owned computing platforms or on personally owned mobile computing platforms unless managed by the State's mobile device management solution or the State's enterprise configuration manager.

Confidential Electronic Messages Classification and Control (6.2.3.4)

E-mail sent from the State's domain out through the public Internet must be encrypted if it contains confidential information in the body or attachment. Confidential information should not be placed into the subject line of the message.

Payment Card Information Classification and Control (6.2.3.5)

Payment card information must be considered confidential when an individual's first name or first initial and last name are present in combination with account number, credit or debit card number, required security code, access code, or password that would permit access to an individual's financial account.

https://www.pcisecuritystandards.org/pci_security/

The Payment Card Industry – Data Security Standards (PCI DSS) comprise a minimum set of requirements for protecting cardholder data and may be enhanced by additional controls and practices to further mitigate risks, as well as local, regional and sector statutes and regulations. Additionally, legislation or regulatory requirements may require specific protection of personally identifiable information or other data elements (for example, cardholder name). PCI DSS does not supersede local or regional statutes, government regulations, or other legal requirements.

All payment card information stored and processed by the State or transmitted over State networks must be in compliance with the PCI-DSS. Storage of the full Primary Account Number (PAN) on State systems is prohibited. Agencies that use payment card services should also comply with statewide accounting policies as documented by the Department of Finance and Administration, Division of Accounts.

All purchased (off the shelf) applications used to process payment card information must be compliant with the Payment Application Data Security Standard (PA-DSS).

Use of Confidential Data (6.2.3.6)

The use of confidential data will only be permitted in production systems. The use of confidential data is prohibited from training, test, and development systems.

To reduce the risk of accidental change or unauthorized access to operational software and business data, there should be a separation of duties based on development, test, and operational facilities. Confidential data should not be copied into test and development systems. Development and test environments should not be directly connected to production environments. Data and operational software test systems should emulate production systems as closely as possible.

Media Handling (6.3)

Objective: To prevent unauthorized disclosure, modification, removal or destruction of data stored on media.

Management of Removable Media (6.3.1)

Procedures should be implemented for the management of removable media in accordance with the classification scheme adopted by the organization.

Repair of Removable Media (6.3.1.1)

Removable media should be sanitized prior to removing it from State facilities for maintenance or repair.

Disposal of Removable Media (6.3.2)

Removable media should be disposed of securely when no longer required, using approved State procedures.

Physical Transfer of Removable Media (6.3.3)

Removable media containing sensitive or confidential data must be protected against unauthorized access, misuse or corruption during transport.

Workstation Computing (6.4)

Objective: To prevent unauthorized disclosure, modification, removal or destruction of data stored on user assigned processing devices.

State Provided Workstation Computing Platforms (6.4.1)

Workstation computing platforms, including laptops should be physically protected against theft when left unattended. Workstation computing platforms should not store confidential data assets where it is not absolutely necessary to perform the specific job-related duties. Storage of confidential data assets on a workstation computing platform should have approval from the asset custodian for such storage. Confidential data assets which have been authorized to be stored on the local workstation should be encrypted while stored on the workstation computing platform.

Workstation Platform Reassignment (6.4.2)

All workstation computing platforms, including all external storage devices, should be sanitized prior to being re-issued or re-purposed to another employee or outsourced employee.

Workstation Platform Disposal (6.4.3)

Hard drives in workstation computing platforms, including all mobile storage devices and phones, should be sanitized using approved sanitization procedures or destroyed prior to transfer or surplus of processing device to non-State agencies.

Sanitization services provided by third parties must meet the State's media sanitization guidelines, and the provider should provide proof of sanitization.

Cloud Services (6.4.4)

Agencies and full- and part-time employees of the State of Tennessee and all third parties, outsourced employees, or vendors who are acting on behalf of the State who use cloud services for State business should seek STS guidance and approval for proposed cloud solutions prior to enabling cloud services.

Cloud Services Procurement (6.4.4.1)

Agencies that procure cloud services that host or process State data must include security language approved by the Department of General Services, Central Procurement Office. Agencies should use legally binding documents to procure those services.

https://www.teamtn.gov/cpo/resources.html

7. PHYSICAL AND ENVIRONMENTAL SECURITY

Secure Areas (7.1)

Objective: To prevent unauthorized physical access, damage and interference to the State's information and information processing facilities.

Physical Security Perimeter (7.1.1)

All enterprise data processing facilities that process or store data classified as critical or sensitive should have multiple layers of physical security. Each layer should be independent and separate of the preceding and/or following layer(s).

All other processing facilities should have, at a minimum, a single security perimeter protecting it from unauthorized access, damage and/or interference.

Physical Entry Controls (7.1.2)

Secure areas should be protected by appropriate entry controls to restrict access only to authorized personnel.

Securing Offices, Rooms and Facilities (7.1.3)

Physical security for offices, rooms and facilities should be designed and applied commensurate with the classification and value of the data being handled or processed.

Protecting against External and Environmental Threats (7.1.4)

Physical protection against natural disaster, malicious attack or accidents should be considered and incorporated in facility design, construction and placement.

Working in Secure Areas (7.1.5)

Procedures for working in secure areas should be created and implemented.

Delivery and Loading Areas (7.1.6)

Access points such as delivery and loading areas and other points where unauthorized persons could enter the premises should be controlled, and if possible, isolated from information processing facilities.

Equipment (7.2)

Objective: To prevent loss, damage, theft or compromise of assets or an interruption to State operations.

Equipment Siting and Protection (7.2.1)

Equipment should be located in secured areas or protected to reduce the risks from environment threats and hazards, and to reduce the opportunities for unauthorized access. Equipment located in areas where the State of Tennessee is unable to maintain a secure perimeter should be locked in a secured manner with access controlled by the State of Tennessee. Secured cabinets or facilities should support further segregation within the State of Tennessee's IT organization based on role and responsibility.

Supporting Utilities (7.2.2)

Infrastructure and related computing equipment should be protected from power failures and other disruptions by failures in supporting utilities.

Cabling Security (7.2.3)

Power and telecommunications cable carrying data or supporting information services should be protected from interception, interference or damage.

Equipment Maintenance (7.2.4)

Equipment should be correctly maintained to ensure its continued availability and integrity.

Removal of Assets (7.2.5)

All equipment, software or information that is a part of State operational systems or processes should not be taken off-site without the prior authorization from executive management or a designated representative and should be removed according to documented agency equipment transfer procedures.

Security of Equipment and Assets Off-Premises (7.2.6)

Security should be applied to off-site assets taking into account the different risks of working outside the organization's premises.

Secure Disposal or Re-Use of Data Processing Equipment (7.2.7)

All data processing equipment including storage devices subject to transfer or reuse should be sanitized in accordance with the State of Tennessee's media reuse procedure or superseding state or federal requirements. Data processing equipment assets that are not subject to transfer or reuse should be destroyed in accordance with the State of Tennessee's media disposal procedures or in accordance with superseding state or federal requirements.

Unattended User Equipment (7.2.8)

Users should ensure that unattended data processing equipment has appropriate protection.

Session Time Outs (7.2.8.1)

All systems and devices owned and operated by or on behalf of the State of Tennessee should be configured to clear and lock the screen or log the user off the system after a defined period of inactivity.

Clear Desk and Clear Screen (7.2.9)

All data classified as confidential must be stored in a locked cabinet or room when unattended. All data processing equipment that provide access to Information Processing Systems will be configured so that a screen-saver, with password protection engaged, or other lock-down mechanism that prevents unauthorized viewing of screen information or unauthorized access to the system will automatically be implemented if the system has been left unattended.

All computing platforms residing in non-secured facilities with attached displays should be oriented away from direct line of sight from unauthorized viewers.

MINIMUM COMPLIANCE REQUIREMENTS:

(7.2.8.1) Session Time Outs
Sessions will be configured to time out after 15 minutes of inactivity.

(7.2.9) Clear Screen
Maximum inactivity interval for engaging screen-saver or other lockdown mechanism is 15 minutes.

8. NETWORK CONNECTIVITY SECURITY

Network Security Management (8.1)

Objective: To ensure the protection of the State's assets that are accessible by suppliers and vendors.

Network Controls (8.1.1)

Networks should be managed and controlled to protect information in systems and applications.

Security of Network Services (8.1.2)

Security mechanisms, service levels and management requirements of all network services should be identified and included in network services agreements, whether these services are provided in-house or outsourced.

Segregation in Networks (8.1.3)

All enterprise network architectures operated by, or on behalf of, the State of Tennessee should be designed to support, at a minimum, separate public, "demilitarized" and private security zones based on role, risk and sensitivity. Bridging between separate security zones is strictly prohibited. All access between separate security zones should be controlled by a security mechanism configured to deny all access by default unless explicitly authorized and approved by the STS Security Management Team.

Information Transfer (8.2)

Objective: To maintain the security of information transferred within network infrastructures managed by on behalf of the State and with any external entity.

Information Transfer (8.2.1)

Formal transfer policies, procedures and controls should be in place to protect the transfer of information through the use of all types of communication facilities.

Agreements on Data Transfer (8.2.2)

Agreements should address the secure transfer of business information between the State and external parties.

Electronic Messaging (8.2.3)

Data involved in electronic messaging should be appropriately protected.

Internal Electronic Messages Control (8.2.3.1)

Email and instant messages internal to the State's domain containing confidential data should be encrypted during transmission. Confidential information should not be placed into the subject line of email or as any part of instant messages.

External Electronic Messages Control (8.2.3.2)

E-mail sent through the public Internet must be encrypted if it contains confidential information in the body or attachment of the email. Confidential information should not be placed into the subject line of the message.

Electronic Messaging Management (8.2.3.3)

All electronic messages created, sent or received in conjunction with the transaction of official business should use the State approved gateway(s) to communicate via the Internet.

Confidentiality or Non-Disclosure Agreements (8.2.4)

When exchanging or sharing information classified as "Sensitive" or "Confidential" with external parties that are not already bound by the contract confidentiality clause, a non-disclosure agreement should be established between the owner of the data and the external party.

Note: Agencies should work with agency legal counsel to ensure proper language is used.

9. MOBILE DEVICE SECURITY

Mobile Devices and Alternate Workplace Solutions (AWS) (9.1)

Objective: To extend the State's security posture to the mobile workforce.

Mobile Device (9.1.1)

All mobile devices that connect to State of Tennessee managed data or infrastructure should be managed by the State's enterprise mobile device management solution or the State's enterprise configuration manager and should comply with appropriate mobile device usage policies as required by state or federal statute or regulation.

Alternate Workplace Solutions (9.1.2)

AWS workers should comply with the appropriate AWS policies as required by state or federal statute, regulation, or state or agency policy.

10. EXTERNAL PARTY SECURITY

Information Security for External Party Relationships (10.1)

Objective: To ensure the protection of the State's assets that are accessed, processed, communicated to, or managed by external parties, suppliers or vendors. This includes any external party who has access to physical data processing facilities, logical access to State data processing systems via local or remote access or access via another external party into the State's data processing facilities.

Information Security for External Party Relationships (10.1.1)

Information and physical security requirements for mitigating the risks associated with supplier or vendor access to the State's assets should be agreed upon in writing with the external party. All external parties must agree in writing to comply with all applicable information security policies, confidentiality agreements, third party connectivity agreements, executive orders, standards, controls and regulations.

Identification of Risk (10.1.2)

Risk involving external parties should be identified and proper controls implemented prior to the granting of access to any State of Tennessee information, information technology asset or information process facility.

Addressing Security within External Party Agreements (10.1.3)

All relevant information security requirements should be established and agreed upon with each supplier or vendor that may access, process, store, communicate, or provide IT infrastructure components for the State's processing systems or infrastructure.

Reporting of Security Incidents (10.1.3.1)

External Party Agreements will require external parties to report perceived security incidents that may impact the confidentiality, integrity or availability of State data immediately.

Sub-Contractor Requirements (10.1.3.2)

Primary external parties should require their sub-contractors to abide by State of Tennessee policies and security requirements, as applicable.

Addressing Security for Access to Citizen Data (10.1.4)

Risk involving external party access to citizen data should be identified and proper controls implemented prior to the granting of access to any State of Tennessee citizen data. Appropriate controls should be agreed upon, documented in external party agreements and implemented prior to the granting of access to any citizen data.

11. SYSTEM ACQUISITION, DEVELOPMENT AND MAINTENANCE

Security Requirements of Information Systems (11.1)

Objective: To ensure that information security is an integral part of information systems throughout their life cycle. This includes application infrastructure, vendor applications, agency-developed, and user-developed applications and information systems which provide services over public networks or the State's internal network.

Security Requirements of Information Systems (11.1.1)

Security requirements should be identified and documented as part of the overall business case for new information systems and for enhancement to existing information systems and should be included early and continuously throughout the lifecycle of the application, including, but not limited to the conception, design, development, testing, implementation, maintenance and disposal phases.

Securing Application Services on Public Networks (11.1.2)

Information involved in application services passing over public networks should be protected from fraudulent activity and unauthorized disclosure or modification.

Protecting Application Services Transactions (11.1.3)

Information involved in application service transactions should be protected to prevent incomplete transmission, misrouting, unauthorized message alteration, unauthorized disclosure, unauthorized message duplication or replay.

Information Security in Project Management (11.1.4)

Information security should be addressed at project initiation and throughout the lifecycle of the project.

Security in Development and Support Processes (11.2)

Objective: To ensure that information security is designed and implemented within the development lifecycle of information systems.

Security Requirements of Information Systems (11.2.1)

Requirements, rules and guidelines for the development of software and systems should be established and applied to all systems development.

Security in Application Systems Development (11.2.1.1)

Input validation, authentication, and authorization should be included in the design, development and implementation of applications.

Input and Data Validation (11.2.1.2)

Applications should not pass raw input to other processes including, but not limited to, other applications, web services, application server and databases. Applications should use parameterized queries or stored procedures, not dynamic SQL statements.

Output Data Validation (11.2.1.3)

Applications should not echo input back to the user or disclose information about the underlying system through error messages.

Application Authorization (11.2.1.4)

Applications that provide access to information in databases or from network shares should perform user authentication.

Inter-process Message Authentication (11.2.1.5)

Inter-process message authentication should be used to verify that a message originated from a trusted source and that the message has not been altered during transmission.

Control of Internal Processing (11.2.1.6)

Security controls should be included to prevent corruption due to processing errors or deliberate acts.

Change Control Procedures (11.2.2)

Changes to systems or applications within the development lifecycle should be controlled by the use of formal change control procedures.

Technical Review of Applications after Operating Platform Changes (11.2.3)

When operating platforms or applications are changed, business critical applications should be reviewed and tested to ensure there is no adverse impact on organizational operations or security.

Restrictions or Changes to Software Packages (11.2.4)

Modifications to software packages should be limited to necessary changes, and all changes should be strictly controlled.

Secure System Engineering Principles (11.2.5)

Principles for engineering secure systems should be established, documented, maintained and applied to any information system implementation efforts.

Secure Development Environment (11.2.6)

Organizations should establish and appropriately protect secure development environments for system development and integration efforts that cover the entire system development life cycle.

Outsourced Development (11.2.7)

Outsourced system development should be monitored and supervised to ensure the State's policies and practices are followed and to ensure appropriate security controls are in place.

System Security Testing (11.2.8)

Testing of security functionality should be carried out during development. Applications should be tested periodically throughout their respective lifecycles, at each major version release and prior to assigning public IP addresses or being moved or promoted into the production environment.

System Acceptance Testing (11.2.9)

Acceptance testing programs and related criteria should be established for new information systems, upgrades and new versions.

Test Data (11.3)

Objective: To ensure the protection of the data used for testing.

Protection of Test Data (11.3.1)

Test data should be selected carefully, protected and controlled. The use of production data for development and testing is prohibited.

12. BUSINESS CONTINUITY MANAGEMENT

Information Business Continuity (12.1)

Objective: To ensure the availability of critical systems and infrastructure and the continued ability to provide services in the event of a crisis or disaster.

Planning Information Systems Continuity (12.1.1)

All State agencies should determine their requirements for the continuity of information management systems in adverse situations, e.g. during a crisis or disaster.

Business Impact Analysis (12.1.1.1)

All State agencies should perform a Business Impact Analysis (BIA) to identify systems and infrastructure that are critical to State operations and services to citizens, other agencies and regulatory bodies.

Critical Applications (12.1.1.2)

Systems including Infrastructure components, applications and security systems identified as critical in the BIA will be recovered in accordance with the Business Impact Analysis and documented system recovery strategy.

Non-Critical Applications (12.1.1.3)

Infrastructure components and applications identified as non-critical in the BIA will be recovered on a best–effort basis. The components and applications listed as non-critical should have an explanation in the BIA justifying their low importance and demonstrating how the loss of their associated functionality will be acceptable during an event or how a manual workaround can be implemented.

Implementing Information Systems Continuity (12.1.2)

All State agencies should establish, document, implement, and maintain processes, procedures and controls in disaster recovery plans to ensure the required level of business continuity for all systems during an adverse situation.

Verify, Review and Evaluate Information Systems Continuity (12.1.3)

All State agencies and vendors or contractors who operate on behalf of the State should verify the established and implemented information systems continuity controls at regular intervals in order to ensure that they are valid and effective during adverse situations.

Redundancies (12.2)

Objective: To ensure availability of information processing facilities.

Availability of Information Processing Facilities (12.2.1)

Information processing facilities should be implemented with redundancy sufficient to meet availability requirements.

MINIMUM COMPLIANCE REQUIREMENTS

Verify, Review and Evaluate Information Systems Continuity (12.1.3)

- BIAs should be performed within every 365 days.
- A sample of critical applications should be tested within every 365 days as part of a scheduled disaster recovery exercise, as a tabletop or prior to go live exercise.

13. INFORMATION SECURITY INCIDENT MANAGEMENT

Management of Information Security Incidents and Improvements (13.1)

Objective: To ensure a consistent and effective approach to the management of information security incidents, including communication on security events and weaknesses.

Responsibilities and Procedures (13.1.1)

The State of Tennessee will establish a Security Incident Response Team (SIRT). The SIRT will ensure that the State of Tennessee can efficiently and effectively communicate information security incidents to the proper stakeholders and respondents of the State. The SIRT members will be appointed based on their position and capabilities within the organization. Each agency should designate an information security "point of contact" (POC), in accordance with the Information Systems Council's "Information Resource Policies" requirements. This POC will act as the central communications figure regarding security incidents within the agency. The POC will have responsibility for incident escalations, actions and authority for the administrative oversight of security for the IT resources under the agency's control. The POC within each agency will participate as a member of the SIRT. The CISO of the State of Tennessee will appoint members from within STS to participate in the SIRT.

Reporting Information Security Events (13.1.2)

Information security events should be reported through appropriate channels using the State of Tennessee Cyber Incident Response Plan (CIRP).

Data Breach and Disclosure (13.1.2.1)

Any State of Tennessee agency that discovers a breach of the information security controls set forth in this document which results in disclosure of unencrypted "personal information" about persons to unauthorized third parties must provide notice of the disclosure in accordance with TCA 47-18-2107 or any other applicable state and/or federal statute or regulations).

Reporting Information Security Weakness (13.1.3)

Employees and outsourced employees using the State's information systems and services are required to note and report any observed or suspected information security weaknesses in systems or services to the STS Customer Care Center.

Assessment of and Decision on Information Security Events (13.1.4)

Information security events should be assessed and a determination made on whether to classify the event as an incident in accordance with the CIRP.

Response to Information Security Incidents (13.1.5)

Information security incidents will be managed in accordance with the documented procedures in the State of Tennessee Incident Response, Alerting and Communications Plan.

Learning from Information Security Incidents (13.1.6)

Knowledge gained from analyzing and resolving information security incidents should be used to reduce the likelihood or impact of future incidents.

Collection of Evidence (13.1.7)

The State should define and apply procedures for the identification, collection, acquisition and preservation of information, which can serve as evidence.

14. CRYPTOGRAPHY

Cryptographic Controls (14.1)

Objective: To ensure proper and effective use of cryptography to protect the confidentiality and integrity of data owned or managed by or on behalf of the State. Confidential information must be encrypted by the use of valid encryption processes for data at rest and in motion as required by state or federal statute or regulation. This includes but is not limited to sensitive information stored on mobile devices, removable drives and laptop computers.

Use of Cryptographic Controls (14.1.1)

Cryptographic controls should be based on the classification and criticality of the data. In deciding what strength and type of control to be deployed, both stand- alone and enterprise level encryption solutions should be considered. Attention should be given to regulations, national restrictions (e.g. export controls) that may apply to the use of cryptographic techniques.

Transmission Integrity (14.1.2)

Information systems should protect the integrity of transmitted information traveling across both internal and external communications. This control applies to communications across internal and external networks.

Transmission Confidentiality (14.1.3)

Information systems should protect the confidentiality of transmitted information. The State will employ mechanisms to recognize changes to information during transmission unless otherwise protected by alternative physical measures.

Cryptographic Module Authentication (14.1.4)

Information systems must use mechanisms for authentication to a cryptographic module that meet the requirements of applicable federal statutes, state statutes, Executive Orders, directives, policies, regulations, standards, and guidance for such authentication. The list of cryptographic modules in use will be compared to the list of NIST validated cryptographic modules quarterly to ensure compliance.

Cryptographic Module Authentication (14.1.5)

Information systems will obtain and issue supported public key and Transport Layer Security (TLS) certificates from an approved service provider. This control focuses certificates with visibility external to the information system and does not include certificates related to internal system operations, for example, application-specific time services. Secure Socket Layer (SSL) protocol must be disabled on all devices.

Wildcard Certificates (14.1.5.1)

Wildcard certificates used for Internet facing systems must be approved by the Office of the CISO

Key Management (14.1.6)

A secured environment should be established to protect the cryptographic keys used to encrypt and decrypt information. Cryptographic key management and establishment will be performed using automated mechanisms with supporting manual procedures. Keys should be securely distributed and stored. Access to keys should be restricted only to individuals who have a business need to access them. All access to cryptographic keys requires authorization and should be documented. Compromise of a cryptographic key would cause all information encrypted with that key to be considered unencrypted.

15. COMPLIANCE

Compliance with Legal and Contractual Requirements (15.1)

Objective: To avoid breaches of legal, statutory, regulatory or contractual obligations related to information security and of any security requirements.

Identification of Applicable Legislation and Contractual Requirements (15.1.1)

All relevant legislative, statutory, regulatory, contractual requirements and the State's approach to meet these requirements should be explicitly identified, documented and kept current for each information system, each agency and each entity that stores, processes or transmits data on behalf of the State.

Intellectual Property Rights (15.1.2)

Appropriate procedures should be implemented to ensure compliance with legislative, regulatory and contractual requirements related to intellectual property rights and the use of proprietary software products.

Protection of Records (15.1.3)

Records should be protected from loss, destruction, falsification, unauthorized access and unauthorized release, in accordance with state or federal statutory, regulatory, contractual and business requirements.

Privacy and Protection of Personally Identifiable Information (15.1.4)

The privacy and protection of personally identifiable information should be ensured as required by relevant federal or state statute or regulation.

Regulation of Cryptographic Controls (15.1.5)

Cryptographic controls should be used in compliance with state or federal statutory, regulatory, contractual and business requirements.

Information Security Reviews (15.2)

Objective: To ensure that information security is implemented and operated in accordance the organizational policies and procedures.

Independent Review of Information Security (15.2.1)

The State's approach to managing information security and its implementation (i.e. control objectives, controls, policies, processes and procedures for information security) should be reviewed independently and at planned intervals or when significant changes occur.

Risk Assessment (15.2.1.1)

A Risk Assessment of the State environments where servers reside that process State data will be performed within every 365 days.

Compliance with Security Policy and Standards (15.2.2)

Managers should regularly review the compliance of information processing and procedures within their area of responsibility for accuracy and applicability with the appropriate security policy, standards and any other security requirements.

Technical Compliance Review (15.2.3)

Information systems should be regularly reviewed for compliance with the State's information security policy and standards.

16. HUMAN RESOURCE

Prior to Employment (16.1)

Objective: To ensure all full- and part-time employees of the State of Tennessee and all third parties, outsourced employees, or vendors understand their responsibilities in regard to information security requirements for the State of Tennessee's computing environments.

Screening (16.1.1)

Background and verification checks on all candidates for employment should be conducted in accordance with relevant statutes and published state policies.

Acceptable Use Policy (16.1.2)

All agencies should ensure that their full- and part-time employees of the State of Tennessee and all third parties, outsourced employees, or vendors who use State of Tennessee's IT resources have read and accept the terms of the relevant State's Acceptable Use Policies. Proof of employee acceptance and acknowledgement will be maintained by the agency.

During Employment (16.2)

Objective: To ensure employees and outsourced employees are aware of and fulfill their information security responsibilities.

Management Responsibilities (16.2.1)

Management should ensure that all employees and outsourced employees are aware of and fulfill their information security responsibilities.

Information Security Awareness, Education and Training (16.2.2)

All non-Executive Branch State employees who have access to State systems and where relevant, outsourced employees should utilize State-provided security awareness education and training when first employed and at least biennially thereafter.

All Executive Branch State employees who have access to State systems and, where relevant, outsourced employees should utilize State-provided security awareness education and training when first employed and within every 365 days thereafter.

17. VERSION HISTORY

Version 2.1 – December 15, 2016	*Converted Office for Information Resources to Strategic Technology Solutions. Updated policy link in 2.4 Made agency specific policies mandatory for agency specific requirements in 3.1.2. Minor wording changes to sections 13.1.1 and 13.1.2. Updated technology requirement for encryption in 14.1.5. Aligned training periodicity with ISC vote in 16.2.2.*
Version 2.2 – December 14, 2017	*Updated policy link in 2.4*
Version 2.3 – December 21, 2018	*Inserted language regarding cloud technologies and contractor hosted solutions in Executive Summary, Introduction and Scope. Converted Security Advisory Council to STS Executive Management Team. Combined 3.1.3 into 3.1.1 and clarified 3.1.2. Updated link in 6.2.3.5 and corrected numbering throughout 6.2.3. Added Cloud Services Procurement 6.4.4.1. Differentiated training requirements between Executive Branch and non-Executive Branch in 16.2.2. Added Risk Assessments 15.2.1.1. Change annual reviews to within review within 365 days throughout document.*

Version 2.4 – January 29, 2020	*Removed "Confidential" status from the policy. Adjusted terminology throughout policy to align with ISC policies and AUPs, Adjusted references. Converted ELT to Policy Review Committee in Review (2.4). Adjusted patch schedule in Patch Management (4.5.1.1) and added section Software Maintenance (4.5.1.2). Added sections System/Application Account Use (5.4.2.4) and System Administrator Account Use (5.4.2.5) adjusted associated minimum requirements, Added language to Removal or Adjustment of Access Rights (5.2.6). Added F&A policy reference to Inventory of Assets (6.1.1). Added PA-DSS requirement to Payment Card Information Classification and Control (6.2.3.5). Added language to Workstation Platform Disposal (6.4.3). Adjusted sections throughout 12. BUSINESS CONTINUITY MANAGEMENT to align with ISC Policy 9, Added section Wildcard Certificates (14.1.15.1). Removed appendices. Removed Terms and Conditions.*
Version 2.4.1– August 3, 2020	*Corrected omission of allowance of non-expiring passwords for service and system/application accounts and standardized nomenclature.*
Version 2.5 – August 2, 2021	*Changed document to be a single policy rather than a compilation of multiple policies. Corrected grammar and punctuation. Expanded scope to include State Cloud Tenants. Deleted duplicate paragraph in scope section. Added clarification to Exceptions (2.3), System/Application Account Use (5.4.2.4) and Password Management System (5.4.3). Added prohibition for using RDP and VPN from personally owned devices to Remote Access (5.1.2.1).*

Enterprise Information Security Policy (EISP)		Document Ref # 300-POL-001
Document Control	**Version #**	2.5
	Signed	Stephanie Weelman
	Signed	Curtis Clan (Aug 2, 2021 12:18 CDT)
	Approval Date	8/02/2021
	Implementation Date	8/02/2021
	Last Reviewed by Policy Review Committee	7/30/2021