Information Security Policy

Final
Original Publication Date: January 11, 2010

Revision Date: Revision 30.0
February 02, 2010
# Table of Contents

1. PURPOSE .......................................................................................................................... 5
2. SCOPE ............................................................................................................................... 5
3. State of New Mexico Information Security POLICY .......................................................... 6
4. Organizational and Functional Responsibilities ................................................................ 6
   4.1. Department of Information Technology (DoIT) ............................................................ 6
   4.2. State Entity Chief Information Officer (CIO) ................................................................. 6
   4.3. State Entity (SE) ........................................................................................................... 7
   4.4. State Entity Information Security Officer ................................................................. 8
   4.5. State Entity Information Technology Leads ............................................................... 8
   4.6. State Entity Designated Security Staff ...................................................................... 9
   4.7. Information Owners .................................................................................................... 9
   4.8. State Entity Users ....................................................................................................... 10
5. Information Management Policy ...................................................................................... 10
   5.1. State Entity Security Plan .......................................................................................... 12
   5.2. Policy and Standards Relationship .......................................................................... 13
6. Asset Identification, Information Classification and Control Policy .................................. 13
   6.1. Inventory of Assets .................................................................................................... 13
   6.2. Assign Asset Responsibility ...................................................................................... 13
       6.2.1. Asset Classification ............................................................................................ 13
       6.2.2. Asset Handling .................................................................................................. 14
   6.3. Information Classification .......................................................................................... 14
       6.3.1. Public Information ............................................................................................. 14
       6.3.2. Sensitive and confidential INFORMATION ......................................................... 14
7. Physical and Environmental Security Policy ..................................................................... 14
8. Operational Management Policy ....................................................................................... 16
   8.1. Documentation of Operational Security .................................................................... 16
   8.2. Segregation of Security Duties .................................................................................. 16
   8.3. Network Management .............................................................................................. 16
   8.4. Privileged Accounts Management ............................................................................ 17
   8.5. Access Control Policy ............................................................................................... 17
8.6. Operating System Access Control .................................................................17
8.7. Application Access Control ..........................................................................18
8.8. Network Access Control .............................................................................18
8.9. User Authentication for External Connections (Remote Access Control) ..........18
8.10. External Network Connections ...................................................................20
8.11. Segregation of Networks ..........................................................................21
8.12. Wireless Networks, Bluetooth, and RFID ...................................................21
8.13. User Registration and Management ............................................................21
8.15. Use of personal computing devices ............................................................22
8.16. Vulnerability Scanning ..............................................................................23
8.17. Penetration and Intrusion Testing ...............................................................23
8.18. Protection against Malicious Code ...............................................................24
8.19. Message Integrity .......................................................................................24
8.20. Key Management .......................................................................................25
8.21. Criticality Assessment ................................................................................25
8.22. System Security Checking ..........................................................................25
8.23. Security of Electronic Mail ..........................................................................25
8.24. Internet and Electronic Mail Acceptable Use ...............................................26
8.25. Portable Devices and Removable Media ......................................................26
8.26. Telephones and Fax Equipment ..................................................................27
8.27. Modem Usage ............................................................................................27
8.28. Public Websites Content Approval Process ...............................................27
8.29. Electronic Signatures ................................................................................28
8.30. Business Continuity ..................................................................................28
8.31. Logon Banner ............................................................................................28
8.32. Monitoring System Access and Use ............................................................28
9.1. Separation of Development, Test, and Production Environments .................30
9.2. System Planning and Acceptance .................................................................30
9.3. Control of Internal Processing ...................................................................31
9.4. Protection of System Test Data........................................................................................31
9.5. Change Control Procedures..............................................................................................31
10. Risk Management ................................................................................................................32
    10.1. Conducting a Risk Assessment ....................................................................................32
    10.2. Implementation of Risk a Risk Mitigation Strategy ....................................................32
11. Cyber Security Citizens’ Notification Policy.................................................................33
12. Compliance Policy...............................................................................................................34
    12.1. Enforcement and Violation Handling ...........................................................................34
    12.2. Amendment of State of New Mexico Security Policy ..................................................35
Definitions and Acronyms ...........................................................................................................36
State of New Mexico
Information Security Policy

1. PURPOSE

The purpose of this policy is to define a set of minimum security requirements that all state entities (SE) shall meet. This policy shall serve as best practices for the State of New Mexico Information Technology Infrastructure. Any SE may, based on its individual business needs and specific legal requirements such as the Health Insurance Portability and Accountability Act (HIPAA) or Federal Tax Information (FTI), exceed the security requirements put forth in this document, but shall at a minimum achieve the security levels required by this policy.

The primary objectives of this Information Security Policy and security program are to:

1. Effectively manage the risk of security exposure or compromise within SE computing infrastructure,
2. Communicate the responsibilities for the protection of SE information,
3. Establish a secure processing base and a stable processing environment,
4. Reduce to the extent reasonably possible the opportunity for errors to be entered into an electronic system supporting SE business processes,
5. In the event of an information asset misuse, loss or unauthorized disclosure, management has the discretion to decide how the incident shall be handled, and
6. Promote and increase the awareness of information security in all SEs.

2. SCOPE

This policy is applicable to State Entities (SE), staff, contractors and other non-staff members, and outsourced third parties, who have access to, store, or manage SE information. This policy is not intended to unilaterally change the terms and conditions of employment. All SEs, when coming into compliance with this policy, shall consider all terms and conditions of employment as well as collective bargaining agreements.

Where conflicts exist between this policy, SE policy, or federal regulations, the more restrictive policy shall take precedence.

The Information Security Policy for state entities encompasses information on all systems both automated and manual for which the state has administrative responsibility, including systems managed or hosted by third parties on behalf of the SE.

The Information Security Policy addresses all information, regardless of the form or format, which is created or used in support of business activities of state entities. This policy shall be communicated to all staff and all others who have access to, manage, or have responsibility for SE information.
3. STATE OF NEW MEXICO INFORMATION SECURITY POLICY

The State of New Mexico Information Security Policy sets the direction, gives broad guidance, defines requirements for information security related processes and actions across state entities (SEs), and contains the minimum requirements and responsibilities required to establish and maintain a secure computing environment and achieve the state’s information security objectives. Compliance with this security policy is mandatory. Where conflicts exist between this policy and SE policy, or federal regulations the more restrictive policy shall take precedence.

4. ORGANIZATIONAL AND FUNCTIONAL RESPONSIBILITIES

4.1. DEPARTMENT OF INFORMATION TECHNOLOGY (DoIT)

The duties of the Department of Information Technology are:

1. To assume ultimate responsibility for the security program in the State of New Mexico in coordination with state agencies;
2. To develop and maintain a statewide Information Technology (IT) Security Program that includes recommended policies, security standards, guidelines, procedures, best security practices, IT disaster recovery planning guidelines, security awareness, training, and an incident response reporting capability;
3. To provide project oversight and compliance, and approve project deviations to established IT security requirements; and
4. To establish the necessary IT security policies to ensure a broad-based information security program that addresses the management, operational, and technical aspects of protecting state networks, information, and information systems.

4.2. STATE ENTITY CHIEF INFORMATION OFFICER (CIO)

The SE CIO has the ultimate responsibility for all aspects of information technology security and privacy within the SE. Specific responsibilities of the SE CIO are to:

1. Assume the ultimate responsibility for all aspects of the SE security program, including all responsibilities outlined in the SE and Information Technology Management sections below;
2. Establish a broad-based SE information security program that addresses all state security policies as well as addressing the management, operational, and technical aspects of protecting SE networks, information, and information systems;
3. Ensure periodic SE security assessments are performed;
4. Assume accountability for the creation and implementation SE security policies, SE security standards, controls, guidelines and procedures, as well as the SE security training program;
5. Ensure the confidentiality, integrity, availability, and accountability of all SE information during processing, storage and transmittal; and
6. Directly manage the SE Information Security Officer, SE Security Administrators, and designated SE security staff unless otherwise arranged by the SE and documented within the SE security plan.

4.3. STATE ENTITY (SE)

Each SE shall:

1. Establish an organizational framework to develop and oversee the implementation of information security within the SE;

2. Appoint SE Information Security Officer (ISO);

3. Assure the confidentiality, integrity, availability, and accountability of all SE information while it is being processed, stored, and/or transmitted electronically, and the security of the resources associated with the processing function;

4. Develop and implement an IT Disaster Recovery Plan for critical SE IT Systems in accordance with IT Disaster Recovery plan Guidelines, tested and reviewed for relevance at least annually;

5. Establish a process to determine information sensitivity to determine the appropriate levels of protection for SE information and infrastructure, based on security best practices, State directives, federal regulations, and all legal and regulatory requirements;

6. Ensure a configuration and change management process is used to maintain the security of the IT system; and

7. Ensure that the CIO of each SE shall develop an organizational structure to:
   
   a. Implement and maintain an information security program based on statewide IT security standards, guidelines, and procedures;
   
   b. Assign information security responsibilities to the CIO or IT manager while ensuring separation of duties and assigning appropriate systems permissions and responsibilities for SE system users;
   
   c. Implement a security awareness program;
   
   d. Monitor significant changes to information assets;
   
   e. Identify security vulnerabilities within SE computing infrastructure and recommend corrective action;
   
   f. Assume the lead role in resolving SE security and privacy incidents;
   
   g. Develop a process to measure compliance with this policy;
   
   h. Communicate requirements of this policy and the associated information security standards to third parties (including all procurement documents) and address them in third-party agreements; and
   
   i. Implement an IT security certification and accreditation process for the SE's computing infrastructure.
4.4. STATE ENTITY INFORMATION SECURITY OFFICER

Under general management and direction of the SE CIO, the SE Information Security Officer (ISO) is given responsibility for ensuring the implementation, enhancement, and monitoring of information security policies and standards for the SE. The SE Information Security Officer is responsible for recommending security direction for their SE through:

1. Recommendation, coordination, and implementation of information security policies, standards, processes, education, training, and awareness programs, to ensure appropriate safeguards are implemented and to facilitate compliance with those policies, standards and processes that meet the business needs of the SE for SE CIO approval;

2. Investigation of all alleged information security violations by following:
   a. State Procedures for referring the investigation to other investigatory entities, including law enforcement;
   b. Coordination of security program activities and reporting processes in support of this policy and other security initiatives;

3. Provide consultation with respect to ensuring proper implementation of security requirements for the various SE computing infrastructures to SE CIO and legal staff, or to those serving in that capacity;

4. Identify new security threats and evaluate countermeasures that could affect the SE, make appropriate recommendations to the SE’s CIO and disseminate threats and controls to SE to mitigate risks;

5. Investigate and report any incident and the discovery of all information pertaining to that incident to appropriate internal management, DoIT, and state of New Mexico security steering committee;

6. Ensure appropriate information security awareness and education to all SE employees and where appropriate third-party individuals; and

7. Agency budget permitting, the recommendation is for all SE ISO’s to complete a minimum of twenty two and one half (22.5) Continuing Professional Education (CPE) credits annually to maintain an adequate level of current knowledge and proficiency in information security.

4.5. STATE ENTITY INFORMATION TECHNOLOGY LEADS

Information technology leads shall:

1. Ensure SE-specific requirements, processes, policies and controls are identified and implemented relative to state security policy requirements;

2. Ensure proper controls of information are implemented for which the SE’s business have assigned ownership responsibility based on the SE’s classification designations;

3. Ensure the participation of the SE Information Security Officer and technical staff in identifying and selecting appropriate and cost-effective security controls and procedures and in protecting information assets; and
4. Ensure that appropriate security requirements for user access to electronic information are defined for files, databases, and that physical devices are properly assigned to their areas of responsibility.

4.6. STATE ENTITY DESIGNATED SECURITY STAFF

Under the direction of the SE CIO, SE security staff shall be responsible for the implementation of this and other information security policies and the compliance of SE employees to this policy. Under direction of the SE CIO, the security staff shall educate SE employees with regard to information security issues. Staff shall explain the issues, why the policies have been established, and what role(s) individuals have in safeguarding information including consequences of non-compliance.

The SE designated staff are responsible for recommending to the SE CIO and to the SE ISO appropriate physical, logical, and procedural controls and ensuring the implementation of appropriate physical, logical, and procedural controls to preserve the security properties of confidentiality, integrity, availability and privacy of SE information.

SE ISO and security administration staff shall be responsible for:

1. Administering security tools,
2. Reviewing security practices,
3. Identifying and analyzing security threats and solutions,
4. Responding to security violations, and
5. Overseeing all userIDs and passwords and the associated processes for reviewing, logging, implementing access rights, emergency privileges, exception handling, and reporting requirements.

4.7. INFORMATION OWNERS

Information owners shall be responsible for:

1. Determining, documenting, and recommending access and privileges to SE information or information systems for SE CIO approval. Such requests for access and privileges shall be made in writing and be based on the user job responsibilities;
2. Making requests for actions in writing to the SE ISO for approval by the SE CIO;
3. Requesting access privileges in accord with their job responsibilities;
4. Communicating in writing to the SE ISO the legal requirements for access and disclosure of their data;
5. Identifying all SE information assets under their control; and
6. As delegated by the SE ISO, assigning responsibility for the installation, implementation, and maintenance of appropriate security measures. Such security measures include, but are not limited to:
   a. Identifying assets, owners, inventory of, classifying, handling and labeling procedures assets,
b. Managing access to their resources, and
c. Assuming responsibility for implementing security measures.

4.8. STATE ENTITY USERS

All SE users and contractors shall be responsible for:

1. Protecting SE information and resources including, but not limited to, userID and passwords;
2. Immediately reporting a suspected security incident to the appropriate business units manager and the SE ISO;
3. Using state computing resources only for intended purposes as defined by state laws, state IT policy, SE policies and procedures, and all state and Federal laws and regulations; and
4. Limiting access to information assets to only those for which they have been expressly given authorization.

5. INFORMATION MANAGEMENT POLICY

Information management policy is used, in part, to ensure the identification (information sensitivity level) of private and sensitive information. Once information sensitivity level is identified, develop and implement policies, standards, guidelines, and procedures to protect the intentional or unintentional unauthorized access, exposure, modification, destruction, or loss of information through by:

1. Developing practices and methods used to create and maintain security policies to translate, clarify, and communicate the SE’s position on high-level security principles and prevent misuse or loss of SE’s information assets;
2. Developing, deploying, communicating, updating, and enforcing SE security policies that address business requirements, state and federal laws, and administrative policies that follow established information security guidelines;
3. Ensuring that all information, regardless of form or format, that is created, acquired, or used in support of SE’s business activities:
   a. Be used only for SE business;
   b. Be protected. Protection shall be based the importance to business activities, risks, and security best practices;
   c. Be protected from its creation, throughout its useful life, and to its authorized disposal; and
   d. Be maintained in a secure and reliable manner that promotes data integrity, confidentiality, and accuracy, and ready availability for authorized use.
4. Information is among SEs’ most valuable assets. Organizations rely on information to support their business activities. The quality and availability of that information is vital to the SE's ability to carry out their mission. Therefore, all management, staff, contractors, or any authorized user has the responsibility to:
a. Secure, preserve, and protect in a consistent and reliable manner both SE’s information and the technologies and systems that support it, and

b. Provide all physical and procedural safeguards and controls required to accomplish business goals.

5. Information security management enables information to be shared, while ensuring protection of that information and its associated computer assets, including the network over which the information travels.

6. Establish and maintain cost-effective risk management practices intended to preserve SE ability to meet state program objectives, and all agreements with state, federal, and non-state entities that cover at a minimum:

   a. Appropriate levels of confidentiality for the data based on data classification,
   b. Standards for transmission, encryption, and storage of the data, if applicable,
   c. Agreements to comply with all state policy and law regarding use of information resources and data,
   d. Signed non disclosure statements that are available on the DoIT web site,
   e. Agreements to apply security patches and upgrades, and keep malware and malicious code software up-to-date on all systems on which data may be used, and
   f. Agreements to notify the state data owners and citizens promptly if a security incident involving the data occurs within 30 days.

7. Establish appropriate SE policies and procedures to protect and secure IT infrastructure, including:

   a. A technology upgrade policy that includes, but is not limited to, operating system upgrades on servers, routers, firewalls, and other computing devices. The policy shall address planning and testing of upgrades as well as SE criteria for deciding which upgrades to apply.
   b. A security patch and security upgrade policy that includes, but is not limited to, servers, routers, desktop computers, mobile devices, and firewalls. The policy shall address application and testing of the patches and security upgrades as well as SE criteria for deciding which patches and security upgrades shall be applied and include a timeframe for rapid upgrade.
   c. A firewall configuration policy that requires the creation and documentation of a baseline configuration for each firewall, updates of the documentation for all authorized changes, and periodic verification of the configuration to ensure the configuration has not changed during software modifications or rebooting of equipment. The firewall configuration policy shall be verified during the periodic independent security assessment is conducted by the SE.
   d. A server configuration policy that clearly addresses all servers that have any interconnection to Internet, extranet, or intranet traffic. The policy shall require creation and documentation of a baseline configuration for each server, updates of the documentation for all authorized changes, and periodic checking of the configuration to ensure that it has not changed during software modifications or rebooting of the equipment.
e. An SE or SE user shall not be allowed to proxy a server or circumvent web filtering software.

f. A server hardening policy that shall be applied to all servers throughout the SE’s computing infrastructure. The policy shall include processes for making changes that are based on published National Institute of Standards and Technology (NIST) standards for security technical implementation guides and all newly published vulnerability information as it becomes available. The policy shall address and be consistent with the SE’s policy for making security upgrades and security patches.

g. A software management and software licensing policy that shall address acquisition of software from reliable and safe sources as determined by national software library maintained by NIST, and clearly states the SE’s policy prohibiting the use of pirated or unlicensed software as addressed in NMAC 1.12.10.

h. A policy prohibiting the use of peer-to-peer technology that includes, but is not limited to, the transfer of music, movies, software, and other intellectual property. If the peer-to-peer policy is violated access to the Internet shall be terminated without any notice by either the SE, DoIT, or both.

i. A policy ensuring access to SE computers, computer systems, and networks through the use of individually assigned unique computer identifiers, such as userIDs or through the use of other technologies like biometrics or token cards.

8. Require that original security controls for information integrity and confidentiality be applied if transferred to a mobile device, desktop computer, or from another computer system.

9. Establish a policy requiring encryption, or equally effective technical controls, for all personally-identifiable, sensitive, or confidential information stored on portable electronic removable media (including, but not limited to CDs) and on portable computing devices (including, but not limited to laptop and notebook computers). This policy does not apply to mainframe and server tapes.

10. Unless data is encrypted, SE’s shall establish a policy prohibiting the use of state-owned USB drives (e.g., flash or thumb drives), unless specifically approved in writing by the SE CIO. State-owned USB drives shall be assessed for malware following each use and before connecting to a state-owned computing device. The use of personal USB drives and personal removable media are prohibited in all case.

11. Define appropriate processes in the SE Disaster Recovery.

12. Create a plan to ensure the reasonable and timely recovery of all SE information, applications, systems and security, regardless of computing platform.

5.1. STATE ENTITY SECURITY PLAN

SE’s are responsible for the management and operation of their information processing facilities. Each SE shall develop a security plan using the DoIT Security Plan template to identify and document security best practices that ensure the integrity and security of the SE’s information assets. The SE security plan shall document:

1. How SE information is shared inside and outside the organization, and
2. How security measures and controls are applied commensurate with the risk, sensitivity, and confidentiality of the information. In most cases for shared data, the security confidentiality requirements shall determine the level of security required.

5.2. **POLICY AND STANDARDS RELATIONSHIP**

SEs shall develop standards and procedures that support the implementation of this policy for systems and technologies being used within their domains. These security standards shall be produced and implemented by the SE to ensure uniformity of information protection and security management across the different technologies deployed within the SE. The standards can be used as a basis for measurement of policy compliance.

6. **ASSET IDENTIFICATION, INFORMATION CLASSIFICATION AND CONTROL POLICY**

Information, like other assets, shall be properly managed throughout its lifespan from creation, through authorized use, and to proper disposal. As with other assets, not all information has the same use or value and can reside different mediums or forms. Therefore, information requires different levels of protection. Each SE shall classify documents, files, and databases.

6.1. **INVENTORY OF ASSETS**

Each SE shall create an inventory of assets that, at a minimum, shall contain:

1. An identification of all assets,
2. Criticality of asset,
3. Identification of all documentation associated with an asset,
4. Archived information assets,
5. Application software, system software, and development tools,
6. Hardware and peripherals, and
7. Locations of assets.

6.2. **ASSIGN ASSET RESPONSIBILITY**

All information shall have information owners assigned from within the SE’s business units, who shall be responsible for ensuring appropriate protection from unauthorized intentional unintentional use, access, disclosure, modification, loss, or deletion by controlling information.

6.2.1. **ASSET CLASSIFICATION**

Information, in all forms, shall be classified at the time it is generated and before implementation by defining:

1. Access restrictions,
2. Criticality requirements, and
3. Required level of protection.
6.2.2. ASSET HANDLING

The SE shall document how each asset is used by defining:

1. Define asset use (e.g., copying, storage, and transmission) according criticality level,
2. Asset destruction requirements,
3. Labeling
   a. Define label process to include classification level and asset identifying information.
   b. Define label requirements while information is in use, disseminated or communicated.
   c. Classification Re-evaluation, and
4. Classification reevaluation to ensure that, as the value of information rises or falls, the asset handling procedure documents and addresses re-classification.

6.3. INFORMATION CLASSIFICATION

Each classification shall have applied a set or range of controls designed to protect the level of information commensurate with the value of the information and risk of loss. The set or range of controls shall also apply to all application software used to collect, store, or report the information.

When information over which the SE has responsibility is stored or used by a third-party, this policy shall be written into every contract with the third-party. Third-parties shall be required to contractually abide by this policy without exception.

This policy also applies to the distribution, sharing, or storage of state information between a third- and a fourth-party. All information shared by the state with a third-party who then shares or distributes that information with a fourth-party, shall have the express written consent of the SE CIO in before the sharing or distribution occurs.

6.3.1. PUBLIC INFORMATION

The public information data classification is used for information that has no security restrictions and is intended for viewing or distribution to the public. Examples include, but are not limited to, application forms, news and press releases, fact sheets, and public reports.

6.3.2. SENSITIVE AND CONFIDENTIAL INFORMATION

SE data categorized as sensitive or confidential information is not for public release.

7. PHYSICAL AND ENVIRONMENTAL SECURITY POLICY

These security practices prevent unauthorized physical access, damage, or interruption of an SE's assets. Physical security practices for each SE shall be sufficient to protect the most sensitive information technology application housed in the SE. Physical access security controls shall be applied to protect all assets (including but not limited to personal computer systems, computer
terminals, mobile devices, and information) from access by SE staff, users, contractors, and the general public.

1. Physical Security and Physical Access Control
   a. The SE shall perform a threat and risk assessment to determine the extent of the perimeter and apply appropriate security controls necessary to mitigate the risk.
   b. A physical security perimeter shall be established. The purpose of the security perimeter is to prevent unauthorized access, theft, or destruction of information or of an information asset. Based on the threat and risk assessment, a physical security perimeter shall be established in SE environments where information or information assets are stored including SE data centers, wiring closets for network and telephonic connections, printers where sensitive or confidential information may be printed, and any other location where information may be in use or stored.

2. Equipment Security
   a. Physical protection of computer equipment is necessary to reduce the risk of unauthorized access to information and to protect against loss or damage.
   b. Computing infrastructure shall be physically protected from security threats and environmental hazards.
   c. Additional or special controls may also be necessary to protect supporting facilities such as electrical supply and cabling infrastructure this protection shall include, but is not limited to, data centers, wiring closets, server rooms, and facilities used for the storage of computers and computer peripherals.

3. Disposal or Re-use of Storage Media and Equipment
   a. Formal processes shall be established to thoroughly sanitize or destroy all media and computing equipment to minimize risk of inadvertent disclosure of sensitive information. These processes shall address all State Auditor requirements for computer equipment disposal.
   b. Storage devices such as hard disk drives and removable media (e.g., tape, diskette, CDs, DVDs, cell phones, digital copiers, or other devices that store information) or paper containing sensitive or confidential information shall be physically destroyed or follow industry standard sanitization procedures to prevent the unauthorized disclosure of sensitive or confidential SE information.

4. Clear Screen
   a. To prevent unauthorized access to information, controls shall be implemented and automated techniques employed to enforce authentication or re-authentication after a predetermined period of inactivity for desktops, laptops, PDA’s, and any other computer systems where authentication is required. These controls may include techniques such as password protected screen savers, automated logoff processes, or re-authentication after a set time out period.
5. The SE shall develop procedures to address the protection, detection, and minimization of loss or disruption of operational capabilities due to electrical power fluctuations or failure at SE datacenters.

8. OPERATIONAL MANAGEMENT POLICY

8.1. DOCUMENTATION OF OPERATIONAL SECURITY

1. All SE IT technical operations shall have documented operating instructions, management processes, and formal incident management procedures that define roles and responsibilities of individuals who operate or use SE IT technical operations and facilities.

2. Computing hardware, software, or system configurations provided by SE shall not be altered or added to or in any way unless specifically exempted by written policy or procedures, and written approval of the SE CIO.

3. Where a SE provides a server, application, or network services to another SE, operational and management responsibilities shall be coordinated by the CIOs of both SEs.

4. The SE shall develop procedures for conducting background investigations on IT employees as required by state law.

8.2. SEGREGATION OF SECURITY DUTIES

Segregation of duties shall be required to reduce the risk of accidental or deliberate system misuse. In small SEs in which separation of duties is difficult to achieve, DoIT approval and other compensatory controls shall be applied including implementation of additional controls including, but not limited to, activity monitoring, audit trails, and close management supervision. In all cases, the periodic security audits shall remain independent and shall be segregated from the security function.

8.3. NETWORK MANAGEMENT

All SEs shall implement a range of network controls to maintain security in its trusted, internal network, and to ensure the protection of connected services and networks. These controls help prevent unauthorized access and use of the SE private network. The following controls, at minimum, shall be implemented:

1. Operational responsibility for networks shall be separate from computer operations when possible,

2. Responsibilities and procedures for remote use shall be established,

3. When necessary, special controls shall be implemented to safeguard data integrity and confidentiality of data passing over public networks (Internet),

4. All VPN connections shall have split tunneling disabled. VPN connections are only permitted from SE managed workstations,
5. SE networks shall adopt private routing and minimize the exposure of public routable address to the Internet,

6. SEs shall define security zones and create logical entities and rules for permissible data and network traffic between different business units and SE groups, and,

7. SE’s shall perform network segmentation in order to control the flow of data between hosts on different segments of the network for enhanced security, performance, and connectivity.

8.4. PRIVILEGED ACCOUNTS MANAGEMENT

The issuance and use of privileged accounts shall be restricted and controlled. Inappropriate use of system account privileges is often found to be a major contributing factor to the failure of systems that have been breached. Processes shall be developed to ensure that uses of privileged accounts are monitored and any suspected misuse of these accounts is promptly investigated. Passwords of multi-user system privileged accounts shall be changed more often than normal user accounts.

8.5. ACCESS CONTROL POLICY

To preserve the properties of integrity, confidentiality, and availability, the SE’s information assets shall be protected by logical and physical access control mechanisms commensurate with the value, sensitivity, consequences of loss or compromise, legal requirements, and ease of recovery of these assets.

1. SE CIO is responsible for determining who shall have access to sensitive and protected information resources within the SE. Access privileges shall be granted in accordance with the user’s role in the SE and job responsibilities, and

2. Enforcement of access control policy shall be verified during an independent annual risk assessment.

8.6. OPERATING SYSTEM ACCESS CONTROL

1. Access to operating system code, services, and commands shall be restricted to individuals such as systems programmers, database administrators, network, and security administrators who require access to perform their daily job responsibilities.

   a. These individuals shall have a unique privileged account (userID) assigned to them.

   b. User IDs shall not give any indication of the user's supervisor, manager, administrator, or privilege level.

2. To allow other activities to be tracked to the responsible individuals, system programmers, database administrators, network administrators and security administrators shall also be given a second userID to use when they perform business transactions unrelated to operating system, database, network and security functions, such as accessing the SE email system.
3. In certain circumstances, where there is a clear business requirement or system limitation, the use of a shared userID/password for a group of users or a specific job can be used by written approval by SE ISO and SE CIO. Additional compensatory controls shall be implemented to ensure accountability is maintained.

4. Where technically feasible, default administrator accounts shall be renamed, removed, or disabled. The default passwords for these accounts shall be changed if the account is retained, even if the account is renamed or disabled.

8.7. APPLICATION ACCESS CONTROL

1. Access to SE business and systems applications shall be restricted to those individuals who have a business need to access those applications or systems in the performance of their job responsibilities.

2. Access to source code for applications and systems shall be restricted and these accesses shall be further restricted so that authorized SE staff and contractors can access only those applications and systems they directly support.

8.8. NETWORK ACCESS CONTROL

Access to a SE’s trusted internal network shall require all authorized users to authenticate themselves through use of an individually assigned userID or an authentication mechanism (e.g., password, token, smart card). Network controls shall be developed and implemented to ensure that an authorized user can access only those network resources and services necessary to perform their assigned job responsibilities.

8.9. USER AUTHENTICATION FOR EXTERNAL CONNECTIONS (REMOTE ACCESS CONTROL)

1. To maintain information security, SE requires that individual accountability be maintained at all times, including during remote access.

2. Connection to SE’s networks shall be done in a secure manner to preserve the integrity of the network, data transmitted over that network, and the availability of the network. Security mechanisms shall be in place to control access to SE systems and networks remotely from fixed or mobile locations.

3. Advance approval for any such connection shall be obtained from the SE management and the SE ISO. An assessment shall be performed and documented to determine the scope and method of access, the risks involved and the contractual process, and technical controls required for such connection to take place.

4. Because of the level of risk inherent with remote access, use of a stronger password or another comparable method is required prior to connecting to any SE network. All sessions are subject to periodic and random monitoring.

5. When accessing a SE network remotely, identification and authentication of the entity requesting access shall be performed in such a manner as to not disclose the password or other authentication information that could be intercepted and used by a third-party.
6. Use of a common access point is required. This means that all remote connections to a computer shall be made through managed central points-of-entry. Using this type of entry system to access a SE computer provides many benefits, including simplified and cost effective security, maintenance, and support.

7. For a vendor to access SE computers or software, individual accountability is also required. For that system (hardware or software) for which there is a built-in userID for periodic maintenance, the account shall be disabled until the userID is needed. The activity performed while this vendor userID is in use shall be logged. Since these accounts are not regularly used, the vendor userID shall be disabled, the password changed, or other controls implemented to prevent or monitor unauthorized use of these privileged accounts during periods of inactivity.

8. In the special case where servers, storage devices, or other computer equipment has the capability to automatically connect to a vendor to report problems or suspected problems, the SE ISO shall review any such connection and process to ensure that connectivity does not compromise the SE or other third-party connections.

9. Working from a remote location shall be authorized by SE management and appropriate arrangements made for this activity through written policy and procedure, to ensure the work environment at the remote location provides adequate security for SE data and computing resources. Appropriate protection mechanisms commensurate with risk and exposure shall be in place to protect against theft of SE equipment, unauthorized disclosure of SE information, misuse of SE equipment, unauthorized access to the SE internal network, or other facilities by anyone including family and friends. To ensure the proper security controls are in place and all SE security standards are followed, the following shall be considered:
   a. The physical security of the remote location, including using a laptop at any location other than an employee’s work station;
   b. The accessing mechanism given the sensitivity of SE’s internal system the sensitivity of and method of transmitting information; and
   c. Appropriate business continuity procedures including backing up critical information.

10. The following controls shall be considered and appropriately implemented. Controls shall be monitored and audited following implementation.
   a. A definition of the classification of the information and the systems and services that the remote user is authorized to access,
   b. Procedures and necessary tools allowing for secure remote access, such as authentication tokens or passwords, shall be documented including procedures for revocation of authorization, and the return of equipment,
   c. Hardware and software support and maintenance procedures including anti-virus software and maintenance of current signature files,
   d. Implementation of suitable network boundary controls to prevent unauthorized information exchange between SE networks connected to remote computers and externally connected networks, such as the Internet. Such measures include firewalls and intrusion detection techniques at the remote location, and
e. Physical security of the equipment used for remote access (e.g. such as cable locking device, or locking computer cabinet/secure storage area).

8.10. EXTERNAL NETWORK CONNECTIONS

1. Because the Internet is inherently insecure, access to the Internet is prohibited from any device that is connected (wired or wireless) to any part of a SE network unless specifically authorized in writing by SE CIO. This includes accounts with third-party Internet service providers.

2. Users shall not use the SE’s Internet accounts to establish connections to these third-party services including third-party email systems, unless specifically authorized in writing to do so by SE CIO, and the security of the connection is reviewed by the SE ISO and authorized in writing by the SE CIO.

3. Any connection from the SE network to any external network (either within or outside state government) shall be approved in writing by the SE CIO. Any non-state network connection shall also be approved by DoIT security staff.

4. Connections shall be allowed only with external networks that have been reviewed and found to have acceptable security controls and procedures, and appropriate security measures have been implemented by the SE to protect SE network resources. A risk analysis shall be performed to ensure that the connection to the external network shall not compromise the SE’s private network. Additional controls, such as the establishment of firewalls and a DMZ (demilitarized zone) maybe implemented between the third-party and the SE. These connections shall be periodically reviewed by the SE to ensure the:
   a. Business case for the connection is still valid and the connection is still required, and
   b. Security controls are in place (e.g., filters, rules, access control lists) are current and are functioning correctly.

5. This policy requires that connection to the SE network be done in a secure manner to preserve the integrity of the SE network, data transmitted over that network, and the availability of the network. The security requirements for each connection shall be assessed individually, and shall be driven by the business needs. Only authorized SE qualified staff or a qualified third-party shall be permitted to use sniffers or similar technology on the network to monitor operational data and security events.

6. The SE ISO or designee shall regularly review audit trails and system logs of external network connections for abuses and anomalies.

7. Any third-party network or workstation connection to a SE network shall:
   a. Have an internal SE sponsor develop a business case for the network connection,
   b. Sign a SE non-disclosure agreement. The non-disclosure agreement shall be signed by a duly appointed representative from the third-party organization who is legally authorized to sign such an agreement,
c. In addition to the agreement, the third-party’s equipment shall also conform to all state security policies and standards, the SE technical architecture, and be approved for connection in writing by the SE CIO, and

d. Any connection between SE firewalls over external networks that involves sensitive or confidential shall use encryption to ensure the confidentiality and integrity of the data passing over the external network.

8.11. SEGREGATION OF NETWORKS

When the SE network is connected to another network or becomes a segment on a larger network, controls shall be in place to prevent users from other connected networks access to sensitive areas of the SE’s private network. Routers or other technologies shall be implemented to control access to secured resources on the trusted SE network.

8.12. WIRELESS NETWORKS, BLUETOOTH, AND RFID

1. No wireless network or wireless access point shall be installed without a risk assessment performed and the written approval of the SE CIO prior to installation.

2. Suitable controls, such as Media Access Control (MAC) address restriction, authentication, and encryption shall be implemented to ensure that a wireless network or access point cannot be exploited to disrupt SE information services or to gain unauthorized access to SE information. When selecting wireless technologies, such as 802.11x or its predecessors, wireless network security features on the equipment shall be available and implemented from the beginning of the deployment.

3. Access to systems that hold sensitive information or the transmission of protected or sensitize information via a wireless network is not permitted unless appropriate and adequate measures have been implemented and approved by the SE CIO. Such measures shall include authentication, authorization, encryption, access controls, and logging.

8.13. USER REGISTRATION AND MANAGEMENT

1. A user management process shall be established and documented by the SE to outline and identify all functions of user management, to include the generation, distribution, modification, and deletion of user accounts for access to resources. The purpose of this process is to ensure that only authorized individuals have access to SE applications and information and that these users only have access to the resources required for authorized purposes.

2. The user management process shall include the following sub-processes as appropriate:

   a. Enrolling new users,
   b. Removing userIDs,
   c. Granting “privileged accounts” to a user,
   d. Removing “privileged accounts” from a user,
   e. Periodic reviewing “privileged accounts,”
f. Periodic reviewing of users enrolled in any system,
g. Assigning a new authentication token (e.g. password reset processing), and
h. Proper enforcement of user management shall be verified during an independent annual risk assessment.

3. The appropriate information owner or other authorized officer shall make requests for the registration and granting of access rights for state employees.

4. For applications that interact with individuals that are not employed by an SE, the information owner is responsible for ensuring an appropriate user management process is implemented. Standards for the registration of such external users shall be defined, to include the credentials that shall be provided to prove the identity of the user requesting registration, validation of the request, and the scope of access that may be provided.

8.14. USER PASSWORD MANAGEMENT

Passwords are a common means of authenticating a user’s identity to access an information system or service. Password standards shall be developed and implemented to ensure all authorized individuals accessing SE resources follow proven password management practices. These password rules shall be mandated by automated system controls whenever possible. These password best practices include but are not limited to:

1. SEs compliance with NMAC 1.12.11.16 (Password Policy),
2. Prohibiting the storage of passwords in clear text,
3. Using passwords that are not easily guessed or subject to disclosure through a dictionary attack is prohibited,
4. Keeping passwords confidential,
5. Prohibiting all password sharing,
6. Changing passwords at regular intervals,
7. Changing temporary passwords at the first logon,
8. Enforcing implementation standard password formats containing a mix of alphabetic, numeric, special, and upper/lower case characters,
9. Not including passwords in any automated logon process (e.g., stored in a macro or function key, web browser or in application code),
10. Implementing password standards on SE computing resources, and
11. Verifying proper enforcement of password management during an independent annual risk assessment.

8.15. USE OF PERSONAL COMPUTING DEVICES

Personal computing devices include, but are not limited to, removable media such as thumb or USB drives, external hard drives, laptop or desktop computers, cellular phones, or personal digital assistants (PDA's) owned by or purchased by SE employees, contract personnel, or other non-state user.
1. The connection of any computing device not owned by the state of New Mexico to a state network or to any state computing device is prohibited.

2. The installation of any software, executable, or other file to any state computing device is prohibited if that software, executable, or other file was downloaded by, is owned by, or was purchased by an employee or contractor with their own funds.

3. The installation of downloaded software, executables, or other files to any state computing device is prohibited when downloaded or installed by an employee or contractor for personal use. Downloaded software, executable, or other files include, but are not limited to: SKYPE, music files or software, and personal photos.

8.16. VULNERABILITY SCANNING

1. All SE-owned computing devices that are, or will be in the future, accessible from outside the SE network shall be scanned for vulnerabilities and weaknesses before installation on the network and after software, operating system, or configuration changes are made.

2. For both internal and external systems, scans shall be performed at least annually to ensure that no major vulnerabilities have been introduced into the environment. The frequency of additional scans shall be determined by the SE ISO, depending on the criticality and sensitivity of the information on the system.

3. Network vulnerability scanning shall be conducted after new network software or hardware have been installed and after major configuration changes have been made on critical and essential SE systems.

4. The output of the scans shall be reviewed in a timely manner by the SE ISO and communicated to the SE CIO.

5. Any vulnerability detected as a result of a scan shall be evaluated for risk and mitigated as appropriate.

6. Tools used to scan for vulnerabilities shall be updated periodically to ensure that recently discovered vulnerabilities are included in any scans.

7. If a SE has outsourced a server, application, or network services to another SE, the responsibility for vulnerability scanning shall be coordinated by both SEs.

8. Anyone authorized to perform vulnerability scanning shall have a process defined, documented, tested, and followed at all times to minimize the possibility of disruption. Reports of exposures to vulnerabilities shall be forwarded to the SE CIO and SE general counsel.

9. Any vulnerability scanning other than that performed by SE ISO shall be conducted only by qualified individuals or organizations contracted with or authorized in writing by the SE’s CIO.

8.17. PENETRATION AND INTRUSION TESTING

All SE computing infrastructure that provides information through a public network, either directly or through another service, and that provides information externally (such as the
World Wide Web), shall be subject to annual independent SE penetration analysis and intrusion testing by qualified third-party.

1. Penetration analysis and testing shall be used to determine whether:
   a. An individual can make an unauthorized change to an application,
   b. A user can access the application and cause it to perform unauthorized tasks, and
   c. An unauthorized individual can access, destroy or change any data,
   d. An unauthorized individual may access the application and cause it to take actions unintended by the application designer(s).

2. The output of the penetration testing and intrusion testing shall be reviewed in a timely manner by the SE ISO and the SE CIO, and any vulnerability detected shall be evaluated for risk and mitigated appropriately.

3. The tools used to perform the penetration testing shall be updated frequently to ensure that recently discovered vulnerabilities are included in any testing.

4. Where a SE has outsourced a server, application, or network services to another SE, independent penetration testing shall be coordinated by both SEs.

5. Only individuals authorized by the SE shall perform penetration testing. The SE ISO shall notify DoIT security staff 24 hours prior to each penetration test. Any attempts to perform penetration testing without prior DoIT notification shall be deemed an unauthorized access attack.

6. All documents pertaining to security penetration tests, security investigations, security data and reports shall be categorized as sensitive and protected from public disclosure.

8.18. PROTECTION AGAINST MALICIOUS CODE

1. Software and associated controls shall be implemented across SE systems to prevent and detect the introduction of malicious code. The introduction of malicious code such as a computer virus, network worm program, and Trojan horses can cause serious damage to networks, workstations, and business data.

2. SE users shall be made aware of the dangers of unauthorized or malicious code.

3. SE shall implement controls to detect and prevent a computer virus from being introduced to the SE environment. The types of controls and frequency of updating signature files shall be dependent on the value and sensitivity of the information at risk.

4. For most SE workstations, virus signature files shall be updated weekly. On host systems or servers, the signature files shall be updated daily or when the virus software vendor’s signature files are updated and made available.

8.19. MESSAGE INTEGRITY

1. A method to detect unauthorized changes to the content of a transmitted electronic message is required.
2. An assessment of threats and risks shall be performed to determine if message integrity is required and to identify the most appropriate method of implementation. Message integrity may not protect against unauthorized disclosure.

3. Message integrity shall be considered for any application in which there is a security requirement to protect the message or data content (e.g. electronic funds transfer, EDI transactions).

8.20. KEY MANAGEMENT

1. A secured environment shall be established to protect the cryptographic keys used to encrypt and decrypt information. Keys shall be securely distributed and stored. Access to cryptographic keys shall be restricted to only those individuals who have a business need to know. Compromise of a cryptographic key would cause all information encrypted with that key to be considered unencrypted.

8.21. CRITICALITY ASSESSMENT

An assessment of the criticality of the services provided and the sensitivity of the information held on all hosts and servers (including all installed software and operating system versions, firewalls, switches, routers and other communication equipment operating systems) shall be maintained.

8.22. SYSTEM SECURITY CHECKING

1. Systems and services that process or store sensitive or confidential or provide support for critical processes shall undergo technical security reviews to ensure compliance with implementation standards and for vulnerabilities to subsequently discovered threats. Reviews of systems and services that are essential to supporting a critical SE function shall be conducted at least once every year. Reviews of a representative sample of all other systems and services shall be conducted at least once every 24 months.

2. Any deviations from expected or required results that are detected by the technical security review process shall be reported to the SE ISO and to the SE CIO and corrected immediately. In addition, the SE staff shall be advised of the deviations and shall initiate investigation of the deviations (including the review of system activity log records if necessary).

8.23. SECURITY OF ELECTRONIC MAIL

Electronic mail provides an expedient method of creating and distributing messages both within the organization and outside of the organization. Users of the SE e-mail system are a visible representative of the State and shall use the systems in a legal, professional, and responsible manner.

1. Unless prior written state CIO approval has been obtained, SE users shall not be allowed to connect to third-party e-mail systems (e.g., AOL, Yahoo) from any SE system or workstation.
2. Users of SE e-mail systems shall comply with this policy and are required to follow NMAC 1.12.10 "Internet, Intranet, and Email and Digital Network Usage".

8.24. INTERNET AND ELECTRONIC MAIL ACCEPTABLE USE

1. SEs users and contractors are required to follow NMAC 1.12.10 "Internet, Intranet, and Email and Digital Network Usage."

2. When SE employees connect to the Internet using any SE Internet address designation, or send electronic mail using the SE designation, that email shall be for purposes authorized by SE management in accord with NMAC 1.12.10. The examples of behavior that could result in a security breach and be subject to disciplinary actions by the SE include, but are not limited to:
   a. Spoofing (e.g., representing yourself as someone else),
   b. Spamming,
   c. Cracking or hacking (e.g., unauthorized attempts to access or break into any computing system, including any state system, for which explicit authorization has not been granted),
   d. Theft or unauthorized copying of electronic files,
   e. Posting sensitive or confidential information without authorization in writing from SE management,
   f. Any activity that creates a denial of services attack, including chain letters, and
   g. Sniffing (e.g., monitoring network traffic) unless specifically authorized by SE IT management to do so as part of a job assignment, and
   h. Connecting to a third-party email system without prior written approval by the SE CIO.

8.25. PORTABLE DEVICES AND REMOVABLE MEDIA

1. All portable computing resources and removable media shall be secured to prevent compromise of confidentiality or integrity. No computer device may store or transmit sensitive information without suitable protective measures that are approved by the SE CIO.

2. When using mobile computing devices such as notebooks, PDAs, laptops, and mobile phones, special care shall be taken to ensure that information is not leaked or compromised. Approval by the SE CIO shall be based on satisfactory documentation that the requirements for physical protection, access controls, cryptographic techniques, back-ups, malware and malicious codes protection and the rules associated with connecting mobile devices to networks and guidance on the use of these devices in public places have been met.

3. Care shall be taken when using mobile computing devices in public places, meeting rooms and other unprotected areas outside of the SE's premises. Protection, such as using cryptographic techniques, shall be in place to avoid the unauthorized access to or disclosure of the information stored and processed by these devices.
4. It is important that when such devices are used in public places care shall be taken to avoid the risk of unauthorized persons viewing sensitive or protected information on-screen.

5. Procedures protecting against malicious software shall be developed, implemented, and be kept up to date.

6. Computing infrastructure containing sensitive or protected information shall be attended at all times shall be secured.

7. Training shall be provided to staff using mobile computing resources to raise their awareness with respect to additional risks resulting from the use of mobile devices and the controls that shall be implemented by the SE.

8. Employees in the possession of portable, laptop, notebook, PDA, or other transportable computing device shall not check these computers in airline luggage systems or left in an unlocked vehicle. These computers shall remain in the possession of the traveler as hand luggage unless other arrangements are required by Federal or state authorities.

8.26 TELEPHONES AND FAX EQUIPMENT

1. Sending documents containing sensitive and confidential information via fax is prohibited unless required by federal law,

2. Using Internet fax services to send or receive sensitive and confidential information is prohibited,

3. Using third-party fax services to send or receive sensitive and confidential information is prohibited,

4. Sending documents containing sensitive and private information via wireless fax devices is prohibited,

5. Sending teleconference call-in numbers and pass codes to a pager is prohibited, when sensitive and confidential information shall be discussed during the conference, and

6. Teleconference chair people shall confirm that all participants in the teleconference are authorized participants, if sensitive or confidential information shall be discussed.

8.27 MODEM USAGE

Connecting any dial-up modem to computer systems which are also connected to SE’s local area network, to the state network, or to another internal communication network is prohibited.

8.28 PUBLIC WEBSITES CONTENT APPROVAL PROCESS

1. Sensitive information shall not be made available through a server that is accessible to a public network without appropriate safeguards approved in writing by the SE CIO. The SE ISO shall implement safeguards to ensure user authentication, data confidentiality and integrity, access control, data protection and logging mechanisms.

2. The design of a hosting service shall be reviewed and approved in writing by the SE CIO to ensure that the security of the web server, protection of SE networks,
performance of the site, integrity, and availability considerations are adequately addressed.

3. Prior to being put into production, all SE websites shall be tested for security vulnerabilities. This testing shall include, but not be limited to, the Open Web Application Security Project (OWASP) "Top 10" vulnerabilities and the OWASP "Top 25" programming errors.

4. SE website content shall be reviewed and approved by the SE CIO to ensure that the collection and processing of information meets SE security and privacy requirements. The review shall ensure that the information is adequately protected in transit over public and SE networks, in storage, and while being processed.

8.29. ELECTRONIC SIGNATURES

Each SE shall provide the personnel and resources to comply with the New Mexico State's Uniform Electronic Transactions Act (NMSA 1978 14-16-1 through 14-16-19).

8.30. BUSINESS CONTINUITY

The scope of this section is limited to the IT infrastructure and the data and applications of the local SE environment.

1. A threat and risk assessment shall be performed by the SE to determine the criticality of business systems and the time frame required for recovery.

2. To ensure interruptions to normal SE business operations are minimized and critical SE business applications and processes are protected from the effects of major failures, each SE business unit or each SE ISO under the direct guidance of the SE CIO shall develop plans that can meet the IT backup and recovery requirements of the SE.

3. Back-ups of critical SE data and software shall be performed regularly.

8.31. LOGON BANNER

1. Logon banners shall be implemented on all systems to inform all users that SE systems are only for SE business and other approved uses consistent with SE policy, to inform that users their activities may be monitored, and to inform the user that they have no expectation of privacy.

2. Logon banners shall be displayed on computer screens during the authentication process.

8.32. MONITORING SYSTEM ACCESS AND USE

1. Consistent with applicable law, contracts, and SE policies, the SE reserves the right to monitor, inspect, and/or search at any time, all SE information systems. Since SE's computers and networks are provided for business purposes, staff members and contract personnel shall have no expectation of privacy in the information stored in, or sent through these information systems. SE management additionally retains the right to remove from its information systems any unauthorized material.
2. Systems and applications shall be monitored and analyzed to detect deviation from the access control policy.

3. Events shall be recorded to provide evidence and to reconstruct lost or damaged data.

4. Audit logs shall be used to record exceptions and other security-relevant events.

5. Audit log reports shall be produced and kept consistent with record retention schedules developed in cooperation with the State Records and Archives and SE requirements to assist in future investigations.

9. SYSTEMS DEVELOPMENT AND MAINTENANCE POLICY

Software applications are developed or acquired to provide efficient solutions to SE business needs. These applications generally store, manipulate, retrieve, and display information used to conduct SE business. As SE business units become dependent on these applications and it is essential the data processed by these applications be accurate, and it is critical that the software that performs these activities be protected from unauthorized access, modification, or destruction.

1. To ensure that security is built into all SE information systems, all security requirements including the need for rollback arrangements, shall be identified during the requirements elicitation phase of the software development lifecycle, and agreed upon and documented in the information system Requirements Document. To ensure this activity is performed, the SE ISO shall be involved in the requirements elicitation, design, and testing phases of the System Development Lifecycle.

2. Security requirements and controls shall be commensurate with the business value of the information and risk of loss and damage that might result from failed or absent of security controls. This policy is especially critical for Internet, Web, and online applications.

3. The framework for analyzing the security requirements, risks, and the application of security controls to mitigate risks is governed by threat assessment and risk management procedures which shall be developed in conjunction with the information owner, reviewed by the SE ISO, and approved in writing by the SE CIO.

4. A process shall be established and implemented for each application to:
   a. Address the business risks and develop a profile of the data to help to understand the risks,
   b. Identify security measures based on the risk profile and protection requirements,
   c. Identify and implement specific controls based on security requirements and technical architecture,
   d. Implement a method to test the effectiveness of the security controls,
   e. Identify processes and standards to support changes, ongoing management and to measure compliance.

5. Controls in systems and applications can be placed in many places and serve a variety of purposes. The specific control mechanisms shall be documented at the application level, SE’s System Development Methodology, and in the SE’s security standards documents.
The security measures that are implemented shall be based on the threat and risk assessments of the information being processed and cost/benefit analysis.

9.1. SEPARATION OF DEVELOPMENT, TEST, AND PRODUCTION ENVIRONMENTS

Separation of the development, test, and production environments is required and can be accomplished either logically or physically. Development and testing can cause serious problems to the production environment if separation of these environments does not exist. The degree of separation between the development, test, and production environments shall be considered by each SE to ensure adequate protection of the production environment.

1. Processes shall be documented and implemented to govern the transfer of software from the development environment to the production platform. The following controls shall be considered:

2. Development software and tools shall be maintained on computer systems that are physically and logically isolated from the production environment.

3. Access to compilers, editors, and other system utilities shall be removed from production systems when not required.

4. Logon procedures shall be sufficiently unique to the production, testing, and development environments.

5. Each SE shall consider the use of a stable quality assurance environment where user acceptance testing can be conducted and changes cannot be made to the programs being tested.

9.2. SYSTEM PLANNING AND ACCEPTANCE

1. Advance planning and preparation shall be performed to ensure the availability of adequate capacity and resources. The security requirements of new systems shall be established, documented, and tested prior to their acceptance and use.

2. Storage and memory capacity demands shall be monitored and future capacity requirements projected to ensure adequate processing and storage capability is available when needed. This information shall be used to identify and avoid potential bottlenecks that might present a threat to system security or user services.

3. Acceptance criteria shall be developed and documented for new information systems, upgrades, and new versions of existing systems. Acceptance testing shall be performed to ensure security requirements are met prior to the system being migrated to the production environment. SE managers shall ensure that the security requirements and criteria for acceptance are clearly defined, agreed, documented, and tested.

9.1. SOFTWARE MAINTENANCE

1. All system software shall be maintained at a vendor-supported level to ensure software accuracy and integrity, unless the SE CIO approves otherwise in writing.
2. Maintenance of SE-developed software shall be logged to ensure changes are authorized, tested, and accepted by SE CIO.

3. All known security patches shall be reviewed, evaluated, and appropriately applied in a timely manner to reduce the risk of security incidents that could affect the confidentiality, integrity, and availability of business data or software integrity.

9.2. INPUT DATA VALIDATION
1. An application’s input data shall be validated to ensure it is correct and appropriate. Data input errors shall be detected and prevented.

2. Data validation may be automated (performed by the system) or performed by personnel. If personnel are used, their roles and responsibilities shall be clearly identified.

3. Data integrity checks performed on the client side shall also be performed at the server.

4. Data integrity checks also shall be performed on the input of business transactions, static data (e.g., names, addresses, and employee numbers) and parameter tables.

5. Processes shall be established to verify and correct fields, characters, completeness of data, and range/volume limits.

9.3. CONTROL OF INTERNAL PROCESSING
Data that has been entered correctly can be corrupted by processing errors or through deliberate acts.

1. Checks and balances shall be incorporated into systems to prevent or stop an incorrect program from running.

2. The application design shall ensure that controls are implemented to minimize the risk of processing failures leading to a loss of data or system integrity. Correction programs to recover from failures, access to add and delete functions, to make changes to application data, and to ensure the correct processing of data should be considered.

9.4. PROTECTION OF SYSTEM TEST DATA
All test data shall not contain sensitive or confidential information.

9.5. CHANGE CONTROL PROCEDURES
To minimize the possibility of corruption of information systems, strict controls over changes to information systems shall be implemented. These change control procedures shall apply to SE business applications as well as systems software used to maintain operating systems, network software, or hardware changes.

1. Each SE is responsible for developing, implementing, and enforcing a formal change control process for all applications that ensures:
   a. Security and control procedures are not compromised.
b. Support programmers are given access only to those parts of a system necessary to perform their jobs.

c. A formal agreement and approval processes for changes are implemented.

d. As changes occur, all associated system documentation and the SE disaster plan are updated accordingly.

e. Access to source code libraries for both SE applications and operating systems shall be tightly controlled to ensure that only authorized individuals have access to these libraries and that access is logged to ensure all activity can be monitored.

10. RISK MANAGEMENT
SE shall conduct periodic assessments of risk, including the cost of loss and the magnitude of harm that could result from the unauthorized access, use, disclosure, disruption, modification, or destruction of information and information systems that support the operations and assets of the SE.

10.1. CONDUCTING A RISK ASSESSMENT
SE shall periodically conduct a risk assessment of system to address changing threats and organizational priorities. At a minimum, SE risk assessments shall:

1. Identify IT systems, resources and information that constitute each system and prioritize the relative importance of the system assets,
2. Identify and document potential threat-sources,
3. Identify and document system vulnerabilities that could be exploited, and
4. Analyze security controls that have been implemented or are planned for implementation that minimize or eliminate the likelihood of a compromise occurring.

10.2. IMPLEMENTATION OF RISK A RISK MITIGATION STRATEGY
SE shall prioritize, evaluate, and implement strategically selected controls. The goal of risk mitigation is to select and implement controls that reduce risk to an acceptable level.

The SE shall:

1. Evaluate and compare the security countermeasures available, and the resources required to implement them, with the resources required to replace the Information system assets.
2. Determine which countermeasures are reasonable to employ.
3. Establish guidelines for implementing management, operational and technical security controls commensurate with the established risk to system assets.
11. CYBER SECURITY CITIZENS’ NOTIFICATION POLICY

For purposes of this Cyber Security Citizens’ Notification Policy, the terms “personal information” and “private information” shall have the meanings prescribed by section of New Mexico Law.

New Mexico State values the protection of private information of individuals. This policy requires notification to both impacted New Mexico residents and non-residents.

1. All SEs are required to notify an individual when there has been or is reasonably believed to have been a compromise of the individual’s private information.

2. The SE, after consulting with DoIT and security steering committee shall determine the scope of the breach and restoration measures, shall notify an individual when it has been determined that there has been or is reasonably believed to have been a compromise of private information through unauthorized disclosure.

3. If encrypted data is compromised along with the corresponding encryption key, the data shall be considered unencrypted and is subject to the notification requirements.

4. Notification may be delayed if a law enforcement agency determines that the notification impedes a criminal investigation. In such case, notification shall be delayed only as long as needed to determine that notification no longer compromises any investigation.

5. SE shall notify the affected individual. Such notice shall be directly provided to the affected persons by one of the following methods:
   a. Written notice;
   b. Electronic notice, provided that the person to whom notice is required has expressly consented to receiving said notice in electronic form and a log of each such notification is kept by the SE who notifies affected persons in such form;
   c. E-mail notice when such SE has an e-mail address for the subject persons;
   d. Telephone notification provided that a log of each such notification is kept by the SE who notifies affected persons;
   e. Substitute notice, if a SE demonstrates to the state Attorney General that the cost of providing notice would exceed two hundred fifty thousand dollars, or that the affected class of subject persons to be notified exceeds five hundred thousand, or such SE does not have sufficient contact information;
   f. Conspicuous posting of the notice on such SE’s web site page, if the SE maintains one; and
   g. Notification to major statewide media.

6. The SE shall notify DoIT, and security steering committee with respect to the timing, content, and distribution of the notices and approximate number of affected persons.

7. When notification to a New Mexico resident is necessary, the SE shall notify the Attorney General and the state Consumer Protection Board with respect to the timing, content and distribution of the notices, and approximate number of affected persons.
8. Regardless of the method by which notice is provided, such notice shall include:
   a. Contact information for the SE making the notification, and a
   b. Description of the categories of information that were, or are reasonably believed to have been, acquired by a person without valid authorization including specification of which of the elements of personal information and private information were or are reasonably believed to have been so acquired.

9. This policy also applies to information maintained on behalf of a SE by a third-party.

10. When more than five thousand (5,000) New Mexico residents are to be notified at one time, the SE shall notify the consumer reporting agencies with respect to the timing, content, and distribution of the notices, and the approximate number of affected individuals. This notice however, shall be made without delaying notice to the individuals.

12. COMPLIANCE POLICY

1. DoIT and security steering committee may periodically review compliance by State entities to this policy. Such reviews may include, but are not limited to, reviews of the technical and business analyses required to be developed pursuant to this policy and other project documentation, technologies, or systems that are the subject of the published policy or standard.

2. Each user shall understand his/her role and responsibilities regarding information security issues and protecting SE’s information. The failure to comply with this or any other security policy that results in the compromise of SE information confidentiality, integrity, privacy, and/or availability may result in appropriate disciplinary action as permitted by law, rule, regulation, or negotiated agreement. Each SE shall take every step necessary, including legal and administrative measures, to protect its assets and shall establish the post of SE Information Security Officer to monitor compliance with policy matters.

3. SE managers and supervisors shall ensure all security processes and procedures within their areas of responsibility are followed. In addition, all business units within the SE may be subject to regular reviews to ensure compliance with security policies and standards.

12.1. ENFORCEMENT AND VIOLATION HANDLING

1. Any compromise or suspected compromise of this policy shall be reported to the appropriate SE CIO, the SE Information Security Officer, DoIT, and security steering committee as required by this policy. Any violations of security policies may be subject to disciplinary or other appropriate action in accordance with law, rule, regulation, policy, or negotiated agreement.

2. Security incident reports indicating the risk level of the violation shall be reported to responsible entities in accordance with SE labor relations.
3. Access authorization for user accounts involved in a compromise may be suspended during the time when a suspected violation is under investigation. Automated violation reports generated by the various security systems shall be forwarded to the SE CIO and the SE Information Security Officer for timely resolution.

12.2. **AMENDMENT OF STATE OF NEW MEXICO SECURITY POLICY**

Requests for changes to this policy shall be presented by the SE CIO to DoIT and to the security steering committee. If DoIT and the security steering committee agree, DoIT shall formally draft the change and have it reviewed and approved through the security steering committee normal policy approval process. Each SE CIO shall be responsible for communicating the approved changes to their organization.

This policy and supporting policies and standards shall be reviewed at a minimum on an annual basis.
<table>
<thead>
<tr>
<th><strong>Definitions and Acronyms</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Approved Storage Facility:</strong></td>
</tr>
<tr>
<td><strong>Asset</strong></td>
</tr>
<tr>
<td><strong>Authentication:</strong></td>
</tr>
<tr>
<td><strong>Authorization:</strong></td>
</tr>
<tr>
<td><strong>Availability:</strong></td>
</tr>
<tr>
<td><strong>Biometric Data:</strong></td>
</tr>
<tr>
<td><strong>Business Risk:</strong></td>
</tr>
<tr>
<td><strong>CIO:</strong></td>
</tr>
<tr>
<td><strong>Classification:</strong></td>
</tr>
<tr>
<td><strong>Computer:</strong></td>
</tr>
<tr>
<td><strong>Confidentiality:</strong></td>
</tr>
<tr>
<td><strong>Consumer Reporting Agency:</strong></td>
</tr>
<tr>
<td><strong>Controls:</strong></td>
</tr>
<tr>
<td><strong>Copyright:</strong></td>
</tr>
<tr>
<td><strong>CPE:</strong></td>
</tr>
<tr>
<td><strong>Cracking:</strong></td>
</tr>
<tr>
<td>---------------</td>
</tr>
<tr>
<td><strong>Cryptographic:</strong></td>
</tr>
<tr>
<td><strong>Cryptographic Key:</strong></td>
</tr>
<tr>
<td><strong>Data:</strong></td>
</tr>
<tr>
<td><strong>Denial of Service:</strong></td>
</tr>
<tr>
<td><strong>Disaster:</strong></td>
</tr>
<tr>
<td><strong>DMZ:</strong></td>
</tr>
<tr>
<td><strong>Electronic Storage Media:</strong></td>
</tr>
<tr>
<td><strong>Encryption:</strong></td>
</tr>
<tr>
<td><strong>Field Level Encryption:</strong></td>
</tr>
<tr>
<td><strong>File Level Encryption:</strong></td>
</tr>
<tr>
<td><strong>Firewall:</strong></td>
</tr>
<tr>
<td><strong>Folder Level Encryption:</strong></td>
</tr>
<tr>
<td><strong>Full Disk Encryption:</strong></td>
</tr>
<tr>
<td><strong>Host:</strong></td>
</tr>
<tr>
<td><strong>Incident:</strong></td>
</tr>
<tr>
<td><strong>Incident Response:</strong></td>
</tr>
<tr>
<td><strong>Information:</strong></td>
</tr>
<tr>
<td><strong>Information Custodian:</strong></td>
</tr>
<tr>
<td>--------------------------</td>
</tr>
<tr>
<td><strong>Information Owner:</strong></td>
</tr>
<tr>
<td><strong>Information Security:</strong></td>
</tr>
<tr>
<td><strong>Information Security Architecture:</strong></td>
</tr>
<tr>
<td><strong>Integrity:</strong></td>
</tr>
<tr>
<td><strong>Intranet:</strong></td>
</tr>
<tr>
<td><strong>Internet:</strong></td>
</tr>
<tr>
<td><strong>Intrusion Detection:</strong></td>
</tr>
<tr>
<td><strong>ISO:</strong></td>
</tr>
<tr>
<td><strong>Least Privilege:</strong></td>
</tr>
<tr>
<td><strong>Malicious Code:</strong></td>
</tr>
<tr>
<td><strong>Media Access Control (MAC) address:</strong></td>
</tr>
<tr>
<td><strong>Multi-User System:</strong></td>
</tr>
<tr>
<td><strong>Need to Know/Need to Do:</strong></td>
</tr>
<tr>
<td><strong>Passphrase:</strong></td>
</tr>
<tr>
<td><strong>PDA:</strong></td>
</tr>
<tr>
<td><strong>Penetration Testing:</strong></td>
</tr>
<tr>
<td><strong>Personal Digital Assistant (PDA):</strong></td>
</tr>
<tr>
<td>-----------------</td>
</tr>
<tr>
<td><strong>Personal Computing Device</strong></td>
</tr>
</tbody>
</table>
| **Sensitive and Confidential Information** | Any information where unauthorized access, disclosure, modification, destruction or disruption of access to or use of such information could severely impact the SE, its critical functions, its employees, its customers, third parties, or citizens of New Mexico. This term shall be deemed to include, but is not limited to, the information encompassed in existing statutory definitions. Sensitive or confidential includes, but is not limited to:  
- Information concerning a person which, because of name, number, personal mark or other identifier, can be used to identify that person, in combination with:
  - Social Security Number or any number derived from the Social Security Number,  
  - Driver’s license number or non-driver identification card number, or  
  - Mother’s maiden name, financial services account number or code, savings account number or code, checking account number or code, debit card number or code, automated teller machine number or code, electronic serial number.  
- Other information which could be used to assume a person’s identity or gain access to a person’s financial resources or credit.  
- Information used to authenticate the identity of a person or process (e.g., PIN, password, passphrase, and biometric data). This does not include distribution of one-time-use PINs, passwords, or passphrases.  
- Information that identifies specific structural, operational, or technical information, such as maps, mechanical or architectural drawings, floor plans, operational plans or procedures, or other detailed information relating to electric, natural gas, steam, water supplies, nuclear or telecommunications systems or infrastructure, including associated facilities, including, but not limited to:  
  - Training and security procedures at sensitive facilities and locations as determined by the |
<table>
<thead>
<tr>
<th>Office of Homeland Security (OHS), TM descriptions of technical processes and technical architecture, TM plans for disaster recovery and business continuity, and TM reports, logs, surveys, or audits that contain sensitive information. • Security related information (e.g., vulnerability reports, risk assessments, security logs). • Other information that is protected from disclosure by law or relates to subjects and areas of concern as determined by SE executive management.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Physical Security:</strong> The protection of information processing equipment from damage, destruction or theft, information processing facilities from damage, destruction or unauthorized entry, and personnel from potentially harmful situations.</td>
</tr>
<tr>
<td><strong>Privacy:</strong> The right of individuals and organizations to control the collection, storage, and dissemination of information about themselves.</td>
</tr>
<tr>
<td><strong>Privileged Account:</strong> The userID or account of an individual whose job responsibilities require special system authorization, such as a network administrator, security administrator, etc. Special authorizations are allocated to this account such as RACF Administrator, auditor, Special, UNIX root or Microsoft Administrator.</td>
</tr>
<tr>
<td><strong>Procedures:</strong> Specific operational steps that individuals shall take to achieve goals stated in this policy.</td>
</tr>
<tr>
<td><strong>Remote Access:</strong> Any access coming into the SE’s network from off the SE’s private trusted network. This includes, but is not limited to, dialing in from another location over public lines by an employee or other authorized individual.</td>
</tr>
<tr>
<td><strong>Risk:</strong> The probability of suffering harm or loss. It refers to an action, event or a natural occurrence that could cause an undesirable outcome, resulting in a negative impact or consequence.</td>
</tr>
<tr>
<td><strong>Risk Assessment:</strong> The process of identifying threats to information or information systems, determining the likelihood of occurrence of the threat, and identifying system vulnerabilities that could be exploited by the threat.</td>
</tr>
<tr>
<td><strong>Risk Management:</strong> The process of taking actions to assess risks and avoid or reduce risk to acceptable levels.</td>
</tr>
<tr>
<td><strong>Role-Based Access Control:</strong> An approach to restricting system access where permissions to perform certain operations are assigned to specific job functions.</td>
</tr>
<tr>
<td><strong>SE:</strong> See State Entity (ies).</td>
</tr>
</tbody>
</table>
| **Security Administration:** The actions and responsibility for administering the security mechanisms including identification and authentication establishment and authorization.
| **Security Management:** | The responsibility and actions required to manage the security environment including the security policies and mechanisms. Imposed for all users. These rules usually rely on a comparison of the sensitivity of the resources being accessed and the possession of corresponding.

| **Security Policy:** | The set of criteria for the provision of security services based on global rules imposed for all users. These rules usually rely on a comparison of the sensitivity of the resources being accessed and the possession of corresponding attributes of users, a group of users, or entities acting on behalf of users.

| **Sensitivity:** | The measurable, harmful impact resulting from disclosure, modifications, or destruction of information.

| **Sniffing:** | Monitoring network traffic.

| **Spamming:** | Blindly posting something to a large number of groups.

| **Spoofing:** | Representing one's self as someone else.

| **Standard:** | Sets of rules for implementing policy. Standards make specific mention of technologies, methodologies, implementation procedures and other detail factors.

| **State:** | The State of New Mexico

| **State Entity(ies):** | State Entity for the purpose of this policy shall include all State agencies, departments, offices, divisions, boards, bureaus, commissions and other entities over which the Governor has executive power.

| **Systems(s):** | An interconnected set of information resources under the same direct management control that shares common functionality. A system may include hardware, software, information, data, applications or communications infrastructure.

| **Technical Security Review:** | A technical security review would consist of reviewing the controls built into a system or application to ensure they still perform as designed and are in compliance with documented security policies and procedures. It would also include reviewing security rules such as access control lists for currency, testing of firewall rules, etc. This type of testing includes intrusion and/or penetration testing of controls.

| **Third-party:** | Any non-SE employee such as a contractor, vendor, consultant, intern, another SE (e.g., Office for Technology), etc.

| **Threat:** | A force, organization or person, which seeks to gain access to, or compromise, information. A threat can be assessed in terms of the probability of an attack. Looking at the nature of the threat, its capability and resources, one can assess it, and then determine the likelihood of occurrence, as in risk assessment.

| **Trojan Horse:** | Malicious code hidden in a legitimate program that when executed performs some unauthorized activity or function.

| **Unauthorized Access:** | Insider or outsider who gains access to network or computer resources without permission or without valid authorization.
<table>
<thead>
<tr>
<th><strong>USB Flash Drive:</strong></th>
<th>A solid state memory storage device integrated with a USB interface.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>User:</strong></td>
<td>Any State entity(ies), federal government entity(ies), political subdivision(s), their employees or third-party contractor(s) or business associates, or any other individual(s) who are authorized by such entities to access a system for a legitimate government purpose.</td>
</tr>
<tr>
<td><strong>Value:</strong></td>
<td>A measure of worth which can be expressed in monetary terms or in terms of importance to the SE.</td>
</tr>
<tr>
<td><strong>Virus:</strong></td>
<td>A program that replicates itself on computer systems by incorporating itself into other programs that are shared among computer systems. Once in the new host, a virus may damage data in the host’s memory, display unwanted messages, crash the host or, in some cases, simply lie dormant until a specified event occurs (e.g., the birth date of a historical figure).</td>
</tr>
<tr>
<td><strong>Volume Level Encryption:</strong></td>
<td>Protects data by encrypting the entire partition of a disk or, in the case of a single partition hard drive, the entire drive.</td>
</tr>
<tr>
<td><strong>Vulnerability:</strong></td>
<td>A weakness of a system or facility holding information which can be exploited to gain access or violate system integrity. Vulnerability can be assessed in terms of the means by which the attack would be successful.</td>
</tr>
<tr>
<td><strong>Vulnerability Scanning:</strong></td>
<td>The portion of security testing in which evaluators attempt to identify physical, network, system or application weaknesses to discover whether these weaknesses may be exploited by persons or machines seeking to gain either unauthorized or elevated privileged access to otherwise protected resources.</td>
</tr>
<tr>
<td><strong>Workforce:</strong></td>
<td>State employees, and other persons whose conduct, in the performance of work for the SE, is under direct control of the SE, whether or not they are paid by the SE.</td>
</tr>
<tr>
<td><strong>Wide Web (WWW):</strong></td>
<td>A hypertext-based system designed to allow access to information in such a way that the information may physically reside on locally or geographically different servers. This access was greatly improved through the introduction of a graphical interface to the World Wide Web called a web browser. Netscape and Explorer are two of the most popular web browsers.</td>
</tr>
<tr>
<td><strong>Worm:</strong></td>
<td>A program similar to a virus that can consume large quantities of network bandwidth and spread from one network to another.</td>
</tr>
</tbody>
</table>