
# State of Nevada

## State Information Security Program Policy

Revision Date:
**01/26/2023**

Approved by the:
**Nevada State Information Security Committee**
**State Chief Information Security Officer**
**State Chief Information Officer**

Published by the:
**Department of Administration,**
**Office of Information Security**

# *DOCUMENT PREFACE*

*Enterprise IT Services (EITS) has the statutory responsibility for establishing regulations and providing guidance to state agencies within the Executive Branch of Nevada State Government, for the protection of state information technology (IT) systems, and the data that those systems process, store, and transmit electronically. To support those responsibilities, EITS established the Office of Information Security (OIS) to develop appropriate security regulations and guidance, along with staff as subject matter experts to guide and assist state agencies in establishing agency security policies, standards, processes, and plans. [NRS 242.101]*

*To ensure the security concerns and needs of state agencies are included in the development of the State Information Security Program, a State Information Security Committee was established. This committee consists of representatives from state agencies with information technology backgrounds who have a vested interest in the development of the security policies, standards, and guidance.*

*As the State Information Security Program and the State Information Security Policy evolve, this document will be subject to review and update, which will occur biennially, or when changes occur that signal the need to revise the State Information Security Policy. These changes may include the following:*

- *Changes in roles and responsibilities;*
- *Release of new executive, legislative, technical, or State guidance;*
- *Identification of changes in governing policies;*
- *Changes in vulnerabilities, risks, or threats; or*
- *Legislative Audit findings that stem from security audit.*

*The National Institute of Standards and Technology (NIST) Special Publications 800 Series documents and the NIST Cybersecurity Framework (CSF) provide continuing guidance for the ongoing development and revision of this policy. These publications focus on security requirements and best practices for the Federal government, which requires state compliance due to the state receiving federal funds for information systems, and the state agencies accessing, processing, storing, or transmitting federal data.*

*In 2019, NRS 603A was amended to identify the Center for Internet Security (CIS) Controls as a baseline security framework for the Executive Branch of Nevada State Government. In situations where neither the state nor the agency has established a policy or standard on a specific security control, the requirements of NIST 800-53 Security and Privacy Controls and 800-100 Information Security Handbook will be the de facto state standard.*

*This policy has been developed, revised, and approved by the State Information Security Committee and the State Chief Information Security Officer, and has received final approval by the State Chief Information Officer. Revisions to this document are subject to the review and approval of the State Information Security Committee and the State Chief Information Security Officer, with final approval of the State Chief Information Officer. When revisions are approved, a new version of the State Information Security Policy will be issued, and all affected state agencies will be informed of the changes.*

*Additionally, compliance with this policy is mandatory. It is the State Chief Information Officer's direction that all state agencies within the Executive Branch of Nevada State Government comply with the direction of this policy.*

*In cases where a state agency cannot comply with any section of the State Information Security Policy, justifications for the noncompliance must be documented using the Exception Request process provided in Appendix A of this document. The Exception Request must be submitted to EITS, Office of Information Security, Chief Information Security Officer (CISO) for approval. Resulting risks from a deviation to policy must be documented in the appropriate Information Security Plan.*

## DOCUMENT HISTORY

| Version | Revision Date | Summary of Changes | Chapter Number/ Paragraph Number | Changes Made By |
|---|---|---|---|---|
| A | 10/28/2008 | Initial Document Release | Consolidate individual State security policies | D. Crutcher |
| B | 7/12/2011 | Revised background checks. | Section 3.4.2 | S. Ingersoll |
| C | 3/30/2017 | Review and Update – Rename 4.100000 to 100 | Multiple | EITS OIS |
| D | 6/27/2019 | Update format and revise for ADA compliance. | All | J. Hensley |
| E | 12/31/2020 | Add Chapter 6, CIS Controls (v7.1), Implementation Group 1, with related content moved to Chapter 6 or cross-referenced. Update terminology. | Multiple | J. Hensley |
| F | 9/01/2021 | Adopt CIS Controls v7.1, Implementation Group 2 sub-controls for Control 3 Continuous Vulnerability Management | Sections 5.11, 6.3 | J. Hensley |
| G | 7/13/2022 | Adopt changes to Boundary Defense and Web/Email Security | Sections 5.4, 6.7 and 6.12 | C. Bowman |
| H | 1/26/2023 | Adopt CIS Controls v7.1 for Control 2.7 Application Whitelist/Blacklisting | Section 6.2.7 | R. Dehnhardt |

### *Current Version Approved By*

| Title | Signature | Date |
|---|---|---|
| State Information Security Committee Chair/ State Chief Information Security Officer | Signature on file | 01/26/2023 |
| State Chief Information Officer | Signature on file | 01/26/2023 |

# TABLE OF CONTENTS

*THIS PAGE INTENTIONALLY LEFT BLANK*

# CHAPTER 1 INTRODUCTION

## 1.1 Purpose

The purpose of this policy is to define a set of minimum security requirements to protect state data and information technology (IT) systems that all state agencies within the Executive Branch of Nevada State Government must meet. Any state agency, based on the business needs and/or specific legal requirements, may exceed the security requirements put forth in this policy, but must, at a minimum, achieve the security levels required by this policy.

The primary objective of Nevada Information Security Program Policy is to:

- effectively manage the risk of security exposure or compromise within state agency IT systems;
- communicate the responsibilities for the protection of state agency information;
- establish a secure processing base and a stable processing environment within state agencies and throughout the state;
- reduce to the extent possible the opportunity for errors to be entered into an IT system supporting state agency business processes;
- preserve management's options in the event of state data, information, or technology misuse, loss, or unauthorized access; and
- promote and increase the awareness of information security in all state agencies and with all state employees.

## 1.2 Scope and Applicability

This State Information Security Program Policy provides a baseline of security policies for the State of Nevada. This policy establishes mandatory policies to ensure confidentiality, integrity, availability, reliability, and non-repudiation within the State's infrastructure and its operations.

This policy applies to all state agencies within the Executive Branch of Nevada State Government that operate, manage, or use IT capabilities in support of the business needs of the agency. This policy is applicable to state employees, contractors, and all other authorized users, including third parties, which have access to or manage state information. Where conflicts exist between this policy, a state agency policy, a federal policy, or any other policy a state agency is governed by, the more restrictive policy will take precedence.

This policy encompasses all systems for which the state has administrative responsibility, including systems managed or hosted by third parties on behalf of a state agency. It addresses all information, regardless of the form or format, which is created or used in support of business activities of state agencies.

## 1.3 Authority

The following state and federal statutes require states to protect their information resources and data by establishing information security programs and imposing special requirements for protecting personal information. The State Information Security Program Policy is the first step to ensuring compliance with these requirements:

- The Clinger-Cohen Act of 1996
- Federal Information Security Management Act of 2002
- Nevada Revised Statute (NRS) 242.101
- Nevada Revised Statute (NRS) 603A

# CHAPTER 2 OVERVIEW

This chapter provides an overview of this State Information Security Program Policy. It highlights the State's information security policy requirements, security responsibilities, and summarizes subsequent sections of this document.

Enterprise IT Services (EITS) is responsible for establishing a State-wide information security program to assure that each information system and associated facility provides a level of security that is commensurate with the risk and magnitude of the harm that could result from loss, misuse, disclosure, or modification of the information contained in the system. Each system's level of security must protect the confidentiality, integrity, and availability of the information, and comply with all security and privacy-related laws and regulations.

The EITS Office of Information Security (OIS) must develop and administer the State Information Security Program that meets statutory, regulatory, and State requirements, as well as the needs of the public. State agency Information Security Programs must comply with the State Information Security Program Policy and must meet the minimum standards set forth by this policy.

## 2.1 Document Organization

Security controls are delineated in three primary categories of administration, operational, and technical, which is the organizational structure of this document. NIST Special Publications, the NIST Cybersecurity Framework (CSF), and the Center for Internet Security (CIS) Controls provide ongoing guidance, direction, and best practices reflected in this policy.

- Chapter 3, **Security Administration Policies**, focuses on security administration, risk assessment/management, asset management, personnel security, security awareness training, and security plans.
- Chapter 4, **Operational Policies**, focuses on security methods for physical security, environmental security, media control, data integrity, equipment security, and security incident management.
- Chapter 5, **Technical Policies**, focuses on security controls that the computer executes, including identification/authentication, system/data access control, audit trails, network security, encryption, and patch management.
- Chapter 6, **CIS Controls,** focuses on those CIS Controls that have been integrated within this version of the State Information Security Program Policy, in a phased implementation of the CIS Controls, a statutory baseline security compliance framework in accordance with NRS 603A.

As noted in section 1.1, this document contains policies that satisfy state minimum security requirements based on industry best practices and federal guidelines.

## 2.2 Document Change Control

Requests for changes to this policy must be presented by the state agency to Enterprise IT Services, Office of Information Security. The requested change will be formally drafted and submitted to the State Information Security Committee for review and approval. Once approved by the committee, the State Information Security Officer (CISO) will submit the change to the State Chief Information Officer (CIO) for final approval. Once final approval is granted, the CISO will cause the change to occur in this document and distribute the change to all state agencies. It is the state agency's responsibility to communicate the approved changes to their organization.

## 2.3 Roles and Responsibilities

### 2.3.1 Enterprise IT Services (EITS), Office of Information Security (OIS)

The Enterprise IT Services (EITS), Office of Information Security (OIS) has the responsibility to:

A. establish, implement, administer, and oversee the State Information Security Program;

B. develop guidance documents for state agencies in developing various information security programs and plans;

C. provide subject matter expertise and assistance to state agencies in establishing specific information security programs; development of information security policies, standards, procedures, and plans; information security awareness training; and information security risk, vulnerability, and physical security assessments;

D. establish a state Information Security Incident Management program to assist state agencies in the determination if a security breach or incident has actually occurred, and to provide an initial administrative review of the incident;

E. chair the State Information Security Committee and provide direction and guidance to the committee in the development of the State Information Security Program, policies, and standards;

F. coordinate and obtain approval of all information security policies and standards from the State Information Security Committee and the State Chief Information Officer;

G. publish all approved information security policies, standards, and procedures;

H. ensure that the state security policies and standards are reviewed and revised every two years.

### 2.3.2 State Agencies

State agencies have the responsibility to:

A. establish and implement a departmental security program, to include policies, standards, and procedures, that is consistent with or exceeds the requirements of this policy, and commensurate with the risk and magnitude of harm of state information resources should unauthorized access, use, disclosure, disruption, modification, or destruction occur;

B. ensure information security management processes are integrated with the state agencies strategic and operational planning processes;

C. appoint an Information Security Officer (ISO) for the agency that will establish, administer, implement, and oversee an agency Information Security Program;

D. communicate state and agency security policies, standards, and procedures to all agency staff.

### 2.3.3 State Agency Information Security Officers

State Agency Information Security Officers (ISOs) have the responsibility to:

A. ensure the establishment, implementation, enhancement, monitoring, and enforcement of the federal, state, and agency information security policies and standards;

B. provide direction and leadership to his or her management and staff through the recommendation of security policies, standards, procedures, processes, and awareness programs to ensure that appropriate safeguards are implemented;

C. facilitate compliance with state and agency policies, standards, and procedures;

D. represent the agency on the State Information Security Committee.

## 2.4 Exceptions to State Policies or Standards

2.4.1 In cases where a state agency cannot comply with any section of the State Information Security Program Policy, justifications for the noncompliance must be documented using the Exception Request process provided in Appendix A of this document. The Exception Request must be submitted to EITS, Office of Information Security, Chief Information Security Officer (CISO) for approval.

2.4.2 Resulting risks from a deviation to policy must be documented in the appropriate Information Security Plan and accepted in writing by the requesting agency management.

2.4.3 OIS will provide an overview of the exception list to the committee on an annual basis.

## 2.5 Compliance

### 2.5.1 EITS, Office of Information Security (OIS)

The Enterprise IT Services (EITS), Office of Information Security (OIS):

A. Has oversight responsibilities to state agencies within the Executive Branch of Nevada State Government. The oversight is to provide a means to review and identify potential new or unaddressed vulnerabilities and to establish a baseline of a state agency and overall statewide security posture to build on to improve the overall security structure;

B. Does not have enforcement authority of state security policies and standards; however, OIS has the responsibility to escalate unaddressed security vulnerabilities as the Chief Information Security Officer (CISO) deems necessary to the State Chief Information Officer (CIO) for resolution per NRS 242.

C. Within the oversight responsibilities, may initiate security assessments of a state agency to identify new or unaddressed risks, threats, and vulnerabilities of the State's information processing environments and infrastructures;

D. Must provide the state agency with a written report of an assessment;

E. Can only release the results of an assessment to other compliance or audit organizations upon written approval of the assessed state agency.

### 2.5.2 State Agencies

State agencies must:

A. periodically review implemented security controls to verify compliance with state and agency security policies, standards, procedures, and processes;

B. establish enforcement and consequences for state and agency security controls.

## 2.6 References

Policies provided in this document are based on federal and industry standards and guidelines, including:

- National Institute of Standards and Technology (NIST) – Special Publications 800 Series
- OMB Circular A-130 – Management of Federal Information Resources
- Center for Internet Security (CIS) Controls v7.1, in accordance with NRS 603A

# CHAPTER 3 SECURITY ADMINISTRATION POLICIES

This State Information Security Policy is a statement that sets the direction, gives broad guidance, and defines the minimum requirements, ethics, responsibilities, and accepted behaviors required to establish and maintain a secure environment, and achieve State information security objectives. Compliance with this policy is mandatory. Exception requests can be submitted requesting an exception to a specific policy stated within this document but must be approved by the State Chief Information Security Officer (CISO).

## 3.1 Organizational and Functional Responsibilities

### 3.1.1 State Agencies

State agencies are responsible and required to:

A. Establish a framework to initiate and control the implementation of information security within their area of authority.

B. Appoint an Information Security Officer (ISO) for the state agency. The appointment may be based on the size of an agency, with individual ISOs appointed for each sub-organization within the agency, if the agency is large. The agency may also choose one ISO to represent and fulfill the ISO responsibilities for an entire agency, or to serve as the agency's lead ISO, to coordinate with all agency ISOs on behalf of the agency.

C. Establish a process to determine information sensitivity, based on best practices, State directives, legal and regulatory requirements, and identified security risks and vulnerabilities, to determine the appropriate level of protection for the information and the operational environment of the agency.

D. Ensure the agency structure is in place for:

1) establishment and implementation of agency information security program to include policies, standards, and procedures;

2) assigning information security responsibilities;

3) implementation of a security awareness program;

4) monitoring significant changes in the exposure of information assets to major threats, legal, or regulatory requirements;

5) coordination of security incidents with EITS, Office of Information Security;

6) consideration and planning of major initiatives to enhance information security within the agency;

7) ensure information security is included in the design of all automated applications;

8) communicating requirements of this policy and associated agency information security policies and standards to third parties, and addressing third party agreements.

### 3.1.2 State Agency Information Security Officer (ISO)

The state agency Information Security Officer (ISO) is responsible for the overall development, implementation, enhancement, monitoring, and enforcement of the agency Information Security Program policies, standards, and procedures.

The appointed state agency ISO is responsible for:

A. providing direction and leadership to the agency management and staff through the recommendation of security policies, standards, processes, and security awareness programs, to ensure that appropriate safeguards are communicated and implemented, and to facilitate compliance with the state and agency information security controls;

B. report and coordinate with EITS, Office of Information Security, security breaches or investigations;

C. coordinate and oversee agency security program activities and reporting processes in support of this State Information Security Program Policy and other security initiatives.

### 3.1.3 Agency Management

A. Agency management is responsible to support and provide resources needed to enhance and maintain a level of control consistent with the State and state agency Information Security Program Policies based on the level of identified risks.

B. Agency management has the following responsibilities in relation to the security of information:

1) ensure processes, policies, and requirements are identified and implemented relative to security requirements defined by the agency's business;

2) ensure the proper controls of information are implemented for which the state agency business has assigned ownership responsibility based on the identified classification designation;

3) ensure the participation of the state agency ISO and technical staff in identifying and selecting appropriate and cost-effective security controls and procedures, and in protecting information assets;

4) ensure participation of the state agency ISO in the development, selection, and implementation of all Request for Proposals and Contracts involving information technology resources;

5) ensure appropriate security requirements for user access to automated information are defined for files, databases, and physical devices assigned to their areas of responsibilities;

6) ensure critical data and recovery plans are backed up and kept at a secured off-site storage facility, and that recovery of backed-up media will work if and when needed.

### 3.1.4 State Employees

A. All state employees have the responsibility to protect state information and resources, including passwords, and to comply with the State and employee state agency Information Security Program Policies, Standards and Procedures.

B. All state employees must report suspected security incidents to the appropriate manager and to their agency's Information Security Officer (ISO).

## *3.2 Information Security Policy*

### 3.2.1 General

A. All information on state systems or infrastructure, regardless of the form or format, which is created, acquired, stored, transported, or used in support of state agency's business activities, must only be used for official state business. State information is an asset and must be protected from its creation, through its useful life, and to its authorized disposal.

B. State information must be maintained in a secure, accurate, and reliable manner and be readily available for authorized use.

C. State information/data must be classified and protected based on its importance to the business activities and risks to any given state agency.

D. Access to state information and information systems must be granted to an individual for only the information or systems required to accomplish the duties of their position.

### 3.2.2 Individual Accountability

Individual accountability is the cornerstone of any security program. Any person having authorized access to state information must:

A. be assigned unique User ID(s) and password(s) for access into state information systems. The original recipient of the User ID(s) and password(s) must not share their User ID or password;

B. only use state information for official business;

C. only access IT systems and information for which they are authorized;

D. be responsible to reasonably protect against unauthorized activities performed under their User ID;

E. report suspected or actual security breaches or incidents, inappropriate content or system access/activity to the state agency's management and ISO, or to the EITS, Office of Information Security.

### 3.2.3 Confidentiality – Integrity – Availability

All state agency information must be protected from unauthorized access to help ensure the information's confidentiality and maintain its integrity. State agencies must:

A. classify and secure information within their jurisdiction based on the information's value, sensitivity to disclosure, consequences of loss or compromise, and ease of recovery.

B. define appropriate processes and develop recovery plans, and implement those processes to ensure the reasonable and timely recovery of all state agency information, applications, systems, and security regardless of computing platform, should that information become corrupted, destroyed, or unavailable for a defined period.

### 3.2.4 State Agency Security Program

A. State agencies must approve, adopt, publish, and communicate to all employees a statement on Information Security detailing management commitment and organizational approach to managing information security within the agency.

B. State agencies must periodically review the statement at established intervals or when significant changes occur to update, reinforce, and ensure the continued management commitment and approach for the agency's information security program.

## *3.3 Organizational Security Policy*

### 3.3.1 Management Commitment to Information Security

A. Management must actively support security efforts within the agency through clear direction, demonstrated commitment, and explicit assignment of information security responsibilities to the agency ISO.

B. Information security initiatives and activities should be coordinated with representatives from different areas within the agency with relevant roles and job functions. All information security responsibilities should be clearly defined.

### 3.3.2 Information Security Function

The purpose and mission of the Information Security function is to:

A. develop, deploy and maintain an information security architecture that will provide security policies, mechanisms, processes, standards, and procedures that meet current and future business needs of the state agency;

B. provide information security consulting to the state agency regarding security threats that could affect the agency's computing and business operations, and make recommendations to mitigate the risks associated with those threats;

C. assist management in the implementation of security measures that protect the IT infrastructure, while at the same time meet the business needs of the state agency;

D. develop and implement security training and awareness programs that educate employees, contractors, and vendors with regard to the agency's information security requirements;

E. participate in the development, implementation, maintenance, and testing of Continuity of Operations Plans (COOP), processes and techniques to ensure the continuity of the agency's business and security controls, in the event of an extended period of computing resource unavailability;

F. report to management and the EITS, Office of Information Security, breaches of security controls, and implement additional compensating controls when necessary to help ensure security safeguards are maintained.

### 3.3.3 Role and Responsibility of the State Agency Information Security Officer

The state agency Information Security Officer (ISO) is responsible for performing, at a minimum, the following tasks:

A. develop or coordinate the development and implementation of state agency information security plans, policies, standards, procedures, and other control processes that meet the business needs of the state agency;

B. provide security consultation to the state agency management with regard to information security practices and controls;

C. work closely with agency management to ensure security measures are implemented to meet policy requirements;

D. evaluate new security threats and countermeasures that could affect the state agency and make appropriate recommendations to management of the state agency to mitigate the risks;

E. inform and coordinate reports of suspected information security incidents or breaches, unauthorized use, and unauthorized disclosure of state information or personal identification information with state agency management and the EITS, Office of Information Security (OIS). OIS will provide support to all state agencies suspecting a breach or incident by performing an initial administrative investigation of the associated IT resource(s), maintain the required chain of custody of all materials, equipment, and evidence, and provide a neutral independent third party review and report to management to assist in making informed decisions on further actions;

F. ensure appropriate follow-up to security violations is conducted;

G. establish and provide appropriate security awareness and education to all state agency employees, and where appropriate third party contractors;

H. be aware of laws and regulations that could affect the security controls and classification requirements of the state agency's information;

I. support, develop, and accomplish actions required by the state agency ISO as defined in other parts of this State Information Security Program Policy;

J. represent the agency on the State Information Security Committee.

## *3.4 Personnel Security*

### 3.4.1 General

The Personnel Security process begins with a review of the user's position needs, relevant policies, regulations, standards, and threats for a defined environment.

A. All state agencies must comply with existing state and federal laws and regulations that impose significant responsibilities on employees for the security of information.

B. All state agencies must establish an Acceptable Use Policy and obtain a signature from the employee indicating acknowledgement of the rules prior to access being granted to information or information systems.

### 3.4.2 Employment Screening of State Employees and IT Contractors

A. Fingerprint-based background checks must be conducted on all persons hired, promoted, or contracted for IT services determined to be sensitive. This requirement is supported by NRS 239B, Disclosure of Personal Information to Governmental Agencies.

B. Background checks must consist of an approved online national records check (if interim access is necessary before receiving the background check results) and a fingerprint-based background check. A conviction in any jurisdiction of any crime involving moral turpitude or indication of lack of business integrity or honesty, whether denominated a felony or misdemeanor, must be considered to be an unfavorable result of a background check. Any unfavorable results from a background check must be submitted to the agency head.

C. Unfavorable results from a background check must not be an automatic cause to refuse employment or cause for termination. The agency head, after consulting with the agency personnel office, has the final decision on action to be taken or not taken based on the results of the report and disposition of court information.

### 3.4.3 Acceptable Use

A. Acceptable Use Policy must be developed for the agency's IT resources, including computers, telecommunications equipment, software, and other data/information services. The policy must provide specific rules for the access and use of the agency's IT systems and information, to include acceptable use of the Internet, email, personal use of assigned IT systems, and use of mobile devices.

B. Each employee, contractor, and vendor must sign and acknowledge receipt of the Acceptable Use Policy prior to granting access to agency IT systems or information, with annual review and acknowledgement.

### 3.4.4 Separation of Duties

Identified sensitive positions must have critical functions divided among different individuals, whenever possible, to ensure that no individual has all necessary authority or information access that could result in fraudulent activities and misuse of confidential/privileged information.

### 3.4.5 Resignation/Termination

A. A process must be developed to establish, implement, and maintain procedures for processing terminations, both voluntary and involuntary, of employees. The procedures for processing termination involving sensitive positions or access to sensitive information must be more restrictive than those in non-sensitive positions.

B. Involuntary termination of an employee must cause immediate revocation of all system and information access privileges.

## *3.5 Security Awareness [Moved to Section 6.17]*

*Security Awareness has been moved to Chapter 6 CIS Controls in Section 6.17 Security Awareness and Training Program.*

## *3.6 Asset Protection [See Related Sections 6.1, 6.2, and 6.13]*

3.6.1 State agencies must establish and maintain protection of their information technology assets, including hardware, software, digital data, and documentation essential to information security.

3.6.2 Where identified, asset inventories have been moved to the relevant sections of Chapter 6 CIS Controls:

A. Section 6.1, Inventory and Control of Hardware Assets.

B. Section 6.2, Inventory and Control of Software Assets.

C. Section 6.13, Data Protection, for inventories of digital data, sometimes referred to by CIS as “information assets”.

D. Security Documentation, including but not limited to system documentation, operational and support procedures, information security plans, contingency and continuity of operations plans, and other documents required to assure information security.

3.6.3 Accurate and up-to-date asset inventories must be incorporated by reference in agency Information Security and Contingency Plans; asset inventories must be readily available for reference and use with these agency security plans.

## *3.7 Risk Assessment and Risk Management*

Risk Assessments are the foundation to establish an effective and appropriate Information Security Program to define and establish necessary controls and processes, commensurate with the level of risks, necessary to provide protection to a state agency’s information processing infrastructure and information.

### 3.7.1 Risk Assessments

A. A full risk assessment must be conducted at each state agency to determine the risks, threats, and vulnerabilities to their IT systems, applications, information, and operational controls and processes. The full risk assessment must include:

1) **security administration assessment** of information security controls, policies, standards, procedures and processes, data classification, and information security plans;

2) **vulnerability assessments** of IT systems and applications, to include networks, servers, wireless, web sites, email systems, and data access controls;

3) **physical security assessments** of agency offices for physical access and environmental controls.

B. Initial risk assessments must be conducted by an independent party with expertise in information security and specific technical expertise.

C. Results of the assessments must be used to determine the level of protection to be provided and to develop, administer, implement, and maintain the state agency Information Security Program which must consist of agency security policies, standards, procedures, processes, internal controls, and continuity of operation plans.

D. The appropriate assessment must be conducted prior to the introduction of a new system application or when a major change occurs to the operating environment.

### 3.7.2 Self-Assessments

State agencies must conduct a self-assessment of their information security controls at least annually and revise their controls according to identified inadequacies or new risks.

### 3.7.3 Independent Review of State Agency Information Security Program

State agencies must have a periodic independent review of established security controls. The Enterprise IT Services (EITS), Office of Information Security (OIS) should be the first resource considered for the independent reviews.

## *3.8 Information Security Plans*

Each state agency must develop Information Security Plans to document the administrative security controls and the controls for each major application and for general support systems.

### 3.8.1 Administrative Security Plan

A. Each state agency must develop and document the administrative security controls established, to include but not limited to controls put in place for security management, personnel security, and security awareness training.

B. The Administrative Security Plan must be reviewed and revised at least biennially.

### 3.8.2 Major Application Security Plan

A major application is defined as an application that is critical to the business function of the state agency and/or requires special attention to security, due to the risk and magnitude of impact to the state agency should the application be subject to unauthorized access, manipulation, or disclosure of information.

A. Each state agency must develop and document the security controls designed within each major application of the agency. The plan must include the controls incorporated within the system design and any additional controls.

B. Major Application Security Plans must be developed prior to any new application being put into production.

C. Major Application Security Plans must be reviewed at least biennially or when a major change is made to the application.

### 3.8.3 Major Support System Security Plan

A major support system is defined as an information system requiring special management attention because of its importance or criticality to the state agency's business, and plays a significant role in the administration of the agency critical programs, finances, property, or other critical resource.

A. Each state agency must develop and document the security controls designed within each major support system of the agency. The plan must include the controls incorporated within the system design and any additional controls.

B. Major Support System Security Plans must be developed prior to any new system being put into production.

C. Major Support Security Plans must be reviewed at least biennially or when a major change is made to the system.

### 3.8.4 General Support System Security Plan

General support systems are defined as one or a combination of multiple systems that support the state agency, such as a Local Area Network (LAN), Wide Area Network (WAN), or email server.

A. Each state agency must develop and document the security controls established for each general support system of the agency.

B. General Support System Security Plans must be developed prior to a new system is put into production.

C. General Support System Security Plans must be reviewed at least biennially or when a major change is made to the system.

## *3.9 Contingency Planning*

State agencies must implement and maintain a business continuity management process to minimize the impact on the organization, counteract interruptions to business activities, and protect critical business processes from the effects of major failures of information systems.

### 3.9.1 Major Application Contingency Plan

A. State agencies must develop a contingency plan for each major application that defines the backup and recovery procedures specific to each application.

B. Contingency plans must include all pertinent information required to identify any applications that the major application relies on to accomplish processing, or any applications that the major application supplies data or processing capabilities to.

C. State agencies must test the procedures defined in the application contingency plans at least biennially or when a major changed to the application has been implemented.

### 3.9.2 Major System Contingency Plan

A. State agencies must develop a contingency plan for each major system that defines the backup and recovery procedures specific to each application.

B. Contingency plans must include all pertinent information required to identify any applications that the major system relies on to accomplish processing, or any applications that the major application supplies data or processing capabilities to.

C. State agencies must test the procedures defined in the application contingency plans at least biennially or when a major changed to the application has been implemented.

### 3.9.3 General Support System Contingency Plan

A. State agencies must develop a contingency plan for each general support IT system that defines the backup and recovery procedures specific to each system.

B. Contingency plans must include all pertinent information required to identify all applications that resides on the general support system, operating system, users, datasets, and responsibilities for the backup and recovery of the system.

C. State agencies must test the procedures defined in the general support system contingency plans at least biennially or when a major changed has been implemented.

*THIS PAGE INTENTIONALLY LEFT BLANK*

## 4.1 Physical Security and Environmental Controls

### 4.1.1 Physical Access

Appropriate controls must be implemented to:

A. limit access to rooms, work areas/spaces, and facilities that contain the agencies information systems, networks, and data to authorized personnel only;

B. deter, detect, monitor, restrict, and regulate access to sensitive areas at all times;

C. ensure controls are commensurate with the level of risk, and must be sufficient to safeguard the IT resources against possible theft, loss, destruction, accidental damage, hazardous conditions, fire, malicious actions, and natural disaster.

### 4.1.2 Physical Security

Appropriate controls must be implemented to ensure that rooms, work areas/space, and facilities that contain IT resources that process, transmit, or store sensitive or privacy information are protected from unauthorized access.

### 4.1.3 Visitor Access

A. Controls must be implemented that restrict and control visitor access at all times to rooms, work areas/spaces, and facilities that contain agency IT resources.

B. Visitor Logs must be established to record visitor access to work areas/spaces that contain sensitive IT equipment, such as servers and communications equipment room.

### 4.1.4 Fire Protection

All systems and networks must be protected against the danger of water damage due to leakage from building plumbing lines, shut-off valves, and other similar equipment through the location of equipment or covers for the equipment.

### 4.1.5 Supporting Utilities

A. An alternate power supply, such as a generator, must be installed to protect large critical IT systems from power spikes, brownouts, or outages.

B. State agency servers must be protected by an appropriately sized uninterruptible power supply.

C. Desktop computers supporting critical functions of a state agency must be protected by an uninterruptible power supply.

### 4.1.6 Data Centers

All servers collecting, processing, and/or storing sensitive information, and servers supporting production services that collect, process, or store sensitive information, must be housed in a properly rated data center with physical and environmental controls appropriate for the criticality of the information and services.

## 4.2 Equipment Security

### 4.2.1 Workstations

Appropriate controls must be implemented commensurate with the sensitivity level of the data accessed, processed, or stored on the workstation.

### 4.2.2 Laptops and Other Mobile Computing Devices Encryption [Moved to Section 6.13.6]

*Mobile device encryption has been moved to Section 6.13.6 in Chapter 6 CIS Controls, Section 6.13.6 Encrypt Mobile Device Data.*

### 4.2.3 Non-State Hardware and Software [Moved to Sections 6.1.6 and 6.2.6]

*Inventory and control of personally owned or non-state hardware and software has been moved to the relevant* sections of Chapter 6 CIS Controls:

A. *Section 6.1.6 Address Unauthorized Hardware Assets*

B. *Section 6.2.6 Address Unapproved Software Assets*

### 4.2.4 Hardware Security

Hardware products must provide dependable, cost-effective security controls and features, and preserve the integrity of the security features provided through the system software.

### 4.2.5 Hardware/Software Maintenance

A. Agency hardware and software must be tested, documented, and approved prior to being placed into production.

B. Maintenance must only be provided by authorized personnel.

## 4.3 Media Control

Agencies must establish procedures to protect media input/output data and system documentation from unauthorized disclosure, modification, removal, and destruction.

### 4.3.1 Media Protection

Electronic media (e.g., disk drives, CDs, internal and external hard drives, and portable devices) must be protected, including backup media, removable media, and media containing sensitive information, from unauthorized access.

### 4.3.2 Media Marking

Media containing data must be marked and labeled to indicate the sensitivity level of the data.

### 4.3.3 Sanitization and Disposal of Information

Methods must be developed and documented to ensure that sanitization and disposal of media is commensurate with the sensitivity and criticality of the data residing on the storage devices, equipment, and hardcopy.

### 4.3.4 Input/output Controls

Physical, administrative, and technical controls must be established and implemented to prevent unauthorized entry into office suites, operations, data storage, library, and other restricted areas to restrict the unauthorized removal of media.

## *4.4 Data Integrity [See Related Section 6.10]*

### 4.4.1 Backup, Recovery, and Data Storage Procedures [Moved to Section 6.10]

*Backup, Recovery and Data Storage Procedures has been moved to Chapter 6 CIS Controls in Section 6.10 Data Recovery Capabilities.*

### 4.4.2 Data Integrity and Validation Controls

Systems and networks must be equipped with data integrity and validation controls to provide assurance that information has not been altered.

### 4.4.3 Technical and Operational Documentation

Documentation for all systems, networks, and applications must be developed, readily available to appropriate personnel, secured, and up to date for routine security audits, tests, and unexpected events such as system disruptions, failures, or outages.

## *4.5 Hardware Configuration Management [See Related Section 6.5]*

4.5.1 State agencies must establish, implement, and maintain documented security configuration standards for all authorized systems and networks hardware.

4.5.2 Documented configuration management procedures must include processes for the request, approval, implementation, and documentation of all hardware configuration changes.

## *4.6 Software Licenses [Moved to Section 6.2.2]*

*Software Licenses has been moved to Chapter 6 CIS Controls in Section 6.2.2 Ensure Software Is Supported by Vendor.*

## *4.7 Software Development and Maintenance*

4.7.1 Separate development, test, and production environments must be established on state systems.

4.7.2 Processes must be documented and implemented to control the transfer of software from a development environment to a production environment.

4.7.3 Development software and tools must be maintained on computer systems isolated from a production environment.

4.7.4 Access to compilers, editors, and other system utilities must be removed from production systems.

4.7.5 Controls must be established to issue short-term access to development staff, to correct problems with production systems allowing only necessary access.

4.7.6 Security requirements and controls must be identified, incorporated in, and verified throughout the planning, development, and testing phases of all software development projects. Security staff must be included in all phases of the System Development Lifecycle (SDLC) from the requirement definition phase through implementation phase.

4.7.7 Vulnerability testing must be conducted on all systems prior to being placed into production.

## *4.8 Security Incident Management [See Related Section 6.19]*

4.8.1 State agencies must establish and maintain an incident response capability to include preparation, identification, containment, eradication, recovery, and follow-up capabilities, to ensure effective recovery from incidents.

4.8.2 State agencies must adhere to a standard methodology for resolving information security events, to ensure a consistent and effective method is applied.

4.8.3 A process of evaluation and continual improvement must be applied to information security events after completion.

4.8.4 Individuals must report any observed or suspected information security events or weaknesses to their manager or agency Information Security Officer.

4.8.5 A formal report must be developed following the discovery of an event or weakness, to allow for timely corrective action.

4.8.6 A security incident involving the disclosure of personal identifiable information (PII) must follow the notification rules of NRS 603A.220, Disclosure of Breach of Security of System Data, Methods of Disclosure.

4.8.7 State agencies must promptly notify the EITS, Office of Information Security of a suspected or actual disclosure of Personal Identifiable Information. The EITS, OIS must be included in the investigation and corrective actions.

## 5.1 Identification and Authentication

Users of state IT systems and networks must be individually identified and accountable for all actions on those systems accessed by that identification.

### 5.1.1 Identification

Each authorized user of state systems and networks must have a unique User ID.

### 5.1.2 Password

A. Logical password controls must be used in conjunction with a unique User ID.

B. Each authorized user of state systems and networks must have a unique password that is to remain confidential, not to be shared with other users, system maintenance personnel, and/or contractors.

C. Passwords granting access to sensitive data or elevated access to the system must not be saved, stored, or hard-coded in any system or application.

## 5.2 Data Access Controls

State IT systems and networks must have logical access controls to provide protection from unauthorized access, alteration, loss, disclosure, and availability of information.

### 5.2.1 Review and Validation of User Accounts [See Related Sections 6.16.8 and 6.16.9]

User accounts must be reviewed quarterly to ensure the continued need for access to a system.

### 5.2.2 Automatic Account Lockout

State IT systems and networks must have automatic account lockout after a third failed attempt to log-in to the system or network.

### 5.2.3 Automatic Session Timeout [Moved to Section 6.16.11]

*Automatic Session Timeout has been moved to Chapter 6 CIS Controls in Section 6.16.11 Lock Workstation Sessions After Timeout.*

### 5.2.4 Warning Banner

State IT systems and networks must display an agency or State Attorney General's Office approved sign-on warning banner at all system access points.

## 5.3 Audit Trails [See Related Section 6.6.2]

5.3.1 Audit logs must be recorded, retained, and regularly analyzed to identify unauthorized activity.

## 5.4 Network Security

### 5.4.1 Network Management

Network infrastructure must be managed and controlled to protect systems and applications using the network, including information in transit.

### 5.4.2 Remote Access and Dial-In [See Related Section 6.12.11]

Remote access and dial-in security controls must be implemented and enforced to provide protection for information stored, accessed, transmitted, and received across public and private networks.

### 5.4.3 Network Security Monitoring

All state systems and networks must have security event-monitoring.

### 5.4.4 Firewalls

All incoming and outgoing connections from state systems and networks to the Internet and extranets must always be made through a firewall.

### 5.4.5 Internet Security

Connectivity of state systems and networks to the Internet must be within a framework of effective technical security controls using firewalls and gateways that provide external network access via Internet Service Providers (ISP) and other public or designated external agencies.

## 5.5 Malicious Code Protection [See Related Section 6.8]

All state systems and networks must have protection programs to minimize the risk of intruding malicious code (e.g., viruses, worms, Trojan horses).

## 5.6 System-to-System Interconnection

Each state agency must implement a plan or schedule to establish, maintain, and terminate interconnections among state agency systems and networks that are operated by different state or federal organizations.

## 5.7 Patch Management [Moved to Sections 6.3.4 and 6.3.5]

*Patch Management has been moved to Chapter 6 CIS Controls in Sections 6.3.4 Deploy Automated Operating System Patch Management Tools and 6.3.5 Deploy Automated Software Patch Management Tools.*

## 5.8 Communications Security

### 5.8.1 Voice Communications

Security controls must be implemented to provide adequate protection at the system and environmental levels.

### 5.8.2 Data Communications

Controls must be established to ensure that sensitive data is protected from unauthorized access during transmission.

### 5.8.3 Wireless Communications [See Related Section 6.15]

A. Wireless networks must not be connected to wired networks except through appropriate controls (e.g., Virtual Private Network (VPN) port).

B. Wireless LANS must not be used to transmit, process, or store sensitive information unless protected with encryption standards that are commensurate with the sensitivity level of the data.

### 5.8.4 Peer-to-Peer File Sharing

Peer-to-Peer file sharing is permitted by state agencies using an approved statewide application with a secure methodology to facilitate authorized internal and external access. Use of other peer-to-peer file sharing applications must be approved by the State CISO.

### 5.8.5 Instant Messaging

Instant messaging is permitted by state agencies using an approved statewide application with a secure methodology to facilitate authorized internal and external access. Use of other instant messaging applications must be approved by the State CISO.

### 5.8.6 Video Conferencing

Adequate controls must be implemented to ensure that appropriate transmission protections are in place commensurate with the highest sensitivity of the information to be discussed over the video conference.

## 5.9 Information Security Architecture [1]

5.9.1 State agencies must develop and document an information security architecture for information systems that:

A. Describes the overall philosophy, requirements, and approach to be taken with regard to protecting the confidentiality, integrity, and availability of state information;

B. Describes how the information security architecture is integrated into and supports the agency information architecture; and

C. Describes any information security assumptions about, and dependencies on, external services.

5.9.2 State agencies must review and update the information security architecture to reflect updates in the agency architecture; and

5.9.3 State agencies must ensure that planned information security architecture changes are reflected in the agency information security plan, the agency information security architecture, and agency procurements and acquisitions.

## 5.10 Email Security [See Related Section 6.7.1]

### 5.10.1 Email Security

A. State email services must have security controls implemented to protect against malicious code attacks and ensure that email services are not used to relay unauthorized messages.

B. State email services must be used for only official state business.

### 5.10.2 Personal Email Accounts

Personal email accounts must not be accessed using state systems and networks without the agency management approval.

## 5.11 Security Testing and Vulnerability Assessment [See Related Section 6.3]

All state systems and networks must have vulnerability scans and/or penetration tests to identify security threats prior to the initiation of a new system or network.

---

[1] State Information Security Policy Section 5.9 Information Security Architecture was added at the recommendation of the SISC workgroup formed in 2019 to reorganize and renumber state security policy statements, standards, and procedures, on security architecture and design that are broader in scope than those policy statements more narrowly focused on individual security control families. Examples of security architecture standards that would be linked to this policy statement include standards on Data Security Architecture and Cloud Services.

The language is based on NIST 800-53r4, PL-8 Information Security Architecture, which applies to Moderate- and High-Impact security control baselines.
https://nvd.nist.gov/800-53/Rev4/control/PL-8

# CHAPTER 6 CIS CONTROLS

In 2019, NRS 603A was amended to establish the Center for Internet Security (CIS) Controls as a state security compliance framework for state agencies. In accordance with this revised statute, the State Information Security Program Policy has been updated to include CIS Controls as part of the state's baseline security controls. As of Version 7.1, CIS has organized the CIS Controls framework into three Implementation Groups, which CIS recommends be implemented in three consecutive phases. CIS defines the CIS Controls Implementation Group 1 as the first set of controls and sub-controls which must be implemented before beginning subsequent phases for Implementation Groups 2 and 3.

This chapter contains those CIS controls and sub-controls identified by CIS as belonging to Implementation Group 1 and selected sub-controls belonging to Implementation Group 2. The section and sub-section numbering in this chapter is intentionally aligned with and corresponds to the CIS numbering of controls and sub-controls. The CIS controls and sub-controls listed below are from CIS Controls v7.1.

## 6.1 Inventory and Control of Hardware Assets [See Related Section 3.6]

### 6.1.1 Reserved [IG2]

*This section is reserved for CIS Controls Implementation Group 2 (IG2), 1.1.*

### 6.1.2 Reserved [IG3]

*This section is reserved for CIS Controls Implementation Group 3 (IG3), 1.2.*

### 6.1.3 Reserved [IG2]

*This section is reserved for CIS Controls Implementation Group 2 (IG2), 1.3.*

### 6.1.4 Maintain Detailed Hardware Asset Inventory

*CIS 1.4: Maintain an accurate and up-to-date inventory of all technology assets with the potential to store or process information. This inventory shall include all hardware assets, whether connected to the organization's network or not.*

State agencies must maintain an accurate and up-to-date inventory of all hardware assets, including but not limited to, computer equipment, communications equipment, removable media, and other equipment, whether connected to the agency's network or not.

### 6.1.5 Reserved [IG2]

*This section is reserved for CIS Controls Implementation Group 2 (IG2), 1.5.*

### 6.1.6 Address Unauthorized Hardware Assets [Moved From Section 4.2.3]

*CIS 1.6: Ensure that unauthorized assets are either removed from the network, quarantined, or the inventory is updated in a timely manner.*

A. State agencies must address unauthorized hardware assets in a timely manner by removing hardware from the network, quarantining the hardware, or updating the hardware asset inventory.

B. Personally Owned or Non-State Hardware

1) State agencies must control the use of personally owned or non-state hardware to process, access, or store state data. Personally owned or non-state hardware includes, but is not limited to, personal computers, mobile devices, and related equipment.

2) Personally owned or non-state hardware must not be used to process, access, or store sensitive information, or to be connected to the state enterprise or state agency's systems or network without the written authorization of the appropriate agency management and/or Information Security Officer.

### 6.1.7 Reserved [IG2]

*This section is reserved for CIS Controls Implementation Group 2 (IG2), 1.7.*

### 6.1.8 Reserved [IG3]

*This section is reserved for CIS Controls Implementation Group 3 (IG3), 1.8.*

## *6.2 Inventory and Control of Software Assets [See Related Section 3.6]*

### 6.2.1 Maintain Inventory of Authorized Software

*CIS 2.1: Maintain an up-to-date list of all authorized software that is required in the enterprise for any business purpose on any business system.*

State agencies must maintain an accurate and up-to-date inventory of all authorized software, including but not limited to, application software, system software, development tools, and utilities.

### 6.2.2 Ensure Software Is Supported by Vendor [Moved From Section 4.6]

*CIS 2.2: Ensure that only software applications or operating systems currently supported and receiving vendor updates are added to the organization's authorized software inventory. Unsupported software should be tagged as unsupported in the inventory system.*

State agencies must establish controls to ensure that:

A. Only state approved and properly licensed software assets are added to the software assets inventory.

B. Only software and operating systems currently supported and receiving vendor updates are added to the software assets inventory.

C. Unsupported software must be identified or tagged as unsupported in the software assets inventory.

### 6.2.3 Reserved [IG2]

*This section is reserved for CIS Controls Implementation Group 2 (IG2), 2.3.*

### 6.2.4 Reserved [IG2]

*This section is reserved for CIS Controls Implementation Group 2 (IG2), 2.4.*

### 6.2.5 Reserved [IG3]

*This section is reserved for CIS Controls Implementation Group 3 (IG3), 2.5.*

### 6.2.6 Address Unapproved Software [Moved From Section 4.2.3]

*CIS 2.6: Ensure that unauthorized software is either removed or the inventory is updated in a timely manner.*

A. State agencies must address unauthorized software assets in a timely manner by removing unauthorized software from the system, quarantining the software, or updating the software assets inventory.

B. Personally Owned or Non-State Software

1) State agencies must control the use of personally owned or non-state software to process, access, or store state data. Personally owned or non-state software includes, but is not limited to, software, Internet service providers, personal email providers (e.g., Yahoo, Hotmail), and personal library resources.

2) Personally owned or non-state software must not be used to process, access, or store sensitive information, or to access the state enterprise or state agency's systems or network without the written authorization of the appropriate agency management and/or Information Security Officer.

### 6.2.7 Application Whitelisting/Blacklisting

*CIS 2.7: Utilize application whitelisting technology on all assets to ensure that only authorized software executes and all unauthorized software is blocked from executing on assets.*

The state shall establish and maintain a blacklist of hardware, software, vendors, and services that are banned from use on State of Nevada assets due to security concerns. Agencies may establish and maintain whitelists and blacklists for their use at their discretion. Agency whitelists shall not allow an item that is banned by the State blacklist.

### 6.2.8 Reserved [IG3]

*This section is reserved for CIS Controls Implementation Group 3 (IG3), 2.8.*

### 6.2.9 Reserved [IG3]

*This section is reserved for CIS Controls Implementation Group 3 (IG3), 2.9.*

### 6.2.10 Reserved [IG3]

*This section is reserved for CIS Controls Implementation Group 3 (IG3), 2.10.*

## 6.3 Continuous Vulnerability Management [See Related Section 5.11]

### 6.7.1 Use of Fully Supported Browsers and Email Clients [See Related Section 5.10]

*CIS 7.1: Ensure that only fully supported web browsers and email clients are allowed to execute in the organization, ideally only using the latest version of the browsers and email clients provided by the vendor.*

State agencies must ensure that only fully supported web browsers and email clients are allowed to execute in the organization, ideally only using the latest version of the browsers and email clients provided by the vendor.

### 6.7.2 Disable Unnecessary or Unauthorized Browser or Email Client Plugins

*CIS 7.2: Uninstall or disable any unauthorized browser or email client plugins or add-on applications.*

State agencies must uninstall or disable any unauthorized browser or email client plugins or add-on applications.

### 6.7.3 Limit Use of Scripting Languages in Web Browsers and Email Clients

*CIS 7.3: Ensure that only authorized scripting languages are able to run in all web browsers and email clients.*

State agencies must ensure that only authorized scripting languages are able to run in all web browsers and email clients.

### 6.7.4 Maintain and Enforce Network-Based URL Filters

*CIS 7.4: Enforce network-based URL filters that limit a system's ability to connect to websites not approved by the organization. This filtering shall be enforced for each of the organization's systems, whether they are physically at an organization's facilities or not.*

State agencies must enforce network-based URL filters that limit a system's ability to connect to websites not approved by the agency. This filtering shall be enforced for each of the agency's systems, whether they are physically at an agency's facilities or not.

### 6.7.5 Subscribe to URL-Categorization Service

*CIS 7.5: Subscribe to URL-categorization services to ensure that they are up-to-date with the most recent website category definitions available. Uncategorized sites shall be blocked by default.*

State agencies must subscribe to URL-categorization services to ensure that they are up-to-date with the most recent website category definitions available. Uncategorized sites shall be blocked by default.

### 6.7.6 Log All URL Requests

*CIS 7.6: Log all URL requests from each of the organization's systems, whether on-site or a mobile device, in order to identify potentially malicious activity and assist incident handlers with identifying potentially compromised systems.*

State agencies must log all URL requests from each of the agency's systems, whether on-site or a mobile device, in order to identify potentially malicious activity and assist incident handlers with identifying potentially compromised systems.

### 6.7.7 Use DNS Filtering Services

*CIS 7.7: Use Domain Name System (DNS) filtering services to help block access to known malicious domains.*

Domain Name System (DNS) filtering services must be used to help block access to known malicious domains and IP addresses.

### 6.7.8 Implement DMARC and Enable Receiver-Side Verification

*CIS 7.8: To lower the chance of spoofed or modified emails from valid domains, implement Domain-based Message Authentication, Reporting and Conformance (DMARC) policy and verification, starting by implementing the Sender Policy Framework (SPF) and the DomainKeys Identified Mail (DKIM) standards.*

To lower the chance of spoofed or modified emails from valid domains, state agencies must implement Domain-based Message Authentication, Reporting and Conformance (DMARC) policy and verification, starting by implementing the Sender Policy Framework (SPF) and the DomainKeys Identified Mail (DKIM) standards.

### 6.7.9 Block Unnecessary File Types

*CIS 7.9: Block all email attachments entering the agency's email gateway if the file types are unnecessary for the agency's business.*

State agencies must *block all email attachments entering the agency's email gateway if the file types are unnecessary for the agency's business.*

### 6.7.10 Sandbox All Email Attachments

*CIS 7.10: Use sandboxing to analyze and block inbound email attachments with malicious behavior.*

State agencies must use sandboxing to analyze and block inbound email attachments with malicious behavior.

## 6.4 Controlled Use of Administrative Privileges

### 6.4.1 Reserved [IG2]

*This section is reserved for CIS Controls Implementation Group 2 (IG2), 4.1.*

### 6.4.2 Change Default Passwords

*CIS 4.2: Before deploying any new asset, change all default passwords to have values consistent with administrative level accounts.*

Before deploying any new asset, all default passwords must be changed to meet password requirements for administrative level accounts.

### 6.4.3 Ensure the Use of Dedicated Administrative Accounts

*CIS 4.3: Ensure that all users with administrative account access use a dedicated or secondary account for elevated activities. This account should only be used for administrative activities and not internet browsing, email, or similar activities.*

All users with administrative account access must use a dedicated account for elevated activities. This account must only be used for administrative activities and not internet browsing, email, or similar activities.

### 6.4.4 Reserved [IG2]

*This section is reserved for CIS Controls Implementation Group 2 (IG2), 4.4.*

### 6.4.5 Reserved [IG2]

*This section is reserved for CIS Controls Implementation Group 2 (IG2), 4.5.*

### 6.4.6 Reserved [IG3]

*This section is reserved for CIS Controls Implementation Group 3 (IG3), 4.6.*

### 6.4.7 Reserved [IG2]

*This section is reserved for CIS Controls Implementation Group 2 (IG2), 4.7.*

### 6.4.8 Reserved [IG2]

*This section is reserved for CIS Controls Implementation Group 2 (IG2), 4.8.*

### 6.4.9 Reserved [IG2]

*This section is reserved for CIS Controls Implementation Group 2 (IG2), 4.9.*

## 6.5 Secure Software Configuration for Mobile Devices, Workstations, and Servers [2]

### 6.5.1 Establish Secure Software Configurations [See Related Section 4.5]

*CIS 5.1: Maintain documented security configuration standards for all authorized operating systems and software.*

State agencies must establish, implement, and maintain documented security configuration standards for all authorized operating systems and software.

### 6.5.2 Reserved [IG2]

*This section is reserved for CIS Controls Implementation Group 2 (IG2), 5.2.*

### 6.5.3 Reserved [IG2]

*This section is reserved for CIS Controls Implementation Group 2 (IG2), 5.3.*

### 6.5.4 Reserved [IG2]

*This section is reserved for CIS Controls Implementation Group 2 (IG2), 5.4.*

### 6.5.5 Reserved [IG2]

*This section is reserved for CIS Controls Implementation Group 2 (IG2), 5.5.*

## 6.6 Maintenance, Monitoring, and Analysis of Audit Logs

### 6.6.1 Reserved [IG2]

*This section is reserved for CIS Controls Implementation Group 2 (IG2), 6.1.*

### 6.6.2 Activate Audit Logging [See Related Section 5.3]

*CIS 6.2: Ensure that local logging has been enabled on all systems and networking devices.*

State agencies must ensure that local audit logging has been enabled on all systems and networking devices.

---

[2] CIS Guidance: CIS confirmed that there are no hardware/equipment-specific configuration sub-controls implied in CIS Control 5 Secure Configuration for Hardware and Software on Mobile Devices, Laptops, Workstations and Servers.

While CIS enumerates Laptops as distinct from Mobile Devices in its guidance for this control, the State Information Security Program categorizes laptops as being one of many types of mobile devices. “Laptops” is redundant within the context of the State Information Security Program Policy and Standards. This control may be more concisely titled as Secure Software Configuration for Mobile Devices, Workstations, and Servers.

### 6.6.3 Reserved [IG2]

*This section is reserved for CIS Controls Implementation Group 2 (IG2), 6.3.*

### 6.6.4 Reserved [IG2]

*This section is reserved for CIS Controls Implementation Group 2 (IG2), 6.4.*

### 6.6.5 Reserved [IG2]

*This section is reserved for CIS Controls Implementation Group 2 (IG2), 6.5.*

### 6.6.6 Reserved [IG2]

*This section is reserved for CIS Controls Implementation Group 2 (IG2), 6.6.*

### 6.6.7 Reserved [IG2]

*This section is reserved for CIS Controls Implementation Group 2 (IG2), 6.7.*

### 6.6.8 Reserved [IG3]

*This section is reserved for CIS Controls Implementation Group 3 (IG3), 6.8.*

## 6.7 Email and Web Browser Protections

### 6.7.1 Use of Fully Supported Browsers and Email Clients [See Related Section 5.10]

*CIS 7.1: Ensure that only fully supported web browsers and email clients are allowed to execute in the organization, ideally only using the latest version of the browsers and email clients provided by the vendor.*

State agencies must ensure that only fully supported web browsers and email clients are allowed to execute in the organization, ideally only using the latest version of the browsers and email clients provided by the vendor.

### 6.7.2 Reserved [IG2]

*This section is reserved for CIS Controls Implementation Group 2 (IG2), 7.2.*

### 6.7.3 Reserved [IG2]

*This section is reserved for CIS Controls Implementation Group 2 (IG2), 7.3.*

### 6.7.4 Reserved [IG2]

*This section is reserved for CIS Controls Implementation Group 2 (IG2), 7.4.*

### 6.7.5 Reserved [IG2]

*This section is reserved for CIS Controls Implementation Group 2 (IG2), 7.5.*

### 6.7.6 Reserved [IG2]

*This section is reserved for CIS Controls Implementation Group 2 (IG2), 7.6.*

### 6.7.7 Use of DNS Filtering Services

*CIS 7.7: Use Domain Name System (DNS) filtering services to help block access to known malicious domains.*

Domain Name System (DNS) filtering services must be used to help block access to known malicious domains and IP addresses.

### 6.7.8 Reserved [IG2]

*This section is reserved for CIS Controls Implementation Group 2 (IG2), 7.8.*

### 6.7.9 Reserved [IG2]

*This section is reserved for CIS Controls Implementation Group 2 (IG2), 7.9.*

### 6.7.10 Reserved [IG3]

*This section is reserved for CIS Controls Implementation Group 3 (IG3), 7.10.*

## *6.8 Malware Defenses [See Related Section 5.3]*

### 6.8.1 Reserved [IG2]

*This section is reserved for CIS Controls Implementation Group 2 (IG2), 8.1.*

### 6.8.2 Ensure Anti-Malware Software and Signatures Are Updated

*CIS 8.2: Ensure that the organization's anti-malware software updates its scanning engine and signature database on a regular basis.*

State agencies must ensure anti-malware software components and signatures are updated on a regular basis.

### 6.8.3 Reserved [IG2]

*This section is reserved for CIS Controls Implementation Group 2 (IG2), 8.3.*

### 6.8.4 Configure Anti-Malware Scanning of Removable Media

*CIS 8.4: Configure devices so that they automatically conduct an anti-malware scan of removable media when inserted or connected.*

Devices must be configured to automatically conduct an anti-malware scan of removable media when inserted or connected.

### 6.8.5 Configure Devices to Not Auto-Run Content

*CIS 8.5: Configure devices to not auto-run content from removable media.*

Devices must be configured to not auto-run content from removable media.

### 6.8.6 Reserved [IG2]

*This section is reserved for CIS Controls Implementation Group 2 (IG2), 8.6.*

### 6.8.7 Reserved [IG2]

*This section is reserved for CIS Controls Implementation Group 2 (IG2), 8.7.*

### 6.8.8 Reserved [IG2]

*This section is reserved for CIS Controls Implementation Group 2 (IG2), 8.8.*

## *6.9 Limitation and Control of Systems Ports, Protocols, and Services [3]*

### 6.9.1 Reserved [IG2]

*This section is reserved for CIS Controls Implementation Group 2 (IG2), 9.1.*

### 6.9.2 Reserved [IG2]

*This section is reserved for CIS Controls Implementation Group 2 (IG2), 9.2.*

### 6.9.3 Reserved [IG2]

*This section is reserved for CIS Controls Implementation Group 2 (IG2), 9.3.*

---

[3] CIS Guidance: The CIS Controls v7.1 guide indicates CIS Control 9 broadly applies to “networked computing devices”, including but not limited to workstations and servers, sometimes referred to as “network endpoints”. Additional security requirements for network equipment, such as firewalls, routers, and switches, are addressed in CIS Controls 11 and 12. For clarity, “Systems” has replaced “Network” in the title of this control, consistent with terminology used in in these sub-controls.

### 6.9.4 Apply Host-Based Firewalls or Port-Filtering

*CIS 9.4: Apply host-based firewalls or port-filtering tools on end systems, with a default-deny rule that drops all traffic except those services and ports that are explicitly allowed.*

Host-based firewalls or port-filtering tools must be implemented and in use on all systems, including servers, workstations, and laptops, with a default-deny rule that drops all traffic except those services and ports that are explicitly allowed.

### 6.9.5 Reserved [IG3]

*This section is reserved for CIS Controls Implementation Group 3 (IG3), 9.5.*

## *6.10 Data Recovery Capabilities [See Related Section 4.4]*

### 6.10.1 Ensure Regular Automated Backups

*CIS 10.1: Ensure that all system data is automatically backed up on a regular basis.*

State agencies must ensure that all system data is automatically backed up on a regular basis.

### 6.10.2 Perform Complete System Backups

*CIS 10.2: Ensure that all of the organization's key systems are backed up as a complete system, through processes such as imaging, to enable the quick recovery of an entire system.*

State agencies must ensure that all agency key systems are backed up as a complete system, through processes such as imaging, to enable the quick recovery of an entire system.

### 6.10.3 Reserved [IG2]

*This section is reserved for CIS Controls Implementation Group 2 (IG2), 10.3.*

### 6.10.4 Protect Backups

*CIS 10.4: Ensure that backups are properly protected via physical security or encryption when they are stored, as well as when they are moved across the network. This includes remote backups and cloud services.*

State agencies must ensure that backups are properly protected via physical security or encryption when they are stored, as well as when they are moved across the network. This includes remote backups and cloud services.

### 6.10.5 Ensure All Backups Have At Least One Offline Backup Destination

*CIS 10.5: Ensure that all backups have at least one offline (i.e., not accessible via a network connection) backup destination.*

State agencies must ensure that all backups have at least one offline (i.e., not accessible via a network connection) backup destination.

## 6.11 Secure Configuration for Network Devices

### 6.11.1 Reserved [IG2]

*This section is reserved for CIS Controls Implementation Group 2 (IG2), 11.1.*

### 6.11.2 Reserved [IG2]

*This section is reserved for CIS Controls Implementation Group 2 (IG2), 11.2.*

### 6.11.3 Reserved [IG2]

*This section is reserved for CIS Controls Implementation Group 2 (IG2), 11.3.*

### 6.11.4 Install Latest Stable Version of Security-Related Updates on All Network Devices

*CIS 11.4: Install the latest stable version of any security-related updates on all network devices.*

State agencies must install the latest stable version of any security-related updates on all network devices.

### 6.11.5 Reserved [IG2]

*This section is reserved for CIS Controls Implementation Group 2 (IG2), 11.5.*

### 6.11.6 Reserved [IG2]

*This section is reserved for CIS Controls Implementation Group 2 (IG2), 11.6.*

### 6.11.7 Reserved [IG2]

*This section is reserved for CIS Controls Implementation Group 2 (IG2), 11.7.*

## 6.12 Boundary Defense

6.12.1 Maintain an Inventory of Network Boundaries

*CIS 12.1: Maintain an up-to-date inventory of all of the organization's network boundaries.*

State agencies must maintain an up-to-date inventory of all agency network boundaries.

6.12.2 Scan for Unauthorized Connections Across Trusted Network Boundaries

*Perform regular scans from outside each trusted network boundary to detect any unauthorized connections which are accessible across the boundary.*

State agencies must perform regular scans from outside each trusted network boundary to detect any unauthorized connections which are accessible across the boundary.

### 6.12.3 Deny Communications With Known Malicious IP Addresses

*CIS 12.3: Deny communications with known malicious or unused Internet IP addresses and limit access only to trusted and necessary IP address ranges at each of the organization's network boundaries.*

State networks must deny communications with known malicious or unused Internet IP addresses and must limit access only to trusted and necessary IP address ranges at each of the agency network boundaries.

### 6.12.4 Deny Communication Over Unauthorized Ports

*CIS 12.4: Deny communication over unauthorized TCP or UDP ports or application traffic to ensure that only authorized protocols are allowed to cross the network boundary in or out of the network at each of the organization's network boundaries.*

State networks must deny communication over unauthorized TCP or UDP ports or application traffic to ensure that only authorized protocols are allowed to cross the network boundary in or out of the network at each of the agency network boundaries.

### 6.12.5 Configure Monitoring Systems to Record Network Packets

*CIS 12.5: Configure monitoring systems to record network packets passing through the boundary at each of the organization's network boundaries.*

Monitoring systems must be configured to record network packets passing through the boundary at each of the agency network boundaries.

### 6.12.6 Deploy Network-Based IDS Sensors

*CIS 12.6: Deploy network-based Intrusion Detection Systems (IDS) sensors to look for unusual attack mechanisms and detect compromise of these systems at each of the organization's network boundaries.*

Network-based Intrusion Detection Systems (IDS) sensors must be deployed to look for unusual attack mechanisms and detect compromise of these systems at each of the agency network boundaries.

### 6.12.7 Deploy Network-Based Intrusion Prevention Systems

*Deploy network-based Intrusion Prevention Systems (IPS) to block malicious network traffic at each of the organization's network boundaries.*

Network-based Intrusion Prevention Systems (IPS) must be deployed to block malicious network traffic at each of the state network boundaries.

### 6.12.8 Deploy NetFlow Collection on Networking Boundary Devices

*Enable the collection of NetFlow and logging data on all network boundary devices.*

Collection of NetFlow and logging data must be enabled on all network boundary devices.

### 6.12.9 Reserved [IG3]

*This section is reserved for CIS Controls Implementation Group 3 (IG3), 12.9.*

6.12.10 Reserved [IG3]

*This section is reserved for CIS Controls Implementation Group 3 (IG3), 12.10.*

6.12.11 Require All Remote Logins to Use Multi-Factor Authentication [See Related 5.4.2]

*CIS 12.11: Require all remote login access to the organization's network to encrypt data in transit and use multi-factor authentication.*

Agency networks must require all remote login access to SilverNet to encrypt data in transit and to use multi-factor authentication.

6.12.12 Reserved [IG3]

*This section is reserved for CIS Controls Implementation Group 3 (IG3), 12.12.*

## *6.13 Data Protection [See Related Section 3.6]*

### 6.13.1 Maintain an Inventory of Sensitive Information

*CIS 13.1: Maintain an inventory of all sensitive information stored, processed, or transmitted by the organization's technology systems, including those located on-site or at a remote service provider.*

State agencies must maintain an accurate and up-to-date inventory of sensitive information assets, including agency-defined essential data, system documentation, operational and support procedures, information security plans, and contingency and continuity of operations plans.

### 6.13.2 Remove Sensitive Data or Systems Not Regularly Accessed by Agency

*CIS 13.2: Remove sensitive data or systems not regularly accessed by the organization from the network. These systems shall only be used as stand-alone systems (disconnected from the network) by the business unit needing to occasionally use the system or completely virtualized and powered off until needed.*

State agencies shall remove sensitive data or systems not regularly accessed from the network. These systems shall only be used as stand-alone systems (disconnected from the network) by the business unit needing to occasionally use the system or completely virtualized and powered off until needed.

### 6.13.3 Reserved [IG3]

*This section is reserved for CIS Controls Implementation Group 3 (IG3), 13.3.*

### 6.13.4 Reserved [IG2]

*This section is reserved for CIS Controls Implementation Group 2 (IG2), 13.4.*

### 6.13.5 Reserved [IG3]

*This section is reserved for CIS Controls Implementation Group 3 (IG3), 13.5.*

### 6.13.6 Encrypt Mobile Device Data [Moved From Section 4.2.2]

*CIS 13.6: Utilize approved cryptographic mechanisms to protect enterprise data stored on all mobile devices.*

State agencies must use approved cryptographic mechanisms to ensure that the storage and transmission of an agency's data on mobile devices is protected with encryption standards that are commensurate with the sensitivity level of the data.

### 6.13.7 Reserved [IG2]

*This section is reserved for CIS Controls Implementation Group 2 (IG2), 13.7.*

### 6.13.8 Reserved [IG3]

*This section is reserved for CIS Controls Implementation Group 3 (IG3), 13.8.*

### 6.13.9 Reserved [IG3]

*This section is reserved for CIS Controls Implementation Group 3 (IG3), 13.9.*

## *6.14 Controlled Access Based on the Need to Know*

### 6.14.1 Reserved [IG2]

*This section is reserved for CIS Controls Implementation Group 2 (IG2), 14.1.*

### 6.14.2 Reserved [IG2]

*This section is reserved for CIS Controls Implementation Group 2 (IG2), 14.2.*

### 6.14.3 Reserved [IG2]

*This section is reserved for CIS Controls Implementation Group 2 (IG2), 14.3.*

### 6.14.4 Reserved [IG2]

*This section is reserved for CIS Controls Implementation Group 2 (IG2), 14.4.*

### 6.14.5 Reserved [IG3]

*This section is reserved for CIS Controls Implementation Group 3 (IG3), 14.5.*

### 6.14.6 Protect Information Through Access Control Lists

*CIS 14.6: Protect all information stored on systems with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities.*[4]

State agencies must protect all information stored on systems with file system, network share, roles, attributes, claims, application, or database specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities.

### 6.14.7 Reserved [IG3]

*This section is reserved for CIS Controls Implementation Group 3 (IG3), 14.7.*

### 6.14.8 Reserved [IG3]

*This section is reserved for CIS Controls Implementation Group 3 (IG3), 14.8.*

### 6.14.9 Reserved [IG3]

*This section is reserved for CIS Controls Implementation Group 3 (IG3), 14.9.*

## *6.15 Wireless Access Control [See Related Section 5.8.3]*

### 6.15.1 Reserved [IG2]

*This section is reserved for CIS Controls Implementation Group 2 (IG2), 15.1.*

### 6.15.2 Reserved [IG2]

*This section is reserved for CIS Controls Implementation Group 2 (IG2), 15.2.*

### 6.15.3 Reserved [IG2]

*This section is reserved for CIS Controls Implementation Group 2 (IG2), 15.3.*

---

[4] CIS Guidance: Through a technical discussion on access control models, CIS clarified that the use of "claims" in this context is a reference to a Microsoft-proprietary access control model, CBAC (Claims-Based Access Control), introduced for Windows Server 2012.

NIST has two publications with standards on access control models, including Role-Based Access Control (RBAC) and Attribute-Based Access Control (ABAC): *NIST SP 800-205 Attribute Considerations for Access Control Systems* and *NIST SP 800-162 Guide to Attribute Based Access Control (ABAC) Definition and Considerations*. In keeping with NIST standards, vendor-agnostic terms would be "roles and "attributes", as possible elements to determine access authorization.

### 6.15.4 Reserved [IG3]

*This section is reserved for CIS Controls Implementation Group 3 (IG3), 15.4.*

### 6.15.5 Reserved [IG3]

*This section is reserved for CIS Controls Implementation Group 3 (IG3), 15.5.*

### 6.15.6 Reserved [IG2]

*This section is reserved for CIS Controls Implementation Group 2 (IG2), 15.6.*

### 6.15.7 Leverage the Advanced Encryption Standard (AES) to Encrypt Wireless Data

*CIS 15.7: Leverage the Advanced Encryption Standard (AES) to encrypt wireless data in transit.*

The AES encryption standard must be used for encryption of all wireless transmissions.

### 6.15.8 Reserved [IG3]

*This section is reserved for CIS Controls Implementation Group 3 (IG3), 15.8.*

### 6.15.9 Reserved [IG2]

*This section is reserved for CIS Controls Implementation Group 2 (IG2), 15.9.*

### 6.15.10 Create Separate Wireless Network for Personal and Untrusted Devices

*CIS 15.10: Create a separate wireless network for personal or untrusted devices. Enterprise access from this network should be treated as untrusted and filtered and audited accordingly.*

State agencies must create a separate wireless network for personal or untrusted devices. Access from this network must be treated as untrusted and must be filtered and audited accordingly.

## 6.16 Account Monitoring and Control

### 6.16.1 Reserved [IG2]

*This section is reserved for CIS Controls Implementation Group 2 (IG2), 16.1.*

### 6.16.2 Reserved [IG2]

*This section is reserved for CIS Controls Implementation Group 2 (IG2), 16.2.*

### 6.16.3 Reserved [IG2]

*This section is reserved for CIS Controls Implementation Group 2 (IG2), 16.3.*

### 6.16.4 Reserved [IG2]

*This section is reserved for CIS Controls Implementation Group 2 (IG2), 16.4.*

### 6.16.5 Reserved [IG2]

*This section is reserved for CIS Controls Implementation Group 2 (IG2), 16.5.*

### 6.16.6 Reserved [IG2]

*This section is reserved for CIS Controls Implementation Group 2 (IG2), 16.6.*

### 6.16.7 Reserved [IG2]

*This section is reserved for CIS Controls Implementation Group 2 (IG2), 16.7.*

### 6.16.8 Disable Any Unassociated Accounts [See Related Section 5.2.1]

*CIS 16.8: Disable any account that cannot be associated with a business process or business owner.*

A. Accounts must be reviewed quarterly to ensure that transferred or resigned users have been deleted.
B. Any account that cannot be associated with an agency-authorized user or state information system must be disabled.

### 6.16.9 Disable Dormant Accounts [See Related Section 5.2.1]

*CIS 16.9: Automatically disable dormant accounts after a set period of inactivity.*

Dormant accounts must be automatically disabled after a set period of inactivity.

### 6.16.10 Reserved [IG2]

*This section is reserved for CIS Controls Implementation Group 2 (IG2), 16.10.*

### 6.16.11 Lock Workstation Sessions After Inactivity [Moved From Section 5.2.3]

*CIS 16.11: Automatically lock workstation sessions after a standard period of inactivity.*

State information systems must have automatic session timeout and re-authentication to re-establish or unlock. The timeout setting will be determined by the agency ISO consistent with the sensitivity of the data and security of the work area.

### 6.16.12 Reserved [IG2]

*This section is reserved for CIS Controls Implementation Group 2 (IG2), 16.12.*

### 6.16.13 Reserved [IG3]

*This section is reserved for CIS Controls Implementation Group 3 (IG3), 16.13.*

## 6.17 Security Awareness and Training Program [Moved From Section 3.5]

### 6.17.1 Reserved [IG2]

*This section is reserved for CIS Controls Implementation Group 2 (IG2), 17.1.*

### 6.17.2 Reserved [IG2]

*This section is reserved for CIS Controls Implementation Group 2 (IG2), 17.2.*

### 6.17.3 Implement a Security Awareness Program

*CIS 17.3: Create a security awareness program for all workforce members to complete on a regular basis to ensure they understand and exhibit the necessary behaviors and skills to help ensure the security of the organization. The organization's security awareness program should be communicated in a continuous and engaging manner.*

A. On-going awareness training programs that addresses the security education needs of all state agency employees must be developed and provided.

B. Security awareness training must be developed by the State agency Information Security Officer to supplement the agency's new employee orientation program and must be reinforced at least annually with all agency employees.

### 6.17.4 Reserved [IG2]

*This section is reserved for CIS Controls Implementation Group 2 (IG2), 17.4.*

### 6.17.5 Train Workforce on Secure Authentication

*CIS 17.5: Train workforce members on the importance of enabling and utilizing secure authentication.*

The security awareness program must include training on the importance of enabling and using secure authentication.

### 6.17.6 Train Workforce on Identifying Social Engineering Attacks

*CIS 17.6: Train the workforce on how to identify different forms of social engineering attacks, such as phishing, phone scams, and impersonation calls.*

The security awareness program must include training on how to identify different forms of social engineering attacks, such as phishing, phone scams, and impersonation calls.

### 6.17.7 Train Workforce on Sensitive Data Handling

*CIS 17.7: Train workforce members on how to identify and properly store, transfer, archive, and destroy sensitive information.*

The security awareness program must include training on how to identify and properly store, transfer, archive, and destroy sensitive information.

### 6.17.8 Train Workforce on Causes of Unintentional Data Exposure

*CIS 17.8: Train workforce members to be aware of causes for unintentional data exposures, such as losing their mobile devices or emailing the wrong person due to autocomplete in email.*

The security awareness program must include training on the causes for unintentional data exposures, such as losing their mobile devices or emailing the wrong person due to autocomplete in email.

### 6.17.9 Train Workforce Members on Identifying and Reporting Incidents

*CIS 17.9: Train workforce members to be able to identify the most common indicators of an incident and be able to report such an incident.*

The security awareness program must include training on how to identify the most common indicators of an incident and be able to report such an incident.

## *6.18 Reserved*

### 6.18.1 Reserved [IG2]

*This section is reserved for CIS Controls Implementation Group 2 (IG2), 18.1.*

### 6.18.2 Reserved [IG2]

*This section is reserved for CIS Controls Implementation Group 2 (IG2), 18.2.*

### 6.18.3 Reserved [IG2]

*This section is reserved for CIS Controls Implementation Group 2 (IG2), 18.3.*

### 6.18.4 Reserved [IG3]

*This section is reserved for CIS Controls Implementation Group 3 (IG3), 18.4.*

### 6.18.5 Reserved [IG2]

*This section is reserved for CIS Controls Implementation Group 2 (IG2), 18.5.*

### 6.18.6 Reserved [IG2]

*This section is reserved for CIS Controls Implementation Group 2 (IG2), 18.6.*

### 6.18.7 Reserved [IG2]

*This section is reserved for CIS Controls Implementation Group 2 (IG2), 18.7.*

### 6.18.8 Reserved [IG2]

*This section is reserved for CIS Controls Implementation Group 2 (IG2), 18.8.*

### 6.18.9 Reserved [IG2]

*This section is reserved for CIS Controls Implementation Group 2 (IG2), 18.9.*

### 6.18.10 Reserved [IG2]

*This section is reserved for CIS Controls Implementation Group 2 (IG2), 18.10.*

### 6.18.11 Reserved [IG2]

*This section is reserved for CIS Controls Implementation Group 2 (IG2), 18.11.*

## 6.19 Incident Response and Management [See Related Section 4.8] [5]

### 6.19.1 Document Incident Response Procedures

*CIS 19.1: Ensure that there are written incident response plans that define roles of personnel as well as phases of incident handling/management.* [6]

State agencies must have written incident response procedures or playbooks that define roles of personnel and the phases of incident handling/management.

### 6.19.2 Reserved [IG2]

*This section is reserved for CIS Controls Implementation Group 2 (IG2), 19.2.*

### 6.19.3 Designate Management Personnel to Support Incident Handling

*CIS 19.3: Designate management personnel, as well as backups, who will support the incident handling process by acting in key decision-making roles.* [7]

State agencies must maintain written documentation that designates management personnel, as well as backups, to act in key decision-making roles, in support of the incident response and management process.

### 6.19.4 Reserved [IG2]

*This section is reserved for CIS Controls Implementation Group 2 (IG2), 19.4.*

---

[5] CIS Guidance: CIS clarified the terminology used to assure a clear understanding of the meaning and intent for Control 19 and its IG1 sub-controls. The word "incident" is used here as a general term, as is commonly understood in Nevada state government. No explicit threshold or other defining criteria are implied by Control 19. CIS cited the definition found in NIST IR-7298 Information Security Glossary (https://csrc.nist.gov/glossary/term/incident) as an example:

> An occurrence that actually or potentially jeopardizes the confidentiality, integrity, or availability of an information system or the information the system processes, stores, or transmits or that constitutes a violation or imminent threat of violation of security policies, security procedures, or acceptable use policies.

[6] CIS Guidance: Sub-control 19.1 requires documented procedures or "playbooks" for common types of incidents which can be handled as part of normal operations, i.e., not an incident that requires an unusual or extreme level of effort, not a contingency or disaster recovery plan. There are different levels of documents and the types of incidents they are intended to address. Some are all encompassing, others are more operational. This sub-control refers to procedures or "playbooks" for handling common incidents that may be 8-10 pages or less, not a comprehensive 80-100 pg. or 200 pg. plan with exhaustive appendices.

[7] CIS Guidance: Sub-control 19.3 references "the incident handling process", which CIS defines as everything in Control 19, the complete Incident Response and Management process from beginning to end.

### 6.19.5 Maintain Contact Information for Reporting Security Incidents

*CIS 19.5: Assemble and maintain information on third-party contact information to be used to report a security incident, such as Law Enforcement, relevant government departments, vendors, and Information Sharing and Analysis Center (ISAC) partners.* [8]

State agencies must compile and maintain written documentation on authorized contact information to be used to report a security incident, such as relevant state and federal agencies and other external partners.

### 6.19.6 Publish Information Regarding Reporting Computer Anomalies and Incidents

*CIS 19.6: Publish information for all workforce members, regarding reporting computer anomalies and incidents, to the incident handling team. Such information should be included in routine employee awareness activities.*

The security awareness program must include training on how to report computer anomalies and incidents to the agency information security officer (ISO).

### 6.19.7 Reserved [IG2]

*This section is reserved for CIS Controls Implementation Group 2 (IG2), 19.7.*

### 6.19.8 Reserved [IG3]

*This section is reserved for CIS Controls Implementation Group 3 (IG3), 19.8.*

## *6.20 Reserved*

### 6.20.1 Reserved [IG2]

*This section is reserved for CIS Controls Implementation Group 2 (IG2), 20.1.*

### 6.20.2 Reserved [IG2]

*This section is reserved for CIS Controls Implementation Group 2 (IG2), 20.2.*

### 6.20.3 Reserved [IG3]

*This section is reserved for CIS Controls Implementation Group 3 (IG3), 20.3.*

---

[8] CIS Guidance: For sub-control 19.5, CIS clarified that this third-party information should be available to those individuals in designated roles, who are required to contact authorized third-parties in the event of a security incident.

This sub-control does not require all employees know all third-party contacts. It is acceptable to use a structured multi-level contacts approach, where employees know to contact their manager and the agency ISO, the agency ISO contacts OIS, required third-parties, and others, and the CISO and OIS may have enterprise and other third-party contact lists. The intent is for internal and third-party contact information to be defined and documented, such that if someone leaves their position, the contact information is not lost.

### 6.20.4 Reserved [IG2]

*This section is reserved for CIS Controls Implementation Group 2 (IG2), 20.4.*

### 6.20.5 Reserved [IG2]

*This section is reserved for CIS Controls Implementation Group 2 (IG2), 20.5.*

### 6.20.6 Reserved [IG2]

*This section is reserved for CIS Controls Implementation Group 2 (IG2), 20.6.*

### 6.20.7 Reserved [IG3]

*This section is reserved for CIS Controls Implementation Group 3 (IG3), 20.7.*

### 6.20.8 Reserved [IG2]

*This section is reserved for CIS Controls Implementation Group 2 (IG2), 20.8.*

*THIS PAGE INTENTIONALLY LEFT BLANK*

# APPENDIX A REQUESTS FOR SECURITY EXCEPTIONS

## A.1 Purpose

State information security policies and standards provide guidance for the security, and effective planning and use, of information technology (IT) resources. In the diverse State IT infrastructure, there may be occasions when compliance with a policy or standard cannot be accomplished; justifications for the noncompliance must be documented.

This policy establishes a mechanism to address requests for an exception to State Information Security policies or standards.

## A.2 Requirements

A.2.1 State agencies that are unable to comply with a State Information Security Policy or Standard must formally request an exception when there is a legitimate reason and reasonable alternatives to meet the policy or standard are not viable.

A.2.2 Exceptions will be evaluated and granted on a case by case basis and consider the nature of the request, systems impacted, security risks, and mitigation alternatives.

A.2.3 Request for exception must be submitted by the appropriate state agency manager, IT manager, Information Security Officer (ISO) or their designee.

A.2.4 Requests must be submitted utilizing the formalized exception request process defined in this document.

A.2.5 Request for an exception must be submitted to the Enterprise IT Services (EITS), Office of Information Security (OIS) for review. OIS will provide the requestor with written notification of the results of any exception request.

A.2.6 Exception requests that are denied by the OIS, Chief Information Security Officer (CISO) may be appealed to the State Chief Information Officer (CIO).

A.2.7 Approved exception requests must be kept on file for audit purposes.

A.2.8 All exceptions requests are temporary and must be reviewed annually.

## A.3 Procedure

A.3.1 A request for exception must use the Exception Request Form. The exception request must include the following:

A. the number and title of the policy or standard the exception request is covering;

B. the business and technical reasons for the exception – requests without specific business or technical reasons identified in the justification will be denied and returned for resubmission;

C. the source and destination addresses and specific ports that require exception if applicable;

D. the specific, temporary length of time the exception will be required;

E. the actions that will be taken to eliminate the exception;

F. the timeframe to eliminate the exception.

A.3.2 The Exception Request Form must be submitted to OIS and assigned to an OIS staff member for review. The request will be evaluated and presented with comments and a recommendation to the CISO for review.

A.3.3 The CISO must evaluate the request, consider the OIS staff recommendation, and grant or deny the request as appropriate. The assigned OIS staff will notify the requestor via email of the decision.

A.3.4 The assigned OIS staff will provide a copy of the final decision to the requestor via inter-departmental mail.

A.3.5 OIS will maintain a copy of all Exception Requests with decision on file.

A.3.6 Granted exception requests will be reviewed annually, in January, by OIS.

A.3.7 The decision of the CISO related to this procedure may be appealed to the CIO. The process to appeal the CISO decision is:

A. the original exception request forms with a memo to the CISO directly, stating the reason(s) why the exception should be approved from the state agency's perspective.

B. The CISO will re-evaluate the exception and submit it to the EITS senior security team (e.g., consisting of the CIO, CISO and Deputy CISO) for final decision.

C. The CISO will return the decision of the EITS senior security team to the requestor.