STATE OF NEVADA

INFORMATION SECURITY PROGRAM POLICY
100 REV C

Original Publication Date: **October 28, 2008 Interim Approval**
Revision Date: March 30, 2017 Approval

Established and Approved by the:
Nevada State Information Security Committee

Approved by the:
State Chief Information Officer

Sponsored by the:
Enterprise IT Services
Office of Information Security

THIS PAGE INTENTIONALLY LEFT BLANK

Preface

Enterprise IT Services (EITS) has the statutory responsibility for establishing regulations and providing guidance to state entities 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 entities in establishing entity specific security policies, standards, processes and plans. NRS 242.101.

To ensure the security concerns and needs of state entities 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 entities 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 evolves, 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; and/or*
- *Legislative Audit findings that stem from security audit.*

The International Standard ISO/IEC 27002:2005 (E) Code of Practice for Information Security Management and the National Institute of Standards and Technology, NIST Publication 800 series were used as guidance in the development of this policy. All reference documents provide the best industry practices and the requirements of the federal government, which require state compliance due to receiving federal funds for information systems or from accessing, processing, storing or transmitting federal data.[The requirements of NIST 800-53 and 800-100 will be the de facto state standard in situations where neither the state nor the agency has established a policy or standard on a specific security control]

This policy has been developed and approved by the State Information Security Committee 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, 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 entities 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 entities within the Executive Branch of Nevada State Government, with the exception of the Nevada System of Higher Education and the Nevada Criminal Justice Information Computer System, comply with the direction of this policy.*

In cases where a state entity 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 Change History

Version Number	Release Date	Summary of Changes	Chapter Number/ Paragraph Number	Changes Made By
A	10/28/2008	Initial Document Release		
B	07/12/2011	Revised background checks.	3.4.2	S. Ingersoll
C	03/30/2017	Review and Update – Rename 4.100000	Multiple	EITS/OIS

TITLE	SIGNATURE	DATE
State IT Security Committee Chair State Chief Information Security Officer		
State Chief Information Officer		

TABLE OF CONTENTS

CHAPTER 1 INTRODUCTION

1.0 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 entities within the Executive Branch of Nevada State Government must meet. Any state entity, 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 entity IT systems;
- communicate the responsibilities for the protection of state entity information;
- establish a secure processing base and a stable processing environment within state entities and throughout the state;
- reduce to the extent possible the opportunity for errors to be entered into an IT system supporting a state entity business processes;
- preserve management's options in the event of state data, information or technology being misused, lost or unauthorized access; and
- promote and increase the awareness of information security in all state entities and with all state employees.

1.1 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 entities within the Executive Branch of Nevada State Government, excluding the Nevada System of Higher Education and the Nevada Criminal Justice Information Computer System, that operate, manage or use IT capabilities in support of the business needs of the entity. This policy is applicable to state employees, contractors and all other authorized users, including outsourced third parties, which have access to or manage state information. Where conflicts exist between this policy, a state entity policy or a federal policy, 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 entity. It addresses all information, regardless of the form or format, which is created or used in support of business activities of state entities.

1.2 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.

Nevada Revised Statute (NRS) 242.101
The Clinger-Cohen Act of 1996
OMB Circular A-130, Management of Federal Information Resources and associated NIST Publications:
NIST 800-53 – Recommended Security Controls for Federal Information Systems and Organizations
NIST 800-100 – Information Security Handbook – Guide for Managers
Federal Information Security Management Act of 2002

THIS PAGE INTENTIONALLY LEFT BLANK

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 entity 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. Best practices from the International Standard, ISO/IEC 27002:2005 (E), Code of Practice for Information Security Management and the National Institute of Standards and Technology, NIST Special Publication 800-100, Information Security Handbook, A Guide for Managers have been referenced and used to develop the State Information Security Program 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, 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

This document contains policies that satisfy 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 entity 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 CISO will submit the change through 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 entities. It is the state entity'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) has the responsibility to:

A. establish, implement, administer and oversee the State Information Security Program;
B. develop guidance documents for state entities in developing various information security programs and plans;
C. provide subject matter expertise and assistance to state entities in establishing specific information security programs, development of information security policies, standards, procedures, and plans, information security awareness training, information security risk, vulnerability and physical security assessments;
D. establish a state Information Security Incident Management program to assist state entities 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 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 entities 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 have the responsibility to:

A. ensure the establishment, implementation, enhancement, monitoring and enforcement of the federal, state and entity 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

A. 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.

B. Resulting risks from a deviation to policy must be documented in the appropriate Information Security Plan.

C. 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):

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, 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 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 industry standards and guidelines provided by:

- International Standard ISO/IEC 27002:2005 (E) – Code of Practice for Information Security Management
- National Institute of Standards and Technology (NIST) – 800 Series
- OMB Circular 130 – Management of Federal Information Resources

THIS PAGE INTENTIONALLY LEFT BLANK

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:

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 ISO's 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 the:

1) establishment and implementation of agency specific 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 specific 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 specific 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, implemented and to facilitate compliance with the state and agency specific 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 have 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, regardless of the form or format, which is created, acquired, stored 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 that 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 entity's management and ISO or to the EITS, Office of Information Security.

3.2.3 Confidentiality – Integrity – Availability

All state entity information must be protected from unauthorized access to help ensure the information's confidentiality and maintain its integrity. State entities 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 entity 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 Entity Security Program

A. State entities 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 entity.

B. State entities 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 entity'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 entity through clear direction, demonstrated commitment, and explicit assignment of information security responsibilities to the entity ISO.

B. Information security initiatives and activities should be coordinated with representatives from different areas within the entity 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 entity;

B. provide information security consulting to the state entity regarding security threats that could affect the entity'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 entity;

D. develop and implement security training and awareness programs that educate employees, contractors and vendors with regard to the entity'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 entity'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 Entity Information Security Officer

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

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

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

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

D. evaluate new security threats and countermeasures that could affect the state entity and make appropriate recommendations to management of the state entity 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 entity management and the EITS, Office of Information Security (OIS). OIS will provide support to all state entities 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 entity 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 entity's information;

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

J. represent the entity 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 entities must comply with existing state and federal laws, and regulations that impose significant responsibilities on employees for the security of information.

B. All state entities 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

A. STATE EMPLOYEES and IT CONTRACTORS:

1) 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.

2) Background checks must be processed through the Department of Public Safety and must consist of a State and a Federal Bureau of Investigation (FBI) 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 State Chief Information Security Officer (CISO).

3) Unfavorable results from a background check must not be an automatic cause to refuse employment or cause for termination. The agency head after consult with the State Chief Information Security Officer (CISO) 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 entity'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 entity's IT systems and information to include acceptable use of the Internet, e-mail, 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 entity 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

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

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

3.6 Asset Management

3.6.1 State entities must establish and maintain protection of their information technology assets.

3.6.2 An inventory of assets must be maintained by state entities. The asset inventory must include:

A. Physical assets: computer equipment, communications equipment, removable media and other equipment;

B. Software assets: application software, system software, development tools, and utilities;

C. Information: entity-defined essential data, system documentation, operational and support procedures; information security plans, contingency and continuity of operations plans.

3.6.3 Updated inventories must be included in the appropriate Information Security and Contingency 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 entity's information processing infrastructure and information.

3.7.1 Risk Assessments

A. A full risk assessment must be conducted at each state entity 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, information security plans;

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

3) **physical security assessments** of entity 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 entity Information Security Program which must consist of entity specific 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 applications or when a major change occurs to the operating environment.

3.7.2 Self-Assessments

State entities 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 Entity Information Security Program

State entities 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 entity must develop Information Security Plans to document the administrative security controls and the controls for each major application and general support systems.

3.8.1 Administrative Security Plan

A. Each state entity must develop and document the administrative security controls established to include but not limited to controls put in place for security management, personnel security, 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 entity and/or requires special attention to security due to the risk and magnitude of impact to the state entity should the application be subject to unauthorized access, manipulation or disclosure of information.

A. Each state entity must develop and document the security controls designed within each major application of the entity. 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

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

A. Each state entity must develop and document the security controls designed within each major support system of the entity. 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 entity, such as a Local Area Network (LAN), Wide Area Network (WAN) or email server.

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

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

CHAPTER 4: OPERATIONAL SECURITY POLICIES

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 entities 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 entity 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 entity servers must be protected by an appropriately sized uninterruptible power supply.

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

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

Appropriate controls must be implemented to ensure that the storage and transmission of an entity's sensitive data is protected with encryption standards that are commensurate with the sensitivity level of the data.

4.2.3 Personally Owned Equipment and Software

A. State entities must control the use of personally owned or non-state equipment and software to process, access, or store state data. Personally owned or non-state equipment and software includes, but is not limited to, personal computers and related equipment and software, Internet service providers, personal e-mail providers (e.g., Yahoo, Hotmail), personal library resources, and handheld or personal digital assistant (PDA) devices.

B. Personally owned equipment and software must not be used to process, access, or store sensitive information or be connected the state enterprise or state entity's systems or network without the written authorization of the appropriate entity management and/or Information Security Officer.

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. Entity 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

Entities 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

State entities must establish formal procedures for backup, recovery and storage of data and related software.

4.4.1 Controls

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

4.4.2 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 Configuration Management

4.5.1 Controls must be established, implemented and enforced on all state entity systems and networks that process, store, or communicate sensitive information.

4.5.2 Controls must include processes for the request, approval, implementation and documentation of all configuration changes.

4.6 Software Security

State entities must establish controls to ensure that only state approved and properly licensed software is installed on state systems.

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 compliers, 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 through out the planning, development, 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

4.8.1 State entities 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 entities 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 Individual must report any observed or suspected information security events or weaknesses to their manager or entity 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 entities 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.

CHAPTER 5: TECHNICAL SECURITY POLICIES

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 UserID.

5.1.2 Password

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

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 System User Accounts

User accounts must be reviewed quarterly to ensure the continued need for access to a system and that transferred or resigned users have been deleted.

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

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

5.2.4 Warning Banner

State IT systems and network must display an entity or State Attorney Generals' Office approved sign-on warning banner at all system access points.

5.3 Audit Trails

5.3.1 All IT systems and networks must generate audit logs that show addition, modification and/or deletion of information.

5.3.2 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

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 entities.

5.4.6 E-Mail Security

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

B. State e-mail services must be used for only official state business.

5.4.7 Personal E-Mail Accounts

Personal e-mail accounts must not be accessed using state systems and networks without the entity management approval.

5.4.8 Security Testing and Vulnerability Assessment

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 and at least annually for existing systems or networks.

5.5 Malicious Code Protection

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

5. 7 Patch Management

State entities must establish and implement patch management to all systems and networks in a manner that ensures maximum protection against security vulnerabilities and minimize impact on entity business operations.

Patch management must contain a systematic process of identifying, prioritizing, acquiring, implementing, testing and validating security patches necessary for each system or network.

A risk-based decision must be documented if security patches are not applied to a system or network.

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

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 must only be permitted internally between state entities.

5.8.5 Instant Messaging

Instant messaging is only permitted internal to state systems and networks.

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.

THIS PAGE INTENTIONALLY LEFT BLANK

APPENDIX A

REQUIREMENTS AND PROCEDURE FOR REQUESTING EXCEPTION

TO STATE INFORMATION SECURITY POLICIES AND STANDARDS

Requirements and Procedure for Exception Requests

1.0 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.

1.1 REQUIREMENTS

1.1.1 State entities 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.

1.1.2 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.

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

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

1.1.5 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.

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

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

1.1.8 All exceptions requests are temporary and must be reviewed annually.

1.2 PROCEDURE

1.2.1 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.

1.2.2 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.

1.2.3 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 e-mail of the decision.

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

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

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

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

A. Send 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 entity's perspective.

B. The CISO will re-evaluate the exception and submit it to the EITS senior security team (e.g., consist 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.