



Department of Transformation and Shared Services

# State of Arkansas

## TSS DIS Cybersecurity Policy

### IT Cybersecurity and Risk Management

**Effective Date:** 10/01/2024

**Creation Date:** 02/01/2023

**Version:** 1.0

## Table of Contents

Cybersecurity Policy .....	6	1.0
Purpose.....	6	1.1
Scope .....	7	1.2
Policy Communication.....	7	1.3
Creation and Distribution.....	7	1.3.1
Enforcement and Compliance .....	8	1.4
Review, Update, and Maintenance .....	8	1.5
Exception Request Process.....	8	1.6
Organizational Cybersecurity.....	8	2.0
Organizational Cybersecurity Objectives.....	9	2.1
IT Cybersecurity Infrastructure .....	9	2.2
Roles and Responsibilities.....	9	2.2.1
Authorization Process for New IT Assets.....	10	2.2.2
Cooperation between Organizations .....	11	2.2.3
Security Requirements for Third Party Access.....	11	2.3
Requirements in Third Party Vendor Contracts.....	11	2.3.1
Requirements for Outsourcing.....	11	2.3.2
Confidentiality Agreements for Non-Employees and Contractors.....	11	2.3.3
Access Control .....	11	3.0
Access Control Objectives .....	11	3.1
Acceptable Use Policy.....	12	3.2
General Acceptable Use Policy.....	12	3.2.1
Electronic Communications and Online Systems Acceptable Use Policy.....	12	3.2.2
Workstation Acceptable Use Policy.....	13	3.2.3
Acceptable Use Banner.....	13	3.2.4
User Access Controls.....	14	3.3
User Conduct Policy.....	14	3.4
User Responsibilities.....	14	3.4.1
Prohibition Against Harassment.....	14	3.4.2
Password Management Policy .....	15	3.5
Concurrent Sessions and Session Timeouts.....	15	3.6
Session Timeout.....	15	3.6.1
Concurrent Sessions.....	15	3.6.2
Security and Audit Logging Requirements.....	15	3.7
Mobile Computing.....	15	3.8

Modems, Remote Access Devices, and Remote Access Software .....	15	3.8.1
Telecommuting.....	15	3.8.2
Mobile Devices.....	16	3.8.3
Asset Classification and Control.....	16	4.0
Asset Classification and Control Objectives .....	16	4.1
Accountability for Assets.....	16	4.2
Inventory of Assets.....	16	4.2.1
Information and Information Asset Classification.....	17	4.3
State Information Classification Levels .....	17	4.3.1
Information Asset Classification.....	18	4.3.2
Management of Cybersecurity-Related Documentation .....	19	4.3.3
Information Asset Labeling.....	20	4.4
Information Asset Handling.....	20	4.5
General Controls.....	20	4.5.1
Collaborative Computing Devices.....	20	4.5.2
Physical Transport .....	21	4.5.3
Electronic Transmission.....	21	4.5.4
Verbal Communication.....	21	4.5.5
General Destruction Requirements.....	21	4.5.6
Communications and Operations Management.....	21	5.0.
Communications and Operations Management Objectives.....	21	5.1
Operational Procedures and Responsibilities .....	22	5.2
General Controls.....	22	5.2.1
Documented Operating Procedures.....	22	5.2.2
Change Management .....	22	5.2.3
Problem Management Procedures .....	23	5.2.4
Cybersecurity Incident Management.....	23	5.2.5
Segregation of Duties.....	23	5.2.6
Separation of Development, Testing, and Production Environments.....	23	5.2.7
System Planning and Acceptance.....	23	5.3
Protection against Malicious and Mobile Code.....	24	5.4
Controls against Malicious Code .....	24	5.4.1
Controls against Mobile Code .....	24	5.4.2
Malware Prevention Policy.....	24	5.4.3
Vulnerability Management .....	25	5.4.4
Patch Management .....	27	5.4.5
Intrusion Detection Systems/Intrusion Prevention Systems (IDS/IPS) .....	27	5.4.6

Backup and Restoration .....	28	5.5
Data Backup.....	28	5.5.1
Network Security and Management .....	28	5.6
Restriction on Physical Access to the State Network .....	28	5.6.1
Requirements for Security of the State Network.....	28	5.6.2
Requirements for Management of the State Network.....	29	5.6.3
State Network Firewall Requirements.....	29	5.6.4
Router and Switch Security Requirements.....	31	5.6.5
Wi-Fi Networks and Devices.....	32	5.6.6.
Remote Access Requirements.....	32	5.6.7
System Configurations.....	32	5.7
Server Security Requirements.....	32	5.7.1
Cloud Service Security Requirements.....	33	5.7.2
Workstation Security Requirements.....	33	5.7.3
Email Security Requirements .....	33	5.7.4
Exchanges of Information and Software .....	33	5.8
Information Confidentiality .....	34	5.8.1
Information Reliability.....	34	5.8.2
Personnel Cybersecurity .....	35	6.0
Personnel Cybersecurity Objectives.....	35	6.1
Cybersecurity Included in Job Roles and Duties.....	35	6.2
Including Cybersecurity in Job Roles Definition.....	35	6.2.1
Personnel Screening Policy.....	35	6.2.2
Terms and Conditions of Employment.....	35	6.2.3
Personnel Education, Training, and Awareness.....	36	6.3
Cybersecurity Awareness Training .....	36	6.3.1
Responding to Cybersecurity Incidents.....	36	6.4
Cybersecurity Incident Response Priorities.....	36	6.4.1
Cybersecurity Incident Authority and General Controls .....	36	6.4.2
Cybersecurity Incident Response Procedures.....	37	6.4.3
Reportable Information Cybersecurity Incident Examples.....	37	6.4.4
Security Incident Information Retention and Classification.....	39	6.4.5
Problem Management Addressed by Reporting Software Malfunctions.....	39	6.5
Information System Acquisition, Development, & Maintenance.....	39	7.0
Information System Acquisition, Development, & Maintenance Framework.....	39	7.1
Cryptographic Controls & Key Management.....	39	7.2
Continuity of Operations and Disaster Recovery .....	39	8.0

Continuity of Operations and Disaster Recovery Objectives.....	39	8.1
Continuity of Operations and Disaster Recovery Management Oversight .....	39	8.2
Continuity of Operations and Disaster Recovery Management Controls .....	39	8.2.1
Physical and Environmental Security .....	40	9.0
Physical and Environmental Security Objectives.....	40	9.1
Physical Security General Controls.....	40	9.2
General Physical Security .....	40	9.2.1
Removal of Property.....	40	9.2.2
Secure Areas.....	41	9.3
Physical Security Perimeter.....	41	9.3.1
Physical Entry Controls.....	41	9.3.2
Securing Offices, Rooms and Facilities.....	41	9.3.3
Working in Secure Areas .....	41	9.3.4
Equipment Security .....	42	9.4
Equipment Protection .....	42	9.4.1
Power Supplies.....	42	9.4.2
Cabling Security .....	42	9.4.3
Security of Offsite Equipment .....	42	9.4.4
Secure Disposal, Transport, or Re-use of Equipment.....	42	9.4.5
Compliance .....	43	10.0
Compliance Objectives.....	43	10.1
Compliance with Legal Requirements and Policy.....	43	10.2
Identification of Applicable Legislation .....	43	10.2.1
Intellectual Property Rights.....	43	10.2.2
Legal Conflicts.....	43	10.2.3
Prevention of Misuse of IT Assets.....	43	10.2.4
System Audit Considerations.....	44	10.3
System Audit Controls.....	44	10.3.1
Protection and Use of State Network Audit Tool.....	45	10.3.2

## 1.0. Cybersecurity Policy

### 1.1. Purpose

The Arkansas Department of Transformation and Shared Services (TSS) Division of Information Systems (DIS) Cybersecurity Policy as well as related policy, procedures, standards, and guidelines owned by the State Cyber Security Office (SCSO) establishes a risk-based information cybersecurity governance program through which compliance controls and privacy requirements to guide and improve capabilities are defined for the protection of information, systems, and solutions owned or managed by the State of Arkansas. This framework establishes a foundation to align cybersecurity with Arkansas's Enterprise Information Technology (IT) Strategy and integrate with its Enterprise IT Architecture.

Implementation of IT Cybersecurity Policy, procedures, standards, and guidelines is an ongoing process with continuous reviews and updating that may or may not accurately reflect Arkansas's current cybersecurity posture. Arkansas adheres to the National Institute of Standards and Technology (NIST) Framework Core Controls necessary for a secure environment. NIST Framework Core Controls support critical infrastructure, cybersecurity risk, and comprehensive IT security.

The delivery of an effective IT cybersecurity governance program requires a team effort involving the participation and support of Arkansas's users at all levels and localities within the State. The Cybersecurity Policy outlines the process by which TSS DIS can effectively identify and respond to a variety of threats to information and information systems resources. These threats include but are not limited to denial of service, destruction, disclosure, duplication, loss, misuse, modification, and unauthorized access.

The TSS DIS SCSO service offerings for IT cybersecurity include the following:

- Strengthening responsibility and accountability for overseeing IT cybersecurity issues.
- Applying a mechanism to notify the appropriate personnel in case of an information cybersecurity incident.
- Administering guidelines to assess cybersecurity and protection methods applied to information, systems, and solutions.
- Maintaining effective security controls designed to protect the state's information, systems, or solutions from theft, abuse, misuse, or any other form of damage.
- Communicating responsibilities concerning IT cybersecurity to public employees, entities, contractors, consultants, customers, potential customers, vendors, public and private organization partners, and other users of state IT, systems, or solutions managed by TSS DIS.
- Promoting information cybersecurity awareness through communications and training.
- Protecting public confidentiality.
- Planning for continuation and continuity of operations in the event of significant information cybersecurity incidents.
- Providing a standard that facilitates compliance with industry recognized information cybersecurity governance frameworks.

## **1.2. Scope**

The scope of this policy includes the Enterprise IT Cybersecurity framework defined by specifics within broader cybersecurity domains. Cybersecurity domains include, but are not limited to:

- Security Management Practices
- Access Control Systems and Methodology
- Telecommunications and Networking Security
- Cryptography Operations Management
- Personnel Security
- Physical Security
- Application and Systems Development and Maintenance Security
- Business Continuity of Operations and Disaster Recovery Management

This policy complies with industry standards and best practices and applies to all users of Arkansas's IT assets working in the office, remotely or otherwise where Arkansas's IT assets are used or accessed, which may include but are not limited to state and local government employees, extra help employees, contractors, consultants, customers, vendors, and public and private organization partners, hereafter known as users.

Arkansas's IT assets include, but are not limited to computing devices, networks, telephones, magnetic or optical media, and paper regardless of the location, organizational unit, or controlling entity where IT assets are generated, created, accessed, viewed, processed, stored, used, acquired, purchased, obtained, manipulated, modified, deleted, or disposed.

## **1.3. Policy Communication**

### **1.3.1. Creation and Distribution**

Arkansas's Chief Information Security Officer (CISO) has overall responsibility for the establishment and distribution of the TSS DIS Cybersecurity Policy. The policy is available for viewing by all authorized parties through the TSS DIS portal.

1.3.2. Policy updates are provided through the following communication procedures:

- Internet
- Electronic Mail Communications
- Employee Forums
- Cybersecurity Awareness Training

TSS provides a monthly newsletter communication. Employee Forums are held on a regular basis. Cybersecurity awareness training is available to all IT users statewide to raise awareness for all public employees of potential threats and how to avoid them, to offer guidance on how to identify and report suspicious activity, to enhance the overall cybersecurity posture, foster a cybersecurity-focused work culture, and comply with industry standards and regulations.

## **1.4. Enforcement and Compliance**

Arkansas's CISO maintains primary responsibility for enforcing compliance with the TSS DIS Cybersecurity Policy and any subordinate policies, procedures, standards, and guidelines. The

State CISO may authorize specific cybersecurity teams to assist in managing these responsibilities. Effective, efficient management and operation requires a team effort involving the participation and support of every user.

All users of State IT resources and assets are responsible for properly using the security controls afforded to them including technical, administrative, or other appropriate measures to protect State IT resources and assets. All users of Arkansas's IT assets will fully comply with this policy and all related cybersecurity documents. Arkansas users found to be in violation of this policy are subject to disciplinary actions under State Human Resources policies and procedures. Third parties found in violation of this policy are subject to immediate termination of partner, and/or vendor relationship. Enforcement and compliance will also include contractual agreements, procurement, finance, and/or insurance contracts to ensure necessary security protections are identified and agreed upon by all parties.

### **1.5. Review, Update, and Maintenance**

Arkansas's CISO may review and approve this policy as necessary to ensure Arkansas's security practices contain the controls required to offset new security threats and vulnerabilities as they arise. The policy and its subordinate security policies, procedures, standards, and guidelines are reviewed and approved annually. The policy and its subordinate security policies are considered living documents and as such are subject to the changes and modifications, with or without notification, as necessary to protect cybersecurity priorities and objectives.

### **1.6. Exception Requests**

As necessary for continuity of operations, the TSS DIS SCSO allows for exceptions to this policy as well as related policies, procedures, standards, and guidelines. Exception requests are allowable with the understanding that the requesting party will expeditiously devise for implementation a recommended solution without cause for deviation from normal security operations. Exception requests may be made to the TSS DIS SCSO.

## **2.0 Organizational Cybersecurity**

### **2.1. Organizational Cybersecurity Objectives**

- To identify and document specific roles and responsibilities to ensure that IT cybersecurity is consistently and structurally reinforced throughout the State of Arkansas and that security controls are successfully implemented.
- To provide guidance for cooperation with external entities.
- To ensure proper authorization for integration of new assets into the TSS DIS environment.
- To ensure adequate security of IT and IT assets when accessed and used by third parties.
- To maintain the cybersecurity of IT when processes have been outsourced.

### **2.2. IT Cybersecurity Infrastructure**

This policy provides the following objectives relating to cybersecurity for Arkansas's IT infrastructure:

- Protect the State IT and IT assets against accidental or deliberate modification or destruction through utilization of a continuous risk assessment and management program.



- Prevent the unauthorized disclosure or misuse of information.
- Detect unauthorized access or misuse of IT or IT assets.
- Perform damage assessments following the detection of unauthorized disclosure of information or the unauthorized penetration or misuse of IT assets.
- Identify, report and correct vulnerabilities and exposures within the State's IT assets.
- Identify and document specific roles and responsibilities to ensure that cybersecurity is consistently reinforced throughout the State and that security controls are successfully implemented.

#### 2.2.1. Roles and Responsibilities

This section outlines the primary roles within the information cybersecurity governance framework as well as the responsibilities associated with the TSS DIS roles.

2.2.1.1. Uphold and sustain the States Information cybersecurity efforts, including adherence to the requirements set forth in this policy as well as related security policies procedures, guidelines, and standards.

2.2.1.2. Provide on-going oversight of permissible risk for all applicable public entities and engagements.

2.2.1.3. Communicate developments to this policy following review or legislative and regulatory changes.

2.2.1.4. Ensure that public employees and contractors are suitable for the roles for which they are considered, including any associated information security responsibilities by performing appropriate screening, background checks, and onboarding processes in accordance with relevant laws, regulations, and ethics measures and in proportion to governance requirements, the classification of the information to be accessed, and the perceived risks:

- Ensure that employees and contractors are informed of their responsibilities and that they understand and fulfill them. For contractual employees and contractors, this includes ensuring that employment agreements include responsibilities for information cybersecurity.
- Oversee investigations into perceived employee misconduct and administration of any resulting disciplinary actions.
- Communicate developments concerning the policy following review or legislative and regulatory changes related to employment.

2.2.1.5. Provide the operational aspects of cybersecurity within the scope of daily management of information, systems, and/or other enterprise IT solutions to fulfill the following responsibilities:

- Maintain the day-to-day management of security controls for the information, systems, and IT solutions within the assigned functional or operational area, in accordance with this policy and its subordinate policies.
- Act in the role of subject matter expert for any technical issues regarding cybersecurity within the area of operational or functional expertise.

- Document and maintain operating cybersecurity standards and procedures with the operational domain.
- When necessary, assist enterprise cybersecurity with investigating unauthorized activities and information cybersecurity incidents related to the operational domain.
- Recommend policy and control improvements to enterprise cybersecurity as necessary for updated technical requirements.
- Assist in providing compliance with this policy.
- Assist in implementing relevant controls purposed to minimize identified risk to their IT, systems, and solutions.
- SCSO works with Enterprise Security and IT Operations to ensure that systems and solutions meet or exceed requirements outlined by the policy.
- Assist IT Operations in reviewing user access to systems and solutions.
- Assist in improving the TSS DIS Information Cybersecurity Governance Framework through communication.
- Comply with Arkansas's cybersecurity and privacy policies related to data handling.

#### 2.2.2. Authorization Process for New IT Assets

The acquisition and use of any new IT assets will receive appropriate review and approval prior to implementation or integration into any environment, all hardware/software assets will be checked to ensure compatibility.

#### 2.2.3. Cooperation between Public Entities and Public and Private Organizations.

TSS DIS will maintain appropriate contacts with public entities and public and private organizations to ensure that appropriate actions can be quickly taken, and advice obtained in the event of a cybersecurity incident that includes, but not limited to: Arkansas's Governor, National Guard, law enforcement authorities, regulatory agencies, Arkansas Legislative Audit, governmental entities, other governmental entities, Information service providers, telecommunications providers, others, as necessary, to protect Arkansas's IT assets. Exchanges of information will be restricted to ensure that confidential information is not inadvertently provided during a cybersecurity incident.

### **2.3. Cybersecurity Requirements for Third-Party Vendor Access**

#### 2.3.1. Requirements in Third-Party Vendor Contracts

- All legal contracts between TSS DIS and a third-party vendor will include language protecting Arkansas's IT assets, and require compliance with Arkansas procurement laws, procedures, and cybersecurity practices.
- Non-Disclosure Agreements will be completed prior to engaging any customer or proposed customer.

#### 2.3.2. Requirements for Outsourcing

- Outsourcing contracts will contain appropriate language identifying which organizations' cybersecurity practices will govern the controls within the specified environment.
- When governing cybersecurity practices that have not been identified this policy will be the governing document.

[Click here to enter text.](#)

- Outsourcing contracts will contain provisions for compliance with international, federal, state, and local requirements as needed.

#### 2.3.3. Confidentiality Agreements for Non-Employees and Contractors

- Non-employee users and contractors will be required to complete a Non-Disclosure Agreement prior to being granted access to IT resources owned or managed by TSS DIS.
- Violations of a Non-Disclosure Agreement are considered in breach of contract, and may be subject to immediate termination of customer, public entity, other public entity, or vendor relationship.

### 3.0. Access Control

#### 3.1. Access Control Objectives

- Control access to IT and IT assets.
- Protect state network services.
- Detect unauthorized activities.
- Ensure information security for mobile computer use and telecommuting.

#### 3.2. Acceptable Use Policy

3.2.1. General Acceptable Use Policy provides guidance for using State IT resources and protects state users.

Use of State IT assets is limited to authorized users. Users of State IT assets will not assume their actions are private, privileged or protected. As permissible by law, TSS DIS maintains the right to monitor users in any manner deemed appropriate that may include video, audio or electronic monitoring of activities including, but not limited to: Telephone conversations, Email content and destinations, Instant messaging communications, Cloud service usage, Social media/networking communications, Internet access and downloading, Data access, Keystrokes, Work practices in the event that monitoring reveals criminal activities, the evidence and related information may be turned over to law enforcement officials without consent or notice to involved users. Violations of the policy, unauthorized use of IT assets or inappropriate use of IT assets are considered a security violation. Arkansas users found to be in violation are subject to disciplinary actions under Human Resources policies and procedures. Third parties found in violation may be subject to termination of customer, partner, and/or vendor relationship.

3.2.2. Electronic Communications and Online Systems are provided to state and local government employees for job-related purposes. Recognizing that employees may, on occasion, wish to use these systems for personal use, employees should keep in mind that use during State time and use that interferes with job performance is not permitted and can be considered a security violation. Arkansas employees found to be in violation are subject to disciplinary action under Human Resources policies and procedures. Third parties found in violation may be subject to immediate termination of customer, partner, and/or vendor relationship. Examples of personal use include, but are not limited to, personal communications, game playing, chat rooms, job searching, online merchandising, sports, personal social media pages, and other entertainment. In all circumstances, TSS DIS reserves the right to monitor the

employee user's electronic communications and online activity. TSS DIS has the right and the ability to track, review, audit or disclose any records originating and/or accessed by an employee user ID, as well as from Arkansas equipment. Accordingly, employee users should not have an expectation of privacy in electronic communications or online systems and should not consider such activities to be private or confidential. All electronic communications and online records are considered State property and are subject to inspection and disclosure to TSS DIS, law enforcement, and other government officials or other third parties as deemed appropriate by TSS DIS. State of Arkansas's electronic communications and online systems will not be utilized to:

- Create any discriminatory, defamatory, offensive, disruptive, or otherwise inappropriate or unprofessional communications. Among those communications considered inappropriate or unprofessional are any communications which contain sexual implications, racial slurs, gender specific comments or any other comments that inappropriately or unprofessionally address someone's age, race, gender, color, national origin, religion, sexual orientation, disability, or veteran status. Accessing any discriminatory, defamatory, offensive, disruptive, or otherwise inappropriate or unprofessional websites including, but not limited to sites that contain information related to the communications described above, pornography, hate speech, illegal drugs, or other illegal activities or gambling is prohibited under this policy.
- Disclose confidential information, financial information, protected data or other documents without approved authorization.
- Load unapproved applications on a computer/workstation that may periodically and automatically download data from the Internet. These applications, when widely installed, can be detrimental to the performance of State networking systems, perform any act that is illegal or otherwise in violation of any applicable federal, state, or local laws, regulations, or ordinances, conduct private business activities, incur unauthorized costs, misrepresent, obscure, suppress or replace a user's identity, establish new Internet Web pages or make modifications to existing Web pages unless done in compliance with policy, duplicate or use unauthorized computer software for any purpose, or download film, art, music or other such entertainment in violation of patent laws. In addition, users will be prohibited from using file sharing or "peer to peer sharing" applications or software for the purpose of acquiring or distributing film, art, music, or other such entertainment in violation of patent laws.

### 3.2.3. Workstation Acceptable Use Policy

Workstations provided by the State of Arkansas for the primary purpose of conducting state business are the property of the State of Arkansas and subject to removal or reallocation at any time. Users are prohibited from using state-provided workstations to negatively impact state business processes. Users are prohibited from altering or changing workstation hardware configurations without approval from TSS DIS. Users are prohibited from altering or changing workstation software configurations that modify or disable administrative controls implemented by TSS DIS IT support personnel. Installation of user-provided software is restricted, and users will adhere to software installation requirements as specified within this policy.

### 3.2.4. Acceptable Use Banner

[Click here to enter text.](#)

The following banner, or similar language, will be displayed wherever user login occurs: *This system is for authorized use only. Any use of the system is subject to monitoring and recording by systems personnel. Anyone using this system expressly consents to such monitoring and recording and is advised that if such monitoring and/or recording reveals possible criminal or unethical activity, system personnel may, in addition to other actions, provide the evidence of such monitoring to law enforcement officials.*

### **3.3. User Access Controls**

Access Control Policy establishes the requirements for user access, management of user accounts and access, and account administration on state owned or managed systems, solutions, and applications.

### **3.4. User Conduct Policy**

3.4.1. User standards, procedures and guidelines are important to the overall information security structure. Users should be aware of the following responsibilities:

- Users will be responsible for the use of their personal user account.
- Users who own a group, shared or undisclosed will be responsible for use of that account.
- Users will not use their authorized access to negatively impact, modify or compromise state IT resources.
- Users will not engage in the subversion of existing security controls unless appropriately authorized by TSS DIS. This includes but is not limited to Password cracking, Network, computer or device hacking, Brute force attacks, Unauthorized file decryption, Bootleg software copying, downloading, or sharing, Unauthorized network, computer, or device scanning.
- Users will be diligent in protecting state information resources and the overall information security of the State of Arkansas.
- Users will report suspected or identified information security incidents as required by this policy. Unauthorized attempts to circumvent an existing security measure may be unlawful and will be considered serious violations of this policy, procedures, standards, and guidelines. Violations by state or local government employees may result in disciplinary actions under Human Resources policies and procedures. Third parties found in violation may be subject to immediate termination of contract, customer, partner, and/or vendor relationship.

#### **3.4.2. Prohibition against Harassment**

TSS strives to maintain a workplace that is free of harassment and is sensitive to the diversity of its users. TSS prohibits the use of any information resource including, but not limited to voicemail, computers, email, and internet systems in ways that are disruptive, offensive, or harmful to others. Examples of inappropriate use of such information systems include, but are not limited to, the following:

- Threatening or harassing other users.
- Using obscene or abusive language.

[Click here to enter text.](#)

- Creating, displaying, or transmitting inappropriate images, messages, animations, or caricatures regarding race, sex, age, color, religion, national origin, marital status, physical or mental capacity or disability, medical condition, or sexual orientation, which in any way violate State policy prohibiting employment discrimination and harassment in employment.
- Creating, displaying, or transmitting inappropriate or unsuitable “chain letters.”
- Creating, displaying, or transmitting inappropriate “junk mail” such as unsuitable drawings, stories, inappropriate gossip or inappropriate “joke of the day” messages.

### **3.5. Password Management Policy**

Access to state information, systems, or solutions will be secured by appropriate authentication methods to verify the identity of the user. All passwords must adhere to required standards. Exceeding those requirements is strongly encouraged. Arkansas follows NIST Password standards and guidelines. All state and local government users are required to practice password management and protection best case study.

### **3.6. Concurrent Sessions and Session Timeouts**

3.6.1. Session Timeout whenever permitted by system software, a computer terminal, workstation, communication device/system, or microcomputer will automatically blank the screen and suspend the session after the recommended ten (10) minutes of system inactivity. Reestablishment of the session must take place only after the user has provided a valid password.

3.6.2. Concurrent Sessions whenever required by contractual obligations, or by the Information Custodian, concurrent sessions may be limited.

### **3.7. Security and Audit Logging Requirements**

- Audit and logging of all Arkansas owned or managed IT assets, including infrastructure systems and devices, will be in accordance with the requirements established in the TSS DIS Audit and Logging Policy and the associated Security and Audit Logging Standard.
- The audit and logging requirements defined in the Security and Audit Logging Standard will be aligned with the policy and its subordinate Security and Audit Logging Policy, as well as industry standards.

### **3.8. Mobile Computing**

#### **3.8.1. Modems, Remote Access Devices, and Remote Access Software**

- Unauthorized modems will not be connected to PCs, workstations, or laptops. When modem use is authorized: - Modems may not be used in the auto answer mode such that they are able to receive incoming dial-up calls. - Users will disconnect from network connections prior to dial out being attempted. This separation ensures that inadvertent access by an outsider is restricted to the individual resource and the exposure is limited.
- The use of unauthorized devices and/or software to facilitate remote access to Arkansas workstations or information systems that circumvent state network access controls is strictly prohibited.

### 3.8.2. Telecommuting

TSS Management must approve the remote access of Arkansas IT resources by their employees on a case-by-case basis. Telecommuting is a privilege and may be revoked at any time.

### 3.8.3. Mobile Devices

TSS Mobile Device Security Standard establishes the requirements for the approved use of mobile devices (including, but not limited to, smartphones, PDAs, and tablet computers) to connect to the Arkansas IT infrastructure and/or to access Arkansas-owned or managed data.

## 4.0. Asset Classification and Control

### 4.1. Asset Classification and Control Objectives

- Maintain appropriate protection of Arkansas's IT assets.
- Ensure appropriate responsibility is identified.
- Ensure an information classification level is assigned to all information assets.
- Identify the default classification level for all State information assets.
- Ensure all users understand classification levels.

### 4.2. Accountability for Assets

#### 4.2.1. Inventory of Assets

This policy utilizes the State Inventory management methodology, which defines the safeguards necessary to ensure the confidentiality, integrity, and availability of key information. For this reason, an asset (or "information asset") is any data, device, or other component of the environment that supports information-related activities that are considered critical. Information assets include, but are not limited to, information, documentation and proprietary information, hardware, software, and virtual assets. Each information asset must have an identified information custodian who is accountable as follows: 1) classification of the asset; 2) ensuring that the asset is part of documented inventory that contains all information necessary for business continuity and disaster recovery; and 3) maintenance of related security controls specified within the policy.

An inventory of critical documentation and proprietary information must be maintained and documented by the identified information custodian(s). The inventory must include the following: Information Custodian, Physical Location, and Classification of the documentation or proprietary information.

#### 4.2.1.2. Hardware Assets

Hardware assets include, but are not limited to, computer equipment, communication equipment, network equipment, infrastructure equipment, electronic storage media (including magnetic and optical media). An inventory of critical hardware assets must be maintained and documented by the identified information custodian(s). The inventory must include the following: Information Custodian, Physical Location, Applicable

Administrator, Classification of Hardware Asset, Classification of Information or Data Used, Processed, Handled, etc. by the applicable hardware asset.

#### 4.2.1.3. Software Assets

Software assets include, but are not limited to: Arkansas products, application software, system software, development tools, software utilities, and development code. An inventory of critical software assets must be maintained and documented by the identified information custodian(s). The inventory must include the following: Information Custodian, Physical Location, and Classification of the Documentation or Proprietary Information.

#### 4.2.1.4. Virtual Assets

Virtual assets include but are not limited to cloud services such as IaaS, PaaS, or SaaS, virtual LANs, and virtual machines. An inventory of critical virtual assets must be maintained and documented by the identified information custodian(s). The inventory must include the following: Information custodian, administrator where applicable: Associated responsible state business unit(s), Classification of the virtual asset, Classification of information or data utilized, processed, handled, etc. by the virtual asset, Virtual lease, License.

### 4.3. Information and Information Asset Classification

4.3.1. Categories for Information Asset Classification Levels are Data Classification and Information Classification.

- Data Classification outlines the categories of state data use and management. Use of this type of data is subject to privacy laws and regulations.
- Information Classification includes all Arkansas-owned information, such as work-related documents, stored files, communications, or other assets that comprise day-to-day operations.

NOTE: Information and its associated data must be classified, protected, handled, stored, and disposed of in accordance with contractual requirements and other policy to ensure continuous alignment with applicable privacy laws, regulations, standards, and industry practices. Necessary security safeguards defined within this policy and its subordinate policies and standards are subsequently leveraged to meet customer, contractual, and regulatory requirements for the classification of the information or data.

Following are four (4) primary levels of classifications with potential sublevels:

Restricted classification applies to any information and data that cannot be considered PUBLIC, due to its nature, but that is also determined by its Information Custodian to not be of a sensitive nature that would require encryption (e.g., electronic distribution of the policy). For this type of information, encryption is preferred but not required. Unauthorized disclosure or access could seriously and adversely impact the State of Arkansas, its employees, public and private partners, and/or departments, divisions, customers, or other governmental entities.



Confidential classification applies to information and data that is releasable to or accessible by a limited number of Arkansas employees. Access to or disclosure of confidential information can be provided to a limited number of individuals who have a legitimate need and with whom TSS has a Non-Disclosure Agreement (NDA) on file. The confidential classification also includes information designated as sensitive by Arkansas law or other regulatory agencies. The information custodian must define who is authorized to access or receive disclosure of confidential information, by job role and/or client team. Access to or disclosure of confidential information must be provided in accordance with all applicable Arkansas law, contractual, and regulatory requirements. Unauthorized disclosure could seriously and adversely impact the State of Arkansas, its employees, and citizens.

Internal Use Only classification applies to information and data that is specific to Arkansas State employees, or Arkansas IT resources, and is intended strictly for use within Arkansas state and local governments, such as, private information like payroll documents, proprietary information, managerial communications, or the contents of Arkansas Intranet sites. Unauthorized disclosure or access could seriously and adversely impact the state, its employees, public and private partners, and customers. Disclosure of Internal Use Only information must be managed by strict controls. Final approval by TSS legal or where applicable with prior completion of a non-disclosure agreement is required before Internal Use Only information is disclosed.

Public classification applies to information that originated within Arkansas state and local governments that does not clearly fit into any of the previous classifications, and, for which, disclosure is not expected to adversely impact the State, its employees, citizens, public or private partners, or customers. Information that has been designated as public can be disclosed to or accessed by anyone without formal management approval.

#### 4.3.2. Information Asset Classification

TSS is responsible for identifying and designating the appropriate classification level for all information assets within their realm of responsibility, in accordance with the following requirements:

- All information assets must be classified, according to their level of confidentiality, sensitivity, and criticality. For example: Information and its associated data must be classified, protected, handled, stored, and disposed of in accordance with contractual requirements and privacy policies and practices to ensure continuous alignment with applicable privacy laws, regulations, standards, and industry practices. Classification of the other information assets such as hardware, software, and virtual assets is determined by the classification of the information and data associated with them. Specifically, the individual asset's classification level must be the same as the most restrictive classification of all information associated with it. For those assets associated with data and/or information considered sensitive, the classification of the information asset is Confidential under this policy.
- All information assets must be protected in a manner to commensurate with their classification, as determined by their confidentiality, sensitivity, and criticality.
- When information assets of different classifications are combined, the resulting information asset must have a classification equal to the most restrictive classification.

- Default classification for any information asset (physical or logical) that is not officially labeled must be considered Internal Use Only.
- All users that create, compile, alter, or procure a new type of production information asset must assign a classification consistent with the prior classification.
- Information Security Assurance Managers are available to assist information custodians with appropriately classifying information assets.
- With the exception of state business correspondence and copyrighted software, all externally provided IT assets that are not clearly in the public domain must receive a classification level, to ensure appropriate protection and handling under this policy. Similarly, externally provided information or data must be classified, protected, handled, stored, and disposed of in accordance with Arkansas privacy policies and procedures.

#### 4.3.3. Management of Cybersecurity-Related Documentation

Cybersecurity-related documentation includes this policy and its subordinate policies, as well as any security documents that are regularly required for audit purposes, such as security standards, processes, procedures, and guidelines. It also includes any documentation related to the TSS DIS cybersecurity posture and security practices. The following are the management requirements for these documents.

##### 4.3.3.1. Review of Cybersecurity-Related Documentation

Cybersecurity-related documentation must be reviewed at least annually, to ensure that it accurately represents current cybersecurity posture and practices. It should also be updated, as necessary, to address any new cybersecurity threats and vulnerabilities and changes in state business requirements.

##### 4.3.3.2. Classification of Cybersecurity-Related Documentation

Cybersecurity-related documentation is classified as Internal Use Only. External disclosure of such documents will require completion of a Non-Disclosure Agreement and approval by TSS. Upon approval by TSS, the classification may be changed to Confidential on Arkansas cybersecurity-related documentation deemed as suitable for sharing with approved parties who have completed a Non-Disclosure Agreement.

##### 4.3.3.3. Disclosure of Cybersecurity-Related Documentation

Cybersecurity-related documentation must be secured appropriately in accordance with its classification. All users are prohibited from disclosing information related to Arkansas's cybersecurity posture or security practices, unless authorized.

#### 4.4. Information Asset Labeling

The following are the labeling requirements for IT assets. See Inventory of IT Assets, the Information Classification Levels, and Information Asset Classification sections for more information.

#### 4.5. Information Asset Handling

The following are the handling requirements for IT assets. See IT Inventory of Assets section for more information. Information and its associated data must be classified, protected, handled, stored, and disposed of in accordance with contractual requirements and Arkansas privacy policies and practices. Necessary security safeguards defined within this policy and its subordinate policies and standards are subsequently leveraged to meet certain identified TSS customer, contractual, and regulatory requirements, as required for the classification of the information or data.

#### 4.5.1. General Controls

All IT assets must be appropriately secured, as determined by their criticality and classification, particularly when unattended during and after work hours. Users must logoff or manually lock their workstation screen or similar action while away from their workstation; after work hours; and when unauthorized persons may potentially see a user workstation screen.

4.5.2. Collaborative Computing Devices include, but are not limited to, networked white boards, cameras, and microphones, such as those used for video teleconferences. The following requirements apply to the use of such devices:

- Remote activation of collaborative computing devices is prohibited.
- Explicit indication of use must be provided to users physically present at the devices, such as a visual and/or audible signal to users when collaborative computing devices are activated.

#### 4.5.3. Physical Transport

4.5.3.1. Physical transport of State IT assets requires the use of an authorized carrier.

4.5.3.2. Physical transport for repair or maintenance outside of TSS control including all media, devices, and equipment with electronic storage capability must receive prior approval from TSS DIS.

4.5.4. Electronic Transmission for all IT assets classified as Internal Use Only or Confidential transmitted to or from the State via any public network must be encrypted using approved cryptographic methods specified within the policy.

4.5.5. Verbal Communication must remain confidential. All communication disclosing IT assets, data, documentation, and other related public information must be confined within an appropriate state business environment and must not be accessible to persons who are not specifically authorized to access said communication.

#### 4.5.6. General Destruction Requirements

4.5.6.1. IT assets must be retained until they are no longer necessary, and their actual holding period has exceeded the required retention period.

4.5.6.2. IT assets in paper form must be shredded when no longer necessary. The use of an approved shredding service is preferable; however, a cross-cut shredder may be used if a shred service bin is unavailable. Users are prohibited from disposing of non-shredded paper IT assets in standard trash cans or recycle bins.

4.5.6.3. Electronic storage of IT media assets includes, but is not limited to, magnetic tapes, reel or cassette tapes, diskettes; optical disks, CDs, DVDs, or Blu-ray Discs; magnetic disks, ATA, or SCSI hard disk drives; and any other media, USB drives or flash drives onto which information is recorded, stored, or printed within an information system, server, workstation, device, or equipment. The strength and integrity of the retention method must be proportional with the security classification and sensitivity of the IT asset stored on the media, and it must also correspond with the media type.

## **5.0. Communications and Operations Management**

### **5.1. Communications and Operations Management Objectives**

- Ensure the correct and secure operation of state business processes.
- Minimize the risk of system failures.
- Protect the integrity of software and information from damage by malicious software.
- Maintain the integrity and availability of state business processes and communication services.
- Ensure the safeguarding of information in networks and the protection of the supporting infrastructure.
- Prevent damage to IT assets and interruptions to state business processes.
- Prevent loss, modification or misuse of information exchanged between public and private entities.
- Ensure correct and appropriately documented IT cybersecurity procedures for all processes related to IT cybersecurity.

### **5.2. Operational Procedures and Responsibilities**

#### **5.2.1. General Controls**

- All processes will be identified and documented within the designated area of responsibility.
- Areas and corresponding responsibility where separation of duties should be implemented to reduce the risk of negligent or deliberate system misuse will be identified and documented.

#### **5.2.2. Documented Operating Procedures**

- All IT cybersecurity procedures documented for operations corresponding to responsibility will be periodically reviewed and maintained.
- IT cybersecurity procedures will effectively include the following: Supporting contracts, instructions for handling errors or other unexpected conditions, system restart and recovery procedures, system maintenance procedures where applicable.

#### **5.2.3. Change Management**

- TSS DIS will be responsible for ensuring that all IT assets within their area of responsibility are part of an identified change management system.
- Formal change management procedures will be implemented to ensure satisfactory control of all changes to equipment, software, code, or applications.

- Audit logs containing relevant information will be retained.
- All significant changes will be identified and recorded.
- Any change to a controlled environment will have a documented state business reason prior to any change being made.
- TSS DIS IT professionals will assess the potential impact for any change to an IT asset within their area of responsibility.
- Changes will always be communicated to all stakeholders.
- All changes will have documented procedures identifying responsibilities for aborting and recovering from unsuccessful changes.

#### 5.2.4. Problem Management Procedures

TSS DIS will be responsible for ensuring all computers or computing devices within their area of responsibility are part of an identified problem management system.

#### 5.2.5. Cybersecurity Incident Management

Cybersecurity incidents must be addressed and managed as specified within Responding to Cybersecurity Incidents standards and procedures.

#### 5.2.6. Segregation of Duties

Reducing opportunities for unauthorized modification or misuse of IT or IT assets, TSS will implement the concept of “separation of duties” to the extent possible.

The separation of security administration and system administration will be implemented to the extent possible. TSS DIS will be responsible for ensuring that supervision and/or audit trails exist for instances in which segregation cannot be achieved.

Individuals considered to be auditors or fulfilling auditing roles will be independent from the organization being audited.

5.2.7. Separation of Development, Testing, and Production Environments must be separated and adhere to the following:

- Communications and Operations Management.
- Development, testing, and production software will be maintained on different systems where possible.
- Development, testing, and production software will be maintained on a logically separated network where possible.
- Compilers, editors, and other system utilities will not be accessible from operational systems when not required.

### 5.3. System Planning and Acceptance

5.3.1. TSS DIS will be responsible for working with system administrators to monitor and plan for capacity limitations and bottlenecks.

5.3.2. TSS DIS IT professionals responsible for production and development environments will develop and document acceptable standards for integration of new systems into areas of their responsibility. Where applicable these standards will include:

- Error recovery, restart procedures and contingency plans.
- A corresponded set of security controls.
- Effective manual procedures.
- Business continuity arrangements.
- Evidence that integration of a new system will not adversely affect existing systems.
- Evidence that consideration has been given to the effect of the new system on overall security of the environment. All systems being considered for use within a production or development environment will be approved by TSS DIS as being acceptable prior to introduction or integration into said environment.

#### **5.4. Protection against Malicious and Mobile Code**

5.4.1. Controls against Malicious Code Malicious code are firmware or software intended to perform an unauthorized process that will adversely impact the confidentiality, integrity, or availability of an IT asset or system. For example: a virus, a worm, spyware, or other code designed to infect a host. Detection, prevention, and recovery controls must be implemented and maintained on Arkansas's core IT assets to protect against malicious code.

5.4.2. Controls against Mobile code include software programs, applications, or content obtained from remote information systems, transmitted across a network, and executed on a local IT asset or system without explicit installation or execution by the recipient. Also known as active capsules, remote code, and executable content, mobile code is usually embedded and downloaded in the body of an HTML email or email attachment. For example: PDF, postscript, Java, JavaScript, ActiveX, Shockwave, and Flash animations. Automated controls such as browser settings must be implemented and maintained on Arkansas's core information assets to authorize and restrict the use of mobile code.

##### **5.4.3. Malware Prevention Policy**

5.4.3.1. Intentional user involvement with computer viruses is prohibited. Any activity with the intention to create and/or distribute malicious programs into the state network or onto any state IT asset will be strictly prohibited. All users will be strictly prohibited from writing, generating, compiling, copying, collecting, propagating, executing, or attempting to introduce any computer code designed to self-replicate, damage or otherwise hinder the performance of or access to any Arkansas IT asset.

5.4.3.2. Anti-Malware protection software will be approved, loaded, enabled, and active on all devices whenever possible including state approved, supported, and managed firewalls, servers, and workstations.

5.4.3.3. Anti-Malware protection software or other endpoint protection solution will be loaded, enabled, and active on all Arkansas owned, supported, and managed remote workstations that remotely connect to Arkansas's network IT resources prior to connecting to Arkansas's IT resources.

[Click here to enter text.](#)

5.4.3.4. Anti-Malware protection software updates are required on all state owned, supported, and managed devices. Automatic updates of Malware Prevention software will be the preferred method for updates. • Users will be responsible for timely updates of Malware Prevention software on their workstations. • System administrators will be responsible for timely updates of Malware Prevention software for devices within their area of responsibility.

5.4.3.5. Software loaded on Arkansas computers and networks will only come from trusted sources. Trusted sources include, but are not limited, to the following: well-known and industry trusted systems security authorities, industry-recognized and approved computer, or network vendors, commercial software vendors, or knowledgeable and trusted user groups. Software downloaded from electronic bulletin boards, shareware, public domain software or other software from untrusted sources will be strictly prohibited unless tested and approved.

5.4.3.6. Screening of software is required prior to use. Users will scan programs using Malware Prevention software or run files through approved state systems to perform analysis prior to installing or running executable programs provided by third parties or by other state or local government departments. Software source code provided by third parties or other state, or local government departments will be visually reviewed prior to compilation, and the resulting executable program will be scanned with virus-checking software prior to installation or execution on any Arkansas system. Users will be prohibited from bypassing a scanning process that could arrest the transmission of a computer virus.

5.4.3.7. Decryption of files is required prior to subjection to the malware checking process for all externally supplied computer readable files including but not limited to software programs, databases, word processing documents, spreadsheets.

5.4.3.8. User response to suspected Malware Infection is required by reporting all significant errors, incomplete processing, and improper processing of production applications to the Help Desk due to potential indication of malicious use. Users will be responsible for working with IT support to resolve malware infestations on their workstations.

#### 5.4.4. Vulnerability Management

Vulnerability management is a necessary part of the overall cybersecurity framework and requires compliance in the following:

5.4.4.1. General Controls will be maintained, supported, and centrally administered for vulnerability detection. A vulnerability detection system is defined as the automated process of proactively identifying vulnerabilities and misconfigurations of computing systems to determine if and where a system can be exploited or threatened. The Enterprise Vulnerability Management program incorporates proactive cybersecurity assessment through scenario-based testing designed to mirror common cybersecurity threat vectors to help validate the effectiveness of in-place controls and drive improvement to threat hunting, breach detection, and incident response solutions. All

[Click here to enter text.](#)

network connected systems, and devices, where applicable, will be included. All new systems will be scanned and remediated prior to use. All systems being moved or transferred, from their current environment to a new environment, will be scanned and remediated prior to being connected to the new environment including development, test, and production environments. Any system, connected to Arkansas's IT infrastructure will be subject to additional vulnerability scans, as warranted by security or operational necessity. Users will be permitted to run independent use vulnerability detection applications against systems for which they are responsible.

5.4.4.2. Administrative Controls will be maintained for setup, administration, and maintenance of all state supported vulnerability detection systems. State supported vulnerability detection systems will be updated on a regular basis. This regular basis will be no less than once a week, or as new updates are available.

5.4.4.3. Configuration will be supported for vulnerability detection solutions and configured for the following: A minimal number of false positives, non-intrusive scans unless an intrusive scan has been requested and approved, integrate offensive security assessments in the form of scenario-based testing into security development lifecycle, allow system administrators to conduct scans within their individually identified timeframes, provide automation of scanning, and provide adequate reporting mechanisms.

5.4.4.4. Security and User Interaction with Vulnerability Detection Systems provides detailed vulnerability scan results classified as INTERNAL USE ONLY. Users will be prohibited from viewing or accessing detailed vulnerability scan results for systems and/or devices in which they do not have a need to know, and from running vulnerability detection applications on or against systems for which they have not been approved.

5.4.4.5. Remediation and Responsibility will be included to ensure that all information assets, within each required area is part of the identified vulnerability detection solution. Notifications of false positives will be provided to vulnerability scanning administrators working to resolve identified vulnerabilities. Corrective action plans will be developed, reviewed, and approved by an appropriate reviewer prior to implementation. Any review of a corrective action plan must occur in a timely manner that does not negatively impact the dates identified within the corrective action plan.

5.4.4.6. Enforcement • In order to protect the state network infrastructure, failure to resolve relevant vulnerabilities within the identified time frames, may result in removal of a system or device from the state network without notification. Compliance reviews of Arkansas's Vulnerability Management Program are regularly conducted.

5.4.4.7. Exception Process Due to the nature of vulnerability detection systems, it is at times possible that the scanning process will adversely affect a machine. To that extent, exceptions can be requested for systems that are impacted by the vulnerability detection system. The exception process will follow the standard process for all exception requests.



Exceptions requests are reviewed and granted on a temporary basis. All security and patch update controls will be implemented as stated within the policy. All granted exception requests will be based on the team requesting the exception resolving all issues by a stated date.

#### 5.4.5. Patch Management Policy

- All State-owned or managed IT assets must be updated with system upgrades or vendor patches when necessary to ensure protection from known vulnerabilities.
- Patches, system upgrades, or other vendor releases must be obtained from trusted sources such as approved vendors or other external parties.
- Downloading patches as necessary within DIS are restricted to designated trusted sources only, such as whitelisted URLs.
- Testing of all applied patches/upgrades and change management procedures are required to ensure effectiveness and against potential side effects.
- Failure to patch or update an IT asset in a timely manner may result in its removal from the state enterprise infrastructure without notification, for the protection of other IT assets.
- All IT professionals responsible for the modification, availability, performance, and security of an IT asset should subscribe to information cybersecurity alerts/advisories from trusted sources that provide up-to-date information about known vulnerabilities.

#### 5.4.6. Intrusion Detection and Prevention Systems (IDS/IPS)

- All state systems and devices will be required to participate in a centrally managed IDS/IPS solution.
- Management of the state IDS/IPS solution will be maintained by the DIS SCSO.
- IT professionals will be responsible for ensuring that devices within their area of responsibility. Data backups critical to recovery efforts must be made on a regular basis.
- Automated solutions are used to track all backups of critical information and software as necessary.
- Off-site and on-site backups must be logged with identifying information, date, time, and action, at a minimum.
- Adequate backup facilities must be provided to ensure that all essential state business information and software can be recovered following an emergency or disaster.
- A minimum level of backup information, together with accurate and complete records of the backup copies and documented restoration procedures, must be stored in a remote location at a sufficient distance to escape any damage from a disaster at the main site.
- Backup information is given the appropriate level of physical and environmental protections.
- Restoration procedures are tested to ensure they are effective and that they can be completed within the time allotted on a per case basis when required by any applicable documented state or local government business requirements and contractual obligations.
- Retention and archive must be performed in accordance with the policy and its subordinate security policies, procedures, standards, guidelines, applicable regulatory requirements, and any relevant documented state or local government business requirements and contractual obligations.

- DIS SCSO recommends both host-based and network-based IDS/IPS solutions, where applicable.
- IDS/IPS solutions will be implemented and maintained to the minimum industry standard expectation.

## **5.5. Backup and Restoration**

### 5.5.1. Data Backup

## **5.6. Network Cybersecurity and Management**

### 5.6.1. Restriction on Physical Access to the State Network

- Access to the state network infrastructure will be denied unless officially authorized.
- All physical connections to the state network will be managed and will be disabled when not in use.
- Managers will be responsible for notifying network personnel when physical connections are no longer needed.

### 5.6.2. Requirements for the Security of the State Network

- All software installed on network-attached devices will be maintained at a level supported by the approved vendor.
- Operational responsibility for network assets will be separated from network security operations as necessary.
- All assets connected to the state network will be identified and documented.
- Regulatory requirements are implemented to safeguard the confidentiality and integrity of data on public networks.
- IT assets such as servers and applications must be appropriately secured during migration activities to ensure protections.
- Network and network-related asset planning, requirement, necessity, design, implementation, administration, maintenance and disposal will take cybersecurity into consideration during all phases of each network asset life cycle.
- Access to or disclosure of state network-related information will be strictly prohibited and will require appropriate authorization prior to disclosure.
- All information assets used to manage, pass or filter network traffic will be maintained within an appropriately physically secured location.
- Firewalls, demilitarized zones (DMZs), intrusion detection systems (IDS)/ intrusion prevention systems (IPS), network zones, and content filtering servers will be implemented as necessary.
- All users will be required to authenticate themselves to the state network prior to establishing a real-time connection with any internal IT asset over the Internet.
- The use of remote-control software will be strictly controlled and will be prohibited from connecting to the state network or state network assets from a public network without official authorization.
- Standard desktop firewall software will be installed and active on all state-owned or managed desktops and laptop workstations.

[Click here to enter text.](#)

### 5.6.3. Requirements for Management of the State Network

- Naming conventions for devices located on the state network will be considered for official authorization.
- Traffic present on the state network will be restricted and will originate or terminate on assets that are authorized to be on the state network.
- IT professionals assigned will work with appropriate teams to document relevant operational procedures for all network assets.
- Network assets will be, at a minimum, maintained to applicable industry standards.

### 5.6.4. State Network Firewall Requirements

5.6.4.1. Firewall General Security Controls encompass firewall infrastructure stationed at all points of ingress into and egress from the state network. Firewall infrastructure will be established between any trusted and non-trusted network. Firewall infrastructure will, at a minimum, meet or exceed all qualified and approved vendor specifications and industry baseline standards or practices. When network connectivity must be continuously maintained, production firewall infrastructure will have a backup solution or system fully capable of fulfilling the obligations of the primary firewall in case of an emergency or failure. Firewalls will be configured as to block all inbound and outbound traffic that has not been permitted by firewall policy.

5.6.4.2. IT Operations is identified as the final decision maker for all management of, changes to, updates to, or modifications of all state managed or owned firewall infrastructure. IT Operations will be responsible for working with relevant teams to identify and document all necessary technical standards for firewall infrastructure. This includes both infrastructure currently in use, as well as infrastructure that is under consideration for use. • IT Operations will be responsible for working with relevant teams for creation, maintenance and administration of any procedure or relevant documentation related to firewall infrastructure.

5.6.4.3. Firewall configuration settings are the parameters that can be changed in hardware, software, or firmware components of the firewall infrastructure that impact the security state of the enterprise network and the IT assets that the firewall infrastructure is intended to protect. Examples of these security-related parameters are registry settings, permission settings for account, file, and directory, and firewall security policies also known as network traffic flow rules or “rulesets”, which are settings related to functions, ports, protocols, services, and remote connections. Firewall infrastructure configuration must, at a minimum, adhere to the following requirements: Baseline configuration standards for firewall infrastructure are defined in accordance with industry-accepted security standards. These baseline configuration standards must be documented and maintained under TSS DIS standard change management processes, reviewed at least annually, and updated as necessary. All firewall infrastructure is configured to baseline configuration standards. All firewall infrastructure is configured to block unauthorized network traffic and services. Changes to cybersecurity policies of the firewall infrastructure must have supporting documentation. Configuration changes that are made outside of the baseline configuration standards, including changes to

cybersecurity policies, are managed through standard change management process. Firewall infrastructure configurations, including cybersecurity policies, must be reviewed at least annually to assess validity and effectiveness in limiting vulnerabilities on an ongoing basis. They must also be reviewed, as required, after major system changes, upgrades, or decommissions. All firewall infrastructure, in the event of a failure, must be configured to “default deny” for all network traffic until such time that the appropriate administrator re-enables all services. All firewall infrastructure will not accept traffic on external interfaces that appears to originate from internal network addresses. All implemented IDS/IPS solutions, at a minimum, detect and immediately report to the identified administrator on any modification to firewall system files. Unless approved, all firewall infrastructure is configured to prohibit real-time connections between two or more internal systems. Application gateway firewall infrastructure must not be configured to route any traffic between the external interface and the network interface. New firewalls must be tested and evaluated before deployment to ensure proper working order.

5.6.4.4. Firewall administration including documentation will be maintained in offline storage. This includes, but is not limited to, diagrams, IP addresses and configurations. Firewall documentation will not be stored on the firewall infrastructure. All changes to a firewall infrastructure will be consistent with policy. All firewall infrastructure will be tested for vulnerabilities and configuration problems prior to introduction into a production environment. The execution of privileged commands on firewall infrastructure such as administrative access will be limited to authorized firewall administrators. The use of remote access to facilitate administration of firewall infrastructure must be authorized prior to use. Privileged remote access to firewall infrastructure also requires the use of multi-factor authentication to appropriately authenticate the authorized firewall administrator and an approved encryption mechanism to secure the network connection such as an approved VPN solution). All firewall administrators will receive periodic training on firewalls and network security practices as necessary. If access through a firewall includes authentication based on source address, authentication will be combined with other security schemes to protect against IP spoofing attacks. All firewall infrastructure will have timely and relevant security patches, updates, and any other required protective actions. All employees tasked with monitoring firewall infrastructure will subscribe to security advisories and other relevant sources providing up-to-date information about firewall vulnerabilities and assist in implementing appropriate countermeasures.

5.7.4.5. Physical Security will be provided for all firewall infrastructure. All locations that house firewall infrastructure will have monitoring and logging capabilities. Access to rooms which house firewall infrastructure will be restricted to authorized personnel whose access is necessary according to their job roles and responsibilities.

5.6.4.6. Logging and Auditing will be enabled on all firewall infrastructure. All log files will comply with the logging requirements specified within the policy and any subordinate policies, procedures, standards and guidelines. All log files for all firewall devices will be maintained and stored for review.

## 5.6.5. Router and Switch Security Requirements

[Click here to enter text.](#)

- All state-owned or managed network routers and switches will be appropriately secured in accordance with the requirements established in standards and procedures and configured in accordance with the appropriate technical network standard.
- Security requirements as defined in standards and procedures will be aligned with the policy and its subordinate policies, as well as industry standards.

#### 5.6.6. Wi-Fi Networks and Devices

5.6.6.1. Restrictions apply on use of Wi-Fi devices. TSS DIS policy prohibits the operation of Wi-Fi networks and devices that have not been approved or implemented. This includes implementation at any state location or state facility that is managed, owned or leased. IT professionals will be authorized to use scanners and other similar tools to monitor for rogue access points, networks, and other wireless devices. Any unauthorized device detected by scanning or identified through physical means as being used while on state premises will be deactivated and can be removed or confiscated by an authorized security administrator.

5.6.6.2. Wi-Fi security requirements exist for employee access where it is deemed appropriate, IT Operations may deploy secured Wi-Fi networks for employee access to internal state networks. Such networks should always be configured and managed to current industry standards and should at a minimum meet the following requirements: Unless prohibited by job role, duties, or contractual/regulatory requirements all state employees with a valid and functional Active Directory account will be permitted to use these approved networks. Individuals who are not state employees will not be permitted to access these Wi-Fi networks. All approved device configurations should be reviewed on a periodic basis to maintain adherence to industry standards. All access to such Wi-Fi networks must be validated by at least two-factor authentication methods. The most robust industry standard Wi-Fi authentication and encryption protocols must be utilized.

5.6.6.3. Wi-Fi security requirements provide for guest access if determined to be appropriate and may deploy secured Wi-Fi networks for guest access to the Internet. Such networks should always be configured and managed to current industry standards and should at a minimum meet the following requirements:

- Unless prohibited by job role, duties, or contractual/regulatory requirements all state employees with a valid and functional Active Directory account will be permitted to use approved networks.
- Devices permitted to access such networks must be identifiable to the individual owner.
- The most robust industry standard Wi-Fi authentication and encryption protocols are required, or devices and networks are not permitted.
- Guest networks will only be permitted to connect to the Internet and must never allow direct connectivity to state internal networks.
- At a minimum, the password used to provide guest Wi-Fi access must be changed at least annually.

### 5.6.7. Remote Access Requirements

All remote access connections to the state network or individual network devices require either an approved secure virtual private network (VPN) solution or an approved secure dial-up system.

5.6.7.1. Remote Access Secure VPN requirements for all remote access VPN connections to the state network or individual network devices must: 1) pass through approved firewalls or secure authentication servers; and 2) require two-factor authentication, at a minimum. All inbound remote access VPN connections must also use an approved dynamic password system. Auditing and logging of significant events for all remote access VPN connections must be enabled and monitored.

5.6.7.2. Remote Access Secure Dial-up requirements for all state-owned or managed remote access dial-up solutions will be appropriately secured in accordance with established requirements.

5.6.7.3. Remote Administration Access requirements including the execution of privileged commands via remote access must be authorized prior to use and limited to authorized administrators only. Remote administration access must use: 1) multi-factor authentication to appropriately authenticate the authorized administrator; and 2) an approved encryption mechanism to secure the network connection such as an approved VPN. Auditing and logging of significant events for all remote administration access sessions are enabled and monitored.

## 5.7. System Configurations

### 5.7.1. Server Security Requirements

- All state-owned or managed servers must be secured in accordance with the requirements established in the TSS DIS standard and hardened in accordance with the appropriate IT system hardening standard.
- The server security requirements defined in the TSS DIS standard and IT system hardening standard will be aligned and maintained with current regulatory requirements, industry standards, and this policy and its subordinate security policies, procedures, standards, and guidelines.
- TSS DIS standards also identify additional security requirements such as encryption for state-owned or managed servers that store, process, or transmit sensitive data. These requirements must be in accordance with sensitive data handling requirements, as defined by the applicable privacy and confidentiality policies and practices.

### 5.7.2. Cloud Service Security Requirements

- All state-owned, managed, or utilized cloud services including, but not limited to Software-as-a-Service (SaaS), Platform-as-a-Service (PaaS), and Infrastructure-as-a-Service (IaaS), must be secured in accordance with the requirements established in the Cloud Security and Acceptable Use policies, procedures, standards and guidelines, as well as hardened in accordance with the appropriate IT cloud service hardening standard.

- The cloud service security requirements defined in the Cloud Security standard and other IT cloud hardening standards will be aligned and maintained with current regulatory requirements, industry standards, and this policy and its subordinate security policies, procedures, standards, and guidelines.
- The Cloud Security and Acceptable Use policies also identify additional approval and secure handling requirements for the state and contribute data/information in a cloud environment. Approvals are required for sensitive data to be hosted in a cloud environment. These requirements must be aligned and maintained with privacy and confidentiality policies and practices.

#### 5.7.3. Workstation Security Requirements

- All state-owned or managed workstations will be appropriately secured in accordance with the requirements established in TSS DIS standards and configured in accordance with the appropriate technical standards.
- The security requirements defined in TSS DIS standards will be aligned with this policy, and its subordinate policies, procedures, standards, guidelines, and industry standards.

#### 5.7.4. Email Security Requirements

- State-owned or managed email systems will be appropriately secured in accordance with the requirements established in the TSS DIS standards and configured in accordance with the appropriate technical standards.
- The security requirements defined in standards will be aligned with this policy, its subordinate policies, procedures, standards, guidelines, and industry standards.

### 5.8. Exchanges of Information and Software

#### 5.8.1. Information Confidentiality

Information classified as Internal Use Only, Confidential, or Restricted, either implied as such or specifically identified as such by contract or other means, should be protected from unauthorized or unintended release or disclosure. All users will adhere to the following:

- Information classified as or known to be Internal Use Only, either formally or informally, will be restricted from disclosure.
- TSS legal will maintain responsibility for final approval of disclosure of any information formally or informally classified as Internal Use Only.
- All exchanges of software and/or data between the state and any third party, not strictly related to a business purpose, will be prohibited unless a legal written agreement is in place.
- All written agreements for the exchange of software and/or data will, at a minimum, contain the following: Terms of the exchange, Date/Period of the agreement, Software/Data handling agreements, Software/Data protection agreements.
- Information classified as Internal Use Only or Restricted will be restricted from transport or transfer across any public network unless appropriately encrypted.
- All encryption solutions used to transport or transfer information classified as Internal Use Only or Restricted will comply with this policy.

### 5.8.2. Information Reliability

Any file, software, or information received, downloaded or acquired from a public network source (e.g., a web page or public ftp site on the Internet) must be considered suspect until verified and authenticated by a second source. Such media is prone to contain malicious or mobile code. For that reason, the following requirements apply when files, software, or information are accessed or obtained from a public network:

- All non-text files downloaded from the Internet must be protected with approved software prior to being used or installed on state-owned or managed information assets.
- Information, software, or programs downloaded from a non-trusted source will be tested on a standalone, non-production machine prior to introduction into the state enterprise infrastructure.
- Downloaded files that are compressed and/or encrypted will be uncompressed and/or decrypted prior to screening with appropriate software.
- Automatic updating of software or information on state computers via background “push” internet technology will be prohibited on all state information resources unless otherwise approved.
- The identity of individuals and/or organizations will be verified prior to being engaged for state business purposes.
- All users will be prohibited from misrepresenting, obscuring, suppressing or replacing another state or local government user’s identity on the Internet or any state IT resource.
- Only users that are specifically authorized are permitted to create and/or alter state-owned or managed web pages, social media, or other types of Internet presence that are publicly accessible.

## 6.0. Personnel Cybersecurity

### 6.1. Personnel Cybersecurity Objectives

- Reduce risks associated with human error, theft or fraud.
- Ensure that users are aware of cybersecurity threats and provide support for users to adhere to state cybersecurity practices.
- Minimize damage from cybersecurity incidents and other problems and assess, track and implement lessons learned.

### 6.2. Cybersecurity Included in Job Roles and Duties

#### 6.2.1. Including Cybersecurity in Job Roles and Duties

- All IT job roles are defined to include appropriate language identifying the correlating IT cybersecurity duties and responsibilities according to industry standards for TSS Office of Personnel Management (OPM).
- TSS DIS collaborates with OPM to identify IT job roles specific to cybersecurity duties and responsibilities to accurately demonstrate need, efficiencies, and justification.

#### 6.2.2. Personnel Screening Policy

[Click here to enter text.](#)



- Employment screening checks, as specified by TSS legal, OPM, and DIS SCSO are conducted for all permanent staff, contractors, temporary staff, and third-party users prior to or starting employment with the State of Arkansas or being granted access to state IT assets. Third parties are responsible for notifying TSS when there is a failure to complete required employment screening.
- Employment screening checks must be successfully passed prior to beginning work at the State of Arkansas or being granted access to Arkansas IT assets.
- All state employees are required to have on file, a signed consent allowing for background screening checks.
- All employees granted cybersecurity related job roles are required to satisfactorily pass supplemental employment screening checks on a periodic basis.

#### 6.2.3. Terms and Conditions of Employment

- All extra help, vendors, partners and contractors, who are given access to state-owned or managed IT assets, will sign confidentiality or non-disclosure agreements prior to being granted access to any state-owned or managed IT assets.
- All extra help, vendors, partners and contractors will be responsible for working with TSS and TSS DIS to support the implementation of a state cybersecurity environment.
- Full compliance with the policy is a condition of employment. Violation of this policy may result in disciplinary action under TSS OPM policies and procedures. Third parties found in violation may be subject to immediate termination of customer, partner, and/or vendor relationship.

### 6.3. Personnel Education, Awareness and Training

#### 6.3.1. Cybersecurity Awareness Training

- All state and local government employees granted access to state IT resources to facilitate completion of training curriculum are offered and required to complete cybersecurity awareness training.
- Cybersecurity training is an ongoing process that teaches industry standards, best practices, and response procedures for addressing and managing cybersecurity emerging threats and risks to computer systems.
- All state and local government employees are required to complete cybersecurity awareness training at least annually, to ensure that all personnel are aware of the importance of basic cybersecurity awareness as it changes over time.
- Failure to complete mandatory cybersecurity awareness training will be considered during annual job performance evaluations.
- Additional and advanced cybersecurity training is provided for those in IT leadership roles and who have critical cybersecurity roles and responsibilities.
- Additional cybersecurity training may be available to security personnel for personal improvement on a voluntary, self-directed basis.

### 6.4. Responding to Cybersecurity Incidents

#### 6.4.1. Cybersecurity Incident Response Priorities:

[Click here to enter text.](#)

- Protection of human life and safety.
- Protection of Internal Use Only, Confidential, or Restricted information.
- Prevention of damage to systems and restoration of systems to routine operation as outlined in response and recovery plans.

#### 6.4.2. Cybersecurity Incident Authority and General Controls

- Physical Security is the recognized authority to complete state investigations where allegations are made in the following areas: - Information Security - Property Loss and Protection - Employee Safety - Drugs - Financial Violations – Other
- All users of state IT assets have the responsibility to report cybersecurity incidents.
- Anonymous reporting of cybersecurity incidents will be permitted.
- All cybersecurity incident inquiries will remain confidential.
- All users have an obligation to report cybersecurity weaknesses in a timely manner.

6.4.3. Cybersecurity Incident Response Procedures will be conducted and carried out as specified within the Arkansas Cybersecurity Incident Response Plan.

#### 6.4.4. Reportable Information Cybersecurity Incident Examples.

6.4.4.1. Unauthorized Disclosure Internal Use Only, Confidential, or Restricted information is disclosed without authorization.

##### 6.4.4.2. System Incapacitation

- A system's ability to function is impaired by a high volume of activity from various sources.
- A resource such as power, network access or routing tables is modified, degrading the system's ability to perform normal functions.
- Malicious code interferes with a system's operation.
- An IT asset is stolen, damaged or destroyed.

##### 6.4.4.3. System Tampering

- A user ID is employed to gain access to system administrative functions without prior authorization.
- A valid user ID is permitted access to the system administrative functions without official authorization.
- A system weakness allows access to system administrative functions by non-authorized users.
- Non-administrative personnel are allowed to perform administrative system functions.

##### 6.4.4.4. Information Tampering

- A user ID is employed without authorization to gain access to password files, protected or restricted data, licensed applications, software, or restricted applications, software and/or code.

- A theft of information resources provides access to password files, protected or restricted data, licensed applications, software, or restricted applications, software or code.
- A system weakness allows unauthorized access to password files, protected or restricted data, licensed applications, software, or restricted applications, software and/or code.

#### 6.4.4.5. Misuse of IT

- User installs unlicensed software.
- User downloads, copies or distributes unlicensed software.
- User's account is employed in violation of state or federal statutes, regulations or organization policies.

#### 6.4.4.6. Unauthorized Access

- Valid user ID or user account is employed without authorization.
- Valid user ID or user account is used to access areas outside of the user's account authorization.
- A system weakness is exploited, but no access is gained outside the account's authorization.
- User's privilege to access information is higher than that which was authorized.
- Access to facilities, buildings, rooms, and other secure areas is gained without authorization.

#### 6.4.4.7. Unauthorized Use

- Internal Use Only, Confidential or Restricted information is used for a purpose not specifically permitted based on the user's need-to-know, or the identified disclosure classifications.
- Any state IT asset is used in such a way as to violate this policy.

#### 6.4.4.8. Attempted Exploration of Information Resources

- Illegal data gathering is directed against a system, such as port scanning, sniffing, net scanning, other.
- Actions are attempted that could impair a system's ability to function.
- Actions are attempted that could result in a system or information compromise.

#### 6.4.4.9. Non-System Incidents

- Unauthorized access to facilities results in IT resource exposure or compromise.
- Unauthorized parties gain access to Internal Use Only, Confidential, or Restricted information
- Data and information resources are exposed or compromised due to an environmental hazard or natural or other disaster.

#### 6.4.4.10. Individual User Reporting Responsibilities

[Click here to enter text.](#)

- Any attempt to interfere with, prevent, obstruct or dissuade a user in their efforts to report a suspected cybersecurity incident or violation is strictly prohibited. Any form of retaliation against an individual reporting or investigating a cybersecurity incident or violation is also prohibited. Either of these actions are subject to disciplinary actions under state Human Resources policies and procedures for employees. Third parties found in violation may be subject to immediate termination of customer, partner, and/or vendor relationship. Prosecution to the fullest extent of the law is also possible.
- TSS will be notified of all offensive communications. State and local government users will not respond directly to the originator of offensive email messages, telephone calls and/or other communications.
- Users will retain copies of messages, notes or voice mail entries of this nature and turn them over to managers.

#### 6.4.5. Cybersecurity Incident Information Retention and Classification

- Information related to or gleaned from a cybersecurity incident will be maintained and retained until such a time as the information is no longer relevant.
- Information related to or gleaned from a cybersecurity incident will be classified Internal Use Only.

### 6.5. Problem Management

Software Malfunctions are reported to identify and document problem management procedures for all IT assets within areas of responsibility.

## 7.0. Information System Acquisition, Development, & Maintenance

### 7.1. Information System Acquisition, Development, & Maintenance Framework

Information System acquisition, development, and maintenance outlines the requirements for security inclusion in the development and acquisition of information systems, components, and services, as well as development and support that includes security requirements for software coding and testing and securing system files, such as production software and source code.

### 7.2. Cryptographic Controls & Management

Cryptographic controls and management provide for encryption and governance of state-owned or managed systems, solutions, applications, and information assets.

## 8.0. Continuity of Operations and Disaster Recovery

### 8.1. Continuity of Operations and Disaster Recovery Objectives

Ensure the continuation of state and local government and expedite a resumption of state business processes in the event of a disruption due to disaster or security failure.

### 8.2. Continuity of Operations and Disaster Recover Management Oversight

#### 8.2.1. Management Oversight Controls

[Click here to enter text.](#)

- Identify and designate a team that has the responsibility for the commission, design, implementation, maintenance, administration and testing of all Continuity of Operations and Disaster Recovery plans.
- Entities will manage teams to identify and document adequate notification processes to be used in the event of a disaster or significant disruption.
- Teams will develop appropriate templates to facilitate plan creation and maintenance.
- Team members are responsible for management of all IT resources within their area of responsibility.
- Governmental entities should have a managed process in place to develop and maintain Continuity of Operations and Disaster Recovery plans that support teams.
- Teams should understand the risks in terms of impact for disasters or disruptions to IT assets.
- Teams will be responsible for determining the gaps analysis and resolution.
- Teams will be responsible for testing and updates.

## 9.0 Physical and Environmental Security

### 9.1. Physical and Environmental Security Objectives

- Prevent unauthorized access, damage and interference to state business premises.
- Prevent loss, damage or compromise of assets and interruptions to state business activities.
- Prevent compromise or theft of information and information processing facilities.

### 9.2. Physical Security General Controls

#### 9.2.1. General Physical Security

- Every user will take steps that are reasonable under the circumstances to maintain the confidentiality of IT assets.
- Users must also take reasonable steps to ensure that information and its associated data is protected, handled, stored, and disposed of in accordance with state and federal laws, policies and procedures.
- Adherence to IT asset handling requirements as specified within the policy are required to ensure that all IT assets are appropriately secured, as determined according to criticality and classification of the IT asset and/or contractual obligations, when unattended during and after work hours.
- Appropriate steps will be taken to prevent unauthorized disclosure of Internal Use Only, Confidential, and Restricted IT assets to unauthorized persons. This includes IT assets that might be disclosed verbally, physically, and/or electronically.
- Keys, security badges, tokens, and other means used to secure IT assets must not be left unattended during and after work hours.

#### 9.2.2. Removal of Property

- All users of a state physical resource will be required to relinquish said resource upon an appropriately authorized request.

- Physical assets containing or possibly containing information assets will not be removed from their appropriate locations without prior approval.

### **9.3. Secure Areas**

#### **9.3.1. Physical Security Perimeter**

Users will be informed of the following approved options for providing a physical security perimeter: Reception areas, security guard posts, magnetic card door locks, other, as determined.

#### **9.3.2. Physical Entry Controls**

- All state and local government employees, extra help and contractors are required to retain and display government issued identification badges while within a state or local government facility or location that is state-owned, managed or leased.
- Employees and other users are required to use their state or local government issued identification to gain physical access to government-owned, managed or leased facilities or location.
- Unless otherwise officially approved, visitors must be escorted while within a facility or location that is government owned, managed or leased.
- All users are fully responsible for the use of their government-provided identification and are prohibited from giving/loaning their identification to another person.
- Physical security alarms are regularly tested to ensure proper operation.
- Physical security professionals are responsible for review of access to secured locations on a periodic basis.

#### **9.3.3. Securing Offices, Rooms and Facilities**

- Access to government offices, computer machine rooms or other areas that contain Internal Use Only, Confidential or Restricted information will be physically restricted from access to only users with a state business security clearance.
- Telecommunication systems and network equipment will be secured with anti-theft devices when located in an open environment and not a limited access environment.
- Servers used to conduct state or local government business will be maintained within an identified data center.
- Access to systems development offices, telephone wiring closets, computer machine rooms, network switch rooms or other IT work areas will be physically restricted.
- Disaster recovery and backup equipment will be maintained in an offsite location.

#### **9.3.4. Working in Secure Areas**

- Physical access to state data centers and other secured locations will be restricted to authorized personnel only.
- Third party and vendor service personnel will be restricted from secure locations unless officially authorized, supervised and monitored.

### **9.4. Equipment Security**

[Click here to enter text.](#)

#### 9.4.1. Equipment Protection

- Equipment used for the state's core business must be protected to reduce the risks from environmental threats, hazards, and other opportunities for unauthorized access.
- Surplus and unused equipment is protected to reduce risks from unauthorized access.

#### 9.4.2. Power Supplies

Equipment used for the state's core business will be protected from power failures and other electrical anomalies.

#### 9.4.3. Cabling Security

Power and telecommunications cabling carrying data or supporting the state's core business will be protected from interception or damage.

#### 9.4.4. Security of Offsite Equipment

- Users will be fully responsible for the security of equipment within their possession when being used offsite.
- Portable devices that contain unencrypted Internal Use Only or Restricted information will not be checked as airline luggage, left with hotel porters or left in the possession of an individual or entity which does not have authorization.
- Users in the possession of a portable computing device will physically secure said device when not in use. For example, the device should be in a locked office, locked desk, locked vehicle or in the person's physical possession. This includes, but is not limited to the following: Laptops, Notebooks, other portable devices.
- Internal Use Only or Restricted information contained on a portable device will be encrypted prior to leaving the device unattended.

#### 9.4.5. Secure Disposal, Transport, or Re-use of Equipment

The preparation of any devices or equipment with electronic storage capability intended to be reused, such as used in a device or equipment other than that from which it originated, sent outside of a governments control for maintenance or repair such as to a vendor or other third-party, or disposed or otherwise discarded must adhere to the requirements specified within the policy to ensure that all IT assets and all licensed software has been completely removed or sanitized. Transport and reuse of equipment must also be in accordance with state standards.

### 10.0. Compliance

#### 10.1. Compliance Objectives

- Avoid breaches of any criminal and civil law, statutory, regulatory, or contractual obligations.
- Ensure compliance with this policy and related cybersecurity documentation.

#### 10.2. Compliance with Legal Requirements

##### 10.2.1. Identification of Applicable Legislation

- Applicable statutory, regulatory, legislative and contractual requirements will be identified and documented.
- Applicable statutory, regulatory, legislative and contractual requirements will be communicated to users to assist in ensuring user compliance.

#### 10.2.2. Intellectual Property Rights

- Users will be prohibited from using state IT resources to circumvent existing security devices in an unauthorized manner, or in a manner inconsistent with the license agreement.
- Users will be prohibited from disclosure of state Intellectual Property without appropriate approval.

#### 10.2.3. Legal Conflicts

All users will be responsible for providing immediate notification to an Information Security Manager in the event any section of this policy is identified as being in conflict with existing laws or regulations.

#### 10.2.4. Prevention of Misuse of IT Assets

- The use of state IT assets will be primarily for state business purposes and must be authorized for each user prior to receiving access.
- Use of state IT assets requires that all users comply with this policy. Violations of this policy are subject to disciplinary action under TSS OPM policies and procedures. Third parties found in violation may be subject to immediate termination of customer, partner, and/or vendor relationships.
- Non-enforcement of any policy requirement does not constitute its consent.
- Evidence provided for external legal proceedings will conform to the rules of evidence as laid down in the relevant law or in rules of the specific court in which the case will be heard.
- IT managers will be responsible for ensuring all IT assets, processes, and security procedures within their area or responsibility comply with this policy subject to auditing requirements.

### **10.3. System Audit Considerations**

#### 10.3.1. System Audit Controls

- System and process audit controls will be identified and documented.
- Notification of system and process audits will be fully communicated in a timely manner, prior to an audit taking place.
- System and process audits will be controlled and scope-limited to areas as specified within the associated notification.
- All access will be monitored and logged to produce a reference trail.
- All audit procedures, requirements and responsibilities will be documented.

#### 10.3.2. Protection and Use of State Network Security Audit Tools



- Use of network security audit tools on the state network will be strictly controlled. These tools include but are not limited to the following: Password cracking utilities, Port scanning utilities, Network sniffing utilities, Vulnerability detection scanners.
- Use of network security audit tools will be restricted to those users whose documented job roles and responsibilities require the periodic use of such resources.
- Use of network security audit tools will require approval from management prior to use.
- Use of a network security audit tool will provide monitoring and protection.

### Revision History

This standard shall be subject to review according to the Regulatory Spreadsheet to ensure relevancy.

Date	Description of Change	Reviewer
01/26/24	Moved from Draft to Final	Gary Vance, Chief Information Security Officer