AGENDA
STATE GOVERNMENT COUNCIL
Executive Building - Lower Level Conference Room
521 S 14th Street
Lincoln, Nebraska
Thursday, April 13, 2017
1:30 p.m.

WORKING SESSION

1:30 p.m.	1.	Roll Call; Meeting Notice; Open Meetings Act Information	Chair
	2.	Discussion of Proposal 17-01 Information Security Policy *(Attachment 2)*	
2:30 p.m.	3.	Adjourn	

Meeting notice was posted to the NITC website and the Nebraska Public Meeting Calendar on March 27, 2017. The agenda was posted to the NITC website on April 10, 2017.

Nebraska Open Meetings Act

Attachment 2

State of Nebraska
Nebraska Information Technology Commission
Technical Standards and Guidelines

Proposal 17-01

A PROPOSED NEW POLICY relating to information security.

Section 1. The following provisions constitute a new CHAPTER 8 of the Technical Standards and Guidelines:

CHAPTER 8

INFORMATION SECURITY POLICY

Article.

1. Purpose; Scope; Roles and Responsibilities; Enforcement and Policy Exception Process.
2. General Provisions.
3. Access Control.
4. Network Security.
5. System Security.
6. Application Security.
7. Auditing and Compliance.
8. Vulnerability and Incident Management.
9. Data Security.

ARTICLE 1

PURPOSE; SCOPE; ROLES AND RESPONSIBILITIES; ENFORCEMENT AND POLICY EXCEPTION PROCESS

8-101. Purpose

The Nebraska Information Technology Commission (NITC) has statutory responsibility to adopt minimum standards and guidelines for acceptable and cost-effective use of information technology, and to provide strategic direction for all State agencies and educational institutions for information technology.

The purpose of this Information Security Policy is to provide a uniform set of reasonable and appropriate security safeguards for protection of the confidentiality, integrity, and availability of State of Nebraska information collected, stored, and used to serve the citizens of the State of Nebraska. This Information Security Policy contains the safeguards, responsibilities and acceptable behaviors required to establish and maintain a secure environment.

8-102. Scope

This policy is applicable to State of Nebraska full-time and temporary employees, third-party contractors and consultants, volunteers and other agency workers (hereafter referred to as "Staff"), all State Agencies, Boards and Commissions (hereafter referred to as "Agency").

This Information Security Policy encompasses all systems, automated and manual, for which the State has administrative responsibility, including systems managed or hosted by third parties on behalf of an Agency.

Guidelines and standards, published by the NITC, which are associated with this policy, provide specific details for compliance with this Information Security Policy.

In the event an Agency has developed policies or additional requirements for Information Security, the more restrictive policy shall apply.

8-103. Roles and Responsibilities

State Agencies: Agencies that create, use or maintain information systems for the State of Nebraska must create and maintain an information security program consistent with this policy to ensure the confidentiality, availability, and integrity of the State's information assets.

Office of Chief Information Officer (OCIO)

The Chief Information Officer is the executor of this Information Security Policy, which establishes and monitors the effectiveness of information security, standards and controls within the State of Nebraska.

The Office of the CIO will modify this policy as directed by the NITC, or as needed to keep current with continually changing threats and technology.

State Information Security Officer (SISO)

The State Information Security Officer, operating through the Office of the Chief Information Officer, performs as a security consultant to Agencies and Agency Information Security Officers to assist the Agencies in meeting the requirements of this policy. The State ISO may also perform periodic reviews of agency security for compliance with this and other security policies and standards.

Agency Information Security Officer (AISO)

The Agency Information Security Officer has overall responsibility for ensuring the implementation, enhancement, monitoring and enforcement of the information security policies and standards for their Agency. The Agency Information Security Officer is responsible for providing direction and leadership to the Agency through the recommendation of security policies, standards, processes and education and awareness programs to ensure that appropriate safeguards are implemented, and to facilitate compliance with those policies, standards and processes. The Agency Information Security Officer is responsible for investigating all alleged information security violations. In this role, the Agency Information Security Officer will follow agency procedures for referring the investigation to other investigatory entities, including law enforcement. The agency Information Security Officer will coordinate and oversee security program activities and reporting processes in support of this policy and other security initiatives.

Nebraska Information Technology Commission (NITC)

The NITC is the owner of this policy with statutory responsibility to promote information security through adoption of policies, standards, and guidelines. The NITC develops strategies for implementing and evaluating the effectiveness of information security.

NITC Technical Panel

The NITC Technical Panel, with advice from the Security Architecture WorkGroup, is responsible for recommending security policies and guidelines and making available best practices to operational entities.

NITC State Government Council

The NITC State Government Council, with advice from the Security Architecture WorkGroup, is responsible for recommending security policies and guidelines and making available best practices to operational entities.

NITC Security Architecture WorkGroup

The NITC Security Architecture WorkGroup prepares policies, standards, and guidelines for state government. Make recommendations to the State Government Council and Technical Panel on matters relating to security within state government. Provide information to state agencies, policy makers, and citizens about security issues. Document existing problems, potential points of vulnerability, and related risks. Determine security requirements of state agencies stemming from state and federal laws or regulations.

8-104. Enforcement and Policy Exception Process

The State of Nebraska has established security policies and standards to describe the controls and activities necessary to appropriately protect information and information technology (IT) resources. While every exception to a policy or standard weakens the protection for Nebraska IT resources and underlying data, it is recognized that at times business requirements dictate a need for temporary policy exceptions. In the event an Agency believes it needs an exception to an NITC Policy or Standard, the Agency may request an exemption by following the procedure outlined in NITC Policy 1-103: Waiver Policy.

ARTICLE 2

GENERAL PROVISIONS

8-201. Acceptable Use Policy

State of Nebraska IT Resources can be effective tools for the staff provided they are used appropriately and adequately protected. It is the responsibility of every member of the staff to understand and comply with these standards. Should a violation of these standards occur, it is the responsibility of the Management for the department in violation to mitigate or remediate the violation in a timely manner.

Any violation of these standards by a party working directly for a Vendor may result in termination of the Vendor's contract or other measures in accordance with applicable state and federal laws and penalty provisions of the Vendor's contract.

Acceptable Use of IT Resources

IT devices are defined as desktop computers, servers, laptop computers, PDA's (personal digital assistant), MP3players, tablet computers, mainframe computers, printers, routers, switches, hubs, portable storage devices, digital cameras, cell phones, smart phone, multi-functional devices, and any other electronic device that creates, stores, processes, or exchanges State information. Hereinafter referred to as "IT devices". All State of Nebraska electronic business shall be conducted on approved IT devices only.

Use of State IT resources for any purpose other than to perform approved activities and as permitted by the Information Security Policy will be considered a violation of this standard. While not an exhaustive list, approved activities include company business and limited personal use that does not interfere with business activity. In all cases, users of IT resources are responsible for exercising good judgment regarding the reasonableness of a use of IT resources. In the event of any uncertainty, users should consult their manager or the SISO/AISO. The State of Nebraska owns all information compiled, stored, and used by the staff on State equipment and reserves the right to monitor all IT resources to verify compliance of this policy.

IT devices used by members of the staff to perform authorized business activities must be owned, leased, managed or approved by the State of Nebraska OCIO and meet specifications and requirements published by OCIO.

Members of the Staff are responsible for the reasonable protection and use of the Internal Network access assigned to them and must follow all State of Nebraska Information Security policies. State of Nebraska IT resources may not be used for any inappropriate or unlawful purpose.

- Sharing your access credentials is prohibited. You are responsible for protecting your credentials just like you would protect access to your own bank account.
- Confidential and Restricted data, as defined in NITC 8-903: Data Classification Standard, should never be sent via email unless it has been encrypted using technology approved by the State Information Security Officer (SISO) or the Agency Information Security

Officer (AISO). Note, password protecting email attachments is NOT the same as encrypting it.

- Confidential or Restricted data should never be place on portable media unless the portable media device is encrypted and approved by the SISO/AISO. Portable media includes laptops, thumb drives, removable disk drives, DVDs, etc. This data may not be stored, accessed, or processed on any equipment or media that is not owned, managed, or approved by the Department.
- The State of Nebraska infrastructure, including the network and all equipment, may not be used for any file storage, sharing, or downloading any music, video, or software unless approved by the OCIO.
- Accessing or attempting to access Confidential or Restricted information for other than a required business "need to know" is prohibited.
- Posting, texting, or otherwise distributing citizen, department, or employee information on any social media is prohibited.
- Remotely accessing systems containing Confidential or Restricted information from any equipment not specifically authorized or maintained by the OCIO is prohibited. All remote access to State resources containing Confidential or Restricted information shall be restricted to an approved remote connection (such as VPN) using multi-factor authorization.
- Conducting or soliciting illegal activities such as attempting to gain unauthorized access to restricted sites (hacking) is prohibited.
- Misrepresenting yourself as another individual or organization is prohibited.
- Sending, posting, recording or encouraging receipt of messages or information that may be offensive or harassing because of their sexual, racist or religious content, is obscene or threatening, and/or is defamatory is prohibited.
- Creating unauthorized Intranet sites or pages or sharing of any copyrighted material is prohibited.
- No Individual may implement wireless technology without the review and approval of the OCIO. Only authorized IT staff may install a wireless access device to the Internal Network connection jack, port, PC, or other devices connected to the Internal Network.
- Use of the Internal Network to perform any malicious activity, including the deliberate spread software viruses, unsolicited email messages, or intentional installation of malicious software of any kind is strictly forbidden.
- Email messages are property of the State of Nebraska. Forwarding email messages containing State Information from a State of Nebraska email account to a personal email account is prohibited unless that activity is approved by the OCIO, SISO, or AISO.

8-202. Personnel Security

New Hires

New hires are required to attend Security and Privacy training within 30 days of receiving their credentials, and shall be prohibited from accessing Confidential or Restricted information until this training is complete.

Access shall be limited to the minimum necessary access required to perform assigned duties, and all personnel are required to read and understand this policy and their obligations in protecting State of Nebraska information.

Terminations

Accounts that have been inactive for 180 consecutive days will be disabled. Accounts that have been inactive for thirteen (13) months will be deleted. Activity logs and records related to all accounts shall be maintained for a minimum of five (5) years after the account is deleted. These logs and records will be classified as Restricted information and secured appropriately.

Temporary accounts for the Staff and Vendors will be terminated or renewed annually, and records will be kept on this activity. Records shall be maintained for five (5) years. Staff that has terminated employment will have their credentials disabled immediately, but no later than 24 hours of their departure.

Individual Accountability

Each user must understand his/her role and responsibilities regarding information security issues and protecting State information. Access to State of Nebraska computer(s), computer systems, and networks where the data owner(s) has authorized access, based upon the "Principle of Least Privilege", must be provided using individually assigned unique computer identifiers, known as UserIDs, or other technologies including biometrics, token cards, etc. Every individual is responsible for reasonably protecting against unauthorized activities performed with their UserID.

Associated with each UserID is an authentication token, such as a password or pin, which must be used to authenticate the person accessing the data, system or network. These authentication tokens or similar technology must be treated as confidential information, and must not be shared or disclosed.

Segregation of Duties

To reduce the risk of accidental or deliberate system misuse, separation of duties must be implemented where practical.

Whenever separation of duties is impractical, other compensatory controls such as monitoring of activities, increased auditing and management supervision must be implemented. At a minimum, the audit of security must remain independent and segregated from the security function.

8-203. Software Management

System Software

Access to operating system code, services and commands must be restricted to only those individuals necessary in the normal performance of their job responsibilities.

Shared accounts are prohibited for systems that store, process, or access Confidential or Restricted information.

Default administrator accounts must be renamed, removed or disabled. Default passwords for renamed or disabled default administrator accounts must be changed. Passwords are subject to periodic password change requirements.

OCIO shall maintain an accurate inventory of all system software, including licensing and usage information, used within the State of Nebraska infrastructure.

Changes to system software shall follow change management procedures as defined in 8-207.

Application Code

Access to source code libraries for both agency business applications and operating systems must 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.

All application source code shall be backed up and access restricted to authorized personnel only. Application changes are required to go through a SDLC process that ensures the confidentiality of information, and integrity/availability of source and executable code. Application changes shall follow Change Management processes as defined in 8-207.

8-204. Hardware Management

Computer assets must be physically protected from physical and environmental hazards to reduce the risk of unauthorized access to information and to protect against loss or damage. Special controls may be necessary for electrical supply and uninterruptible power, fire protection and suppression, air and humidity controls, and cabling infrastructure in data centers, wiring closets, server rooms, and storage facilities where computers and computer peripherals are stored.

Agencies are required to keep an inventory of all information technology hardware used within their environment. This inventory shall include specific details including:

- Network diagram of hardware location related to security protections
- Hardware Manufacturer
- Hardware Model Number
- Serial numbers
- Firmware Version (if applicable)
- Configuration settings and hardening requirements (for “sensitive” hardware)

Hardware changes shall follow Change Management processes as defined in 8-207.

8-205. Change Control Management

To protect information systems and services, a formal change management system must be established to enforce strict controls over changes to all information processing facilities, systems, software, or procedures. Agency management must formally authorize all changes before implementation and ensure that accurate documentation is maintained. These change control procedures will apply to

agency business applications as well as systems software used to maintain operating systems, network software, hardware changes, etc.

The change management process can differ between changes to IT infrastructure (which includes all hardware, system software, and network assets) and application software. (which includes commercial off the shelf data applications and in-house developed data application software). However, underlying requirements for managing change are the same. All IT infrastructure and application development changes are required to follow a change management process to ensure the change is approved for release and does not unknowingly add security risks to the State's environment. All changes to network perimeter protection devices should be included in the scope of Change Management.

IT Infrastructure - The following change management standards are required to be followed for all IT infrastructure.

1. The OCIO requires a change management process with assigned responsibilities to ensure all changes to hardware, system software, and network infrastructure are authorized. This process will include representation from the OCIO, Department IT, State Information Security Officer, and application development (when application changes impact or are impacted). This process must occur on a periodic basis with sufficient frequency to meet demands for changes to the environment.
2. All records, meetings, decisions, and rational of the Change Control group shall be documented and securely stored for audit purposes. The agenda for this meeting is flexible but should generally address a review of at least the following:
    A. Change summary, justification and timeline
    B. Functionality, Regression, Integrity, and Security Test plans and results
    C. Security review and impact analysis
    D. Documentation and baseline updates
    E. Implementation timeline and recovery plans
3. The OCIO or Agency is required to maintain baseline configuration documentation in use throughout the infrastructure. These baseline configuration documents shall be categorized as Confidential information, and secured appropriately. The baseline documents must be reviewed and updated on an annual basis or after any significant changes to the baseline have been installed.
4. All changes to the production infrastructure are required to be made by authorized personnel only, using access credentials assigned to that individual. Actions performed by these user credentials will be logged.
5. All ports, services, protocols, etc. on all technology that is not needed to support State business shall be disabled. This information shall be documented, and the State Information Security Officer will conduct a review of the environment on a periodic basis to ensure that only necessary and required ports, services, protocols, etc. remain enabled.

Application Development – The following change management standards are required to be followed for application software systems that create, process, or store Confidential or Restricted data.

1. Application change management processes shall be performed with assigned responsibilities to ensure all changes to appropriate OCIO or Agency application software are approved and documented. Change management teams will include appropriate

application development staff and appropriate staff to represent State Information Security requirements.

2. The change management processes may vary depending on the data application size and configuration, however all processes must include formal procedures with tools to support the documentation, review and approval for each change request.
3. The change management processes will retain a documented history of the change process as it passes through the SDLC with documentation securely stored for audit purposes. Documentation should address a review of the following:
    A. Change summary, justification, and timeline
    B. Functionality, Regression, Customer Acceptance, and Security Test plans
    C. Security review and impact analysis
    D. Documentation and baseline updates
    E. Implementation timeline and recovery plans
4. Changes to software applications must be controlled and production installations shall be made by personnel assigned to update production libraries. Mechanisms to maintain and ensure the integrity of the application code shall be implemented.
5. Changes to production libraries should not be the same personnel who made the application changes unless documented procedures are in place which ensure the confidentiality, integrity, and availability of the data maintained in the production library.
6. Application development changes that impact IT infrastructure must be submitted to the Infrastructure change management process for review, approval, and implementation coordination.

8-206. Identification Badges

Only authorized individuals are allowed to enter State of Nebraska facilities that contain sensitive information. Those individuals will be issued an electronic identification (ID) badge. All authorized individuals are required to scan their ID badge before entry into these sensitive facilities. ID badges must be visible always, and Staff are encouraged to question anyone they do not recognize who is not wearing a badge. Staff who forget their badges will be issued a temporary badge after Management approval. Temporary badges must be returned at the end of the day.

All Visitors are required to sign a visitor's log, including name, organization, signature, purpose of visit, date, time in, time out, and person to see. Visitors will be assigned a temporary badge that must be visible at all times. Visitors are not allowed into unsupervised areas such as data centers. If it is necessary for a Visitor to enter an unsupervised area, they must be escorted at all times. When exiting the facility, the Visitor must sign out and return the badge while under Staff supervision.

Access to certain secured areas requires additional approval. Access to secured IT areas, such as data centers and network closets, must be approved by the OCIO, and access to certain other secured areas must be approved by the SISO before access is allowed. All access to secured areas shall be electronically logged and monitored, and any temporary access to these areas must include an authorized escort.

8-207. Operational and Functional Responsibilities

Agencies that create, use or maintain information systems for the State of Nebraska must create and maintain an information security program that ensures the confidentiality, availability, integrity, of the State's information assets.

All information processing facilities must have detailed documented operating instructions, management processes and formal incident management procedures authorized by agency management and protected from unauthorized access. Where an agency provides a server, application or network services to another agency, operational and management responsibilities must be coordinated by both agencies.

Agency Accountability

All agency information must be protected from unauthorized access to help ensure the information's confidentiality and privacy while maintaining its integrity and availability. As with other assets, not all information has the same use or value, and therefore information requires different levels of protection. Each agency will follow established data classification processes as defined in **Data Classification** (see Policy 8-900). All information will be classified and managed based on its level of sensitivity.

Including Security in Job Responsibilities

Specific security roles and responsibilities for those individuals responsible for information security must be documented. Each Agency will have an individual assigned to ensure all security policies and procedures are implemented and managed within that Agency, and meet all State of Nebraska Information Security Policies and Procedures.

8-208. Right to Monitor and Record

Consistent with applicable law, employee contracts, and agency policies, the OCIO reserves the right to monitor, inspect, and/or search all State of Nebraska information systems at any time. Since agency computers and networks are provided for business purposes, staff shall have no expectation of privacy of the information stored in or sent through these information systems. The OCIO additionally retains the right to remove from agency information systems any unauthorized material.

Monitoring System Access and Use

Activities of information systems and services must be monitored and events logged to provide a historical account of security related events. Agencies will implement appropriate audit logs to record events, exceptions and other security-relevant events. The Agency Information Security Officer or designee will regularly review logs for abuses and anomalies. Logs will be kept consistent with Record Retention schedules developed in cooperation with the State Records Administrator and agency requirements to assist in investigations and access control monitoring.

Only individuals with proper authorization from the OCIO will be permitted to use "sniffers" or similar technology on the network to monitor operational data and security events on the State network. Network connection ports should be monitored for unknown devices and unauthorized connections.

8-209. Mobile Computing Devices and Portable Media

Portable Devices

All portable computing devices (e.g. notebooks, USB flash drives, PDA's, laptops and mobile phones) and information must be secured to prevent compromise of confidentiality or integrity. No device may store or transmit confidential or restricted information without approved encryption enabled on the device or other suitable protective measures that are approved by the agency data owner(s) and the State Information Security Officer.

Special care must be taken to ensure that information stored on the device is not compromised. Appropriate safeguards must be in place for the physical protection, access control, cryptographic technique, back up, virus protection, and proper connection to the State network. All mobile devices must utilize the screen locking feature on their device when not in use and after 15 minutes of inactivity.

Devices storing sensitive and/or critical information must not be left unattended and, where possible, must be physically locked away, or utilize special locks to secure the equipment.

Employees in the possession of portable devices must not check these devices in airline luggage systems. These devices must remain in the possession of the traveler as hand luggage unless restricted by Federal or State authorities.

All mobile computing devices containing or accessing Confidential or Restricted Information must be provisioned to meet these security policies and be approved by the OCIO and SISO. All devices that will be connected to the network must be logged with device type and approval date.

8-210. Multi Function Devices (MFD)

All MFDs used to process, store, or transmit data shall be approved by the SISO or AISO. They shall be configured and managed to adequately protect sensitive information.

Configuration and management of MFDs shall include minimum necessary access to the processing, storing, or transmitting function of the MFD. All unnecessary network protocols and services shall be disabled. Access controls shall be in place, and administrator privileges shall be controlled and monitored. Access to the internal storage of the MFD will be physically controlled, and those storage devices shall be securely disposed or cleansed when no longer needed. Software and firmware of the MFD shall be updated to the latest version supported by the Vendor. All Confidential or Privileged Information shall be encrypted in transit when moving across a WAN as well as when stored on the internal storage unit of the device. If the MFD stores information and is not capable of encrypting internal storage, then it must be physically secured or not used for Confidential or Restricted information. Encryption technology must be approved by the SISO or AISO.

Auditing and logging of MFDs shall be enabled. This includes creating and securing logs on the MFD and its print spoolers, auditing of user access and fax logs (if fax is enabled), and review of audit logs by authorized personnel.

8-211. Email, Messaging, and Communication

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 state E-mail system are ~~a~~ visible

representatives of the state and must use the system in a legal, professional and responsible manner. An account holder, user, or administrator of the State email system must not set up rules, or use any other methodology, to automatically forward emails to a personal or other account outside of the State of Nebraska network.

Email containing Confidential or Restricted information may not be sent to an account outside of the State of Nebraska network unless the contents of that email are encrypted.

Telephones and Fax Equipment

Communication outside the state telephone system for business reasons is sometimes necessary, but it can create security exposures. Employees should take care that they are not overheard when discussing sensitive or confidential matters; avoid use of any wireless or cellular phones when discussing sensitive or confidential information; and avoid leaving sensitive or confidential messages on voicemail systems.

Modem Usage

Connecting modems to computer systems on the state network is prohibited unless a risk assessment is performed, risks are appropriately mitigated, and the Office of the Chief Information Officer approves the request.

8-212. Printed Material

Regardless of its form, electronic or printed, all Information shall be classified and secured with controls that are commensurate with its classification. It is required to maintain two barriers to access any printed material containing Confidential or Restricted information always. Barriers to access include, but are not limited to:

- Physical presence and observation by trusted personnel
- Locked file cabinets or drawers
- Locked office
- Locked trunk of a car
- The secured State campus and locked facilities
- Video surveillance with motion sensor and alerting
- Sealed envelope

Unattended Confidential or Restricted information shall be secured, even when located in a secured facility.

8-213. Physical Security Requirements for system facilities

To detect and prevent unauthorized access attempts in areas within facilities that house sensitive or confidential information, where possible, agencies must utilize physical access controls designed to permit access by authorized users only that identify, authenticate and monitor all access attempts to restricted areas within agency facilities.

Agencies will perform a periodic threat and risk assessment to determine the security risks to facilities that contain State information, and implement reasonable and appropriate physical security measures to prevent and detect unauthorized access, theft, damage or interference.

Based on the threat and risk assessment, a multi-layered physical security perimeter must be established in agency environments where information or information assets are stored or where operational data centers, network wiring closets, or telephony connection equipment exists, or where

printers that print confidential or restricted information are used, and any other location where information may be in use or stored, such as file cabinets, microfiche storage areas, etc. The security layers create a perimeter that would require multiple methods of access control to gain entry. These layers could be in the form of an entry point with card key access, a staffed reception area, a locked cabinet or office, or another physical barrier. Confidential or Restricted information must maintain at least two barriers to access at all times.

8-214. State and Agency Security Planning and Reporting

It is the Policy of the State of Nebraska that the Information Security Program includes oversight and reporting as defined by these standards. The purpose of the Nebraska Information Security Reporting Policy and Procedures is to provide the State and Agency leadership with appropriate information in a consistent format to support their information security planning, fact-based decision making and allocation of future funding. Consistent reporting standards will also help to ensure that information security controls are consistent across the State of Nebraska's Information Technology infrastructure, meet all necessary regulations and requirements, and are appropriate for the level of risks facing the State and various Agencies. Formal reporting helps keep the information security mission consistent, well understood and continually progressing as planned.

Required Reports and Standards:

The following standard and recurring reports are required to be produced by the SISO and each AISO:

1. Information Security Strategic Plan for the State/Agency
2. System Security Plan(s)
3. Plan of Actions and Milestones (POA&M)

These reports will reflect the current and planned state of information security at the Department.

A. <u>Information Security Strategic Plan</u>

Proper risk-based planning is critical to ensure the most appropriate projects are prioritized and funded by the State and its Agencies. Information Security planning is no exception. Planning for information protection will be given the same level of executive scrutiny at the State as planning for information technology changes. This plan shall be updated and published on an annual basis, and should include a 5-year projection of key security business drivers, planned security infrastructure implementation and forecasted costs. It should include an educated view of emerging threats and protections, and an analysis of the potential impacts to State/Agency information assets. This plan is necessary to ensure that information security is viewed as a strategic priority, and is included as part of the overall State of Nebraska planning process.

<u>Contents of the Information Security Strategic Plan:</u>

1. Summary of the information security, mission, scope, and guiding principles

2. Analysis of the current and planned technology and infrastructure design for the State/Agency, and the corresponding changes required for Information Security to stay aligned with these plans.
3. Summary of the overall State/Agency Information Risks Assessments and current risk levels. Detailed descriptions of significant security risks, and plans to mitigate or remediate those risks.
4. Assessment of the current information security posture related to the future targeted posture, identified gaps, and high-level timeline necessary to close or mitigate those gaps.
5. Summary of the Policies, Standards, and Procedures for State/Agency Information Security, and projected changes necessary to stay current and relevant.
6. Summary of the Information Security Education and Awareness Program, progress, and timeline of events.
7. Summary of Disaster Recovery and Business Continuity activity and plans.
8. Analysis of the regulatory and contractual compliance environment, including potential new regulations or pending contractual requirements that will affect State/Agency Information Security.
9. Proposed five-year timeline of events and key deliverables or milestones
10. Line item cost projections for all information security activity is itemized by:
    a. Steady State Investments: The costs for current care and maintenance of the information security program.
    b. Risk Management and Mitigation: The line item expenses necessary to mitigate or resolve security risks for the Agency in a prioritized order.
    c. Future Technology: The line item forecasted expenses and timelines necessary to support emerging or changing technology, and to be ready for new and emerging threats to State/Agency information.
    d. Regulatory: The line item expense necessary to meet all regulatory and contractual compliance requirements.

B. <u>System Security Plan</u>

State and Agency information assets have become increasingly more difficult to protect due to advances in technology such as easy-to-use high-level query languages, the use of personal computers, the accelerating use of the Internet and other networks, as well as universal familiarity with data processing. Because new technology is too often adopted before protective measures are developed, these factors have resulted in increased vulnerability of information and information systems. Without a corresponding growth in good information security practices, such advances could result in a higher likelihood of inadvertent or deliberate corruption of State information assets and even the loss of the public's trust in the State of Nebraska information integrity and credibility.

The State and Agency *System Security Plan (SSP)* provides an overview of the security requirements of the information system including all State/Agency in-house or commercially developed and maintained systems and installations and to all external business partner systems and installations operated by, or on behalf of the State. The SSP describes the controls in place or planned for meeting those requirements and delineates responsibilities and expected behavior of all individuals who access the system. The SSP will address all Control Areas identified in the NIST 800-53 control framework, and shall describe the current controls in place to protect information at a level commensurate with the sensitivity level of the system.

The State Information Security Officer will work with each AISO to maintain an SSP incorporating each identified system managing information or used to process Agency business.

The AISO and the SISO are required to develop or update the SSP in response to each of the following events:

- New system
- Major system modification
- Increase in security risks / exposure
- Increase of overall system security level
- Serious security violation(s)
- Every three years (minimum) for an operational system

Contents of the System Security Plan:

1. System name and title, description and scope of system including each all in-house or commercially developed system and installations included in the SSP.
2. Responsible organization: Name and contact information for business area responsible for the systems defined in the SSP. Decision authority for business functionality and business risks.
3. Key Contacts: Name and contact information for personnel who can address system characteristics and operation. IT maintenance personnel for the system, applications, and infrastructure.
4. System operation status and description of the Business Process, including a description of the function and purpose of the systems included in the SSP.
5. System information and inventory, including a description or diagram of system inputs, processing, and outputs. Describe information flow and how information is handled. Include the information classification for all information processed, accessed, or exposed. Include a system network and workflow diagram.
6. A detailed diagram showing the flow of sensitive information, including Confidential and Restricted information. Describe details where this data is stored, accessed, or processed and include details of the security mechanisms applicable to this type of data.

7. Detailed information security descriptions, procedures, protocols, and/or implemented controls for all NIST 800-53 control areas within the scope of the system. Identify compensating controls or compliance gaps within this section of the SSP.
8. System interconnection or information sharing: Describe all interfacing or connections between two or more systems or business partners.
9. Applicable laws, regulations, or compliance requirements - list any laws, regulations, or specific standards, guidelines that specify requirements for the Confidentiality, Integrity, or Availability of information in the system.
10. Review of security controls and assessment results that have been conducted within the past three years.
11. Information Security Risk Assessment which includes identification of potential threat/vulnerabilities in the information system, analysis of planned or actual security controls, and potential impacts on operations, assets, or individuals.

C. Plan of Action and Milestones Report (POA&M)

The POA&M is a reporting tool that outlines weaknesses and delineates the tasks necessary to mitigate them. The State/Agency Information Security POA&M process will be used to facilitate the remediation of Information Security and system-level weaknesses, and will provide a means for:

- Planning and monitoring corrective actions
- Defining roles, responsibilities, and accountabilities for weakness resolution
- Assisting in identifying the security funding requirements necessary to mitigate weaknesses
- Tracking and prioritizing resources
- Ensuring appropriate progress and priorities are continually addressed
- Informing decision makers

The POA&M process provides significant benefits to the State of Nebraska. It is a dynamic management tool useful for ongoing efforts to address programmatic and system-specific vulnerabilities. It assists in essential decision-making activities, facilitating and helping to ensure the oversight and mitigation of security weaknesses and the cost-effective use of mitigation resources. To function effectively, a POA&M must be continually monitored and diligently updated. The SISO and AISOs are responsible for maintaining the POA&M and for providing quarterly updates to the State/Agency Leadership team.

Contents of the Information Security Plan of Action with Milestones:

- Source – Identifies the audit, review, event or procedure which identified this action item
- ID – Identification tracking number of this action item which can be tied to the source and timeframe of identification
- Project/Task – Defines the project, task objective and goals of the action item
- Key Content and Description – Narrative describing the key elements of the action item
- Key Milestones – Lists each measurable activity required to complete the action item
- Milestone Status – Lists the status of each milestone (Open, Completed, Closed Assigned, In Progress)
- Target or Completion Date – Expected date each milestone will be completed. The Department should also accommodate approved changes to target dates in a manner that reflects the new date while keeping record of the original due date.
- Responsible Party – List of individuals or support unit assigned to address the action item

ARTICLE 3

ACCESS CONTROL

8-301. Remote Access Standard

It is the responsibility of all State of Nebraska agencies to strictly control remote access from any device that connects from outside of the State of Nebraska network to a desktop, server or network device inside the State of Nebraska network and ensure that employees, contractors, vendors and any other agent granted remote access privileges to any State of Nebraska network utilize only approved secure remote access tools and procedures.

Purpose and Objectives

As employees and organizations utilize remote connectivity to the State of Nebraska networks, security becomes increasingly important. Accompanying and contributing to this trend is the explosive growth in the popularity of broadband connections and other technologies for remote access. These standards are designed to minimize the potential exposure from damages which may result from unauthorized use of resources; which include loss of sensitive or confidential data, intellectual property, damage to public image or damage to critical internal systems, etc. The purpose of this document is to define standards for connecting to any State of Nebraska agency from any host.

Objectives include:

- Provide requirements to State of Nebraska agencies for employees, contractors, vendors and any other agent that requests remote access to any State of Nebraska network.
- Provide a high level of security that uses standardized technology and remains adaptable in the face of changing technology products.
- Ensure a solution that is scalable to meet the current and future needs of state agencies, their employees, clients and customers, and business partners.
- Meet federal security requirements for remote access control.

Remote Access Standards and Requirements

The following standards apply to all Workforce (employees and contractors) that connect to State of Nebraska IT assets through the Internet. This includes all approved work-from-home arrangements requiring access to State systems and Agency office locations that use the Internet to access the State of Nebraska network. Each state agency will be responsible for ensuring that remote access to State resources is secured and compliant with this Policy.

External access from a personally owned computer or a computer not owned, maintained, or approved by OCIO is prohibited from accessing any State of Nebraska network resources that store, process, or access Confidential or Highly Restricted information. Exceptions must be approved in advance by the AISO, OCIO and the SISO. All remote access must occur via an OCIO or Agency authorized and configured remote access connection. Remote access for Staff must have prior authorization by and be requested by their

Supervisor or Division Management. No classified information other than Public information may be stored on a personal device. These requirements do not apply to remote access to web applications or systems intended for public access.

1. Staff approved for remote connectivity are required to comply with all policies and standards, and are required to have approval from AISO and the SISO. Staff are prohibited from using such equipment for private or inappropriate purposes as defined in State and Agency Acceptable Use Policies.
2. It is the responsibility of all Staff with remote access privileges to the State of Nebraska network to ensure that their remote access work environment is given the same security consideration as the user's on-site connection to the State network. All personal devices connecting to the network must have up to date anti-virus protection, active firewalls, and appropriate security patch levels equivalent to those provided for State equipment. This monitoring shall ensure the remote computer is free from Spyware, Adware, rootkits, or any other threats that would place State resources in jeopardy.
3. Staff shall use State provided or approved equipment and software for authorized activities only.
4. All remote access sessions shall be logged. OCIO, or the Agency IT Team shall perform periodic monitoring of the remote access session and random inspection of the user security settings and protocols to ensure compliance with policy and standards.
5. All remotely accessible information systems containing Confidential or Restricted data must employ mechanisms to ensure Personally Identifiable Information (PII), or other sensitive information cannot be downloaded or remotely stored.
6. Remote access to Confidential or Restricted information, unless explicitly approved by the SISO and/or AISO, is prohibited.
7. All State owned or managed portable devices that have the ability to store Confidential or ~~Highly~~ Restricted information must be password protected and full-disk encrypted using approved technology. Encryption technology will be provided or approved by the OCIO and should be FIPS 140-2 compliant.
8. Remote sessions that store, process, or access Confidential or Highly Restricted information or systems must use access control credentials and an approved form of multi-factor authentication before connecting to the State network. Remote sessions must employ OCIO approved cryptography during the entire session when connected to the State network.
9. Staff with remote access privileges to the State network must only use their assigned State @nebraska.gov email account to conduct State of business. Use of personal email accounts such as Hotmail, Yahoo, Gmail or other external resources to conduct official business will be considered an unauthorized disclosure and may result in a disciplinary action.
10. Remote access logon failures shall be logged. Credentials shall be disabled after three (3) consecutive failed login attempts.
11. Remote sessions shall be locked after 15 minutes of inactivity until the user re-establishes access with the appropriate credentials and authentication procedures.

12. At no time, should any State employee or contractor provide their login or email password to anyone, not even family members.
13. Nebraska workforce with remote access privileges must ensure that their computer which is remotely connected to the State network, is not connected to any other network at the same time, except for personal networks that are under the complete control of the user.
14. OCIO will authorize, document, and monitor all remote access capabilities and connections used on the system. The SISO and AISO are required to approve all remote access requests.
15. The SISO and or AISO will provide annual training for all staff authorized for remote access to the State network. This training shall include details on remote work location security, protection of mobile devices, and incident identification and reporting.

Remote Access from Non-State Owned and/or Managed Devices, when approved

Remote access from devices not owned, controlled or managed by the OCIO or Agency IT department must be approved by the OCIO or Agency before accessing State of Nebraska networks.All Remote Access Users must sign and renew annually an agreement with the State and/or Agency which addresses at a minimum the following:

- Remote access users are responsible for all actions incurred during their session in accordance with all State of Nebraska and agency standards and policies.
- All home networks connected to the Internet via a broadband connection should have a firewall installed, updated and operational.
- Web browsers settings should be selected or disabled as appropriate to increase security and limit vulnerability to intrusion.
- Operating systems should contain the most current security patches.
- All home computers must contain an Anti-Virus program with current signatures and that the computer is free from Spyware, Adware, and rootkits.
- Devices must have “split tunneling” disabled, which prevents unauthorized connections to the State network.
- Remote access to Confidential or Restricted information is prohibited on these devices, unless approval is granted by the Office of the CIO.

8-302. Minimum Password Configuration

A. Password Requirements

The following are the minimum password requirements for State of Nebraska passwords:

- Must contain a minimum Eight (8) characters
- Must contain at least Three (3) of the following Four (4):
- At least One (1) uppercase character
- At least One (1) lowercase character
- At least One (1) numeric character

- At least One (1) symbol (!@#$%^&)
- Cannot repeat any of the passwords used during the previous 365 days.

In addition to the Minimum Password Complexity outlined above, additional password requirements are necessary for differing levels of data classification when authenticating users to networks or applications. The highest data classification level that a user has access to during an authenticated session will determine the additional password requirements. All employees and contractors of the State of Nebraska shall use a password that follows at least a confidential level of authentication when logging into a state network or application.

B. Additional Access Requirements for Restricted Information

Information that is deemed Restricted requires the highest level of security. This includes Root/Admin level system information accessed by Privileged accounts. A password used to access Restricted information must follow the password complexity rules outlined in 8-303 (A), and must contain the following additional requirements:

- Multi-factor authentication
- Expire after 60 days
- Minimum Password Age set to 15 days
- Accounts will automatically be disabled after three unsuccessful password attempts

C. Additional Access Requirements for Confidential Information

Information that is deemed Confidential requires a high level of security. A password used to access Confidential information must follow the password complexity rules outlined in 8-303 (A) and must contain the following additional requirement:

- Expire after 90 days
- Accounts will automatically lock after three consecutive unsuccessful password attempts

D. Password Requirements for Managed Access Public Information

Information that is deemed Managed Access Public requires minimal level of security and need not comply with section 8-303 (A). of this policy. Typically, this data would not include personal information but may carry special regulations related to its use or dissemination. Managed Access Public data may also be data that is sold as a product or service to users that have subscribed to a service.

E. Password Requirements for Accessing Public Information

Information that is deemed Public requires no additional password security and need not comply with section 8-303 (A) of this policy.

F. Non-Expiring Passwords

Non-expiring passwords require a unique high level of security. Typically this information is confidential in nature and must follow the requirements in 8-303 (A). The additional requirements for access to Confidential or Highly Restricted Information data with a non-expiring password are:

- Extended password length to 10 characters
- Independent Remote Identity Proofing may be required

- Personal security question may be asked
- Multi-factor authentication
- Any feature not included on this list may also be utilized upon approval of the State Information Security Officer or upon enactment of federal, state or departmental laws, policies or directives.

G. Automated System Accounts

Examples of automated system accounts include those that act as an intermediary between the public user and state systems, internal system to system interfaces, perform backups or run batch jobs. System account passwords shall expire after 365 days, unless mechanisms to restrict the use of those credentials to just the authorized service can be implemented and approval is granted by the State Information Security Officer.

H. Multi-user Computers

Multi-user computers include those computers in kiosks or training labs, where users have limited or restricted access to state resources. Agencies may use non-expiring passwords on multi-user computers.. In these cases, mechanisms to ensure the user account with non-expiring passwords is unable to access Confidential or Highly Restricted information.

I. System Equipment/Devices

Agencies may use non-expiring passwords for system equipment/devices. It is common for many devices (e.g. IP cameras, HVAC controls) in today's IT environment to utilize login capabilities to protect the device from unauthorized access. While many of these devices make use of a user ID and password in a manner like those found while authenticating a user, the distinction to be made is that the User ID is used to authenticate the device itself to the system and not a person.

8-303. Identification and Authorization

All Workforce authorized to access any State of Nebraska Information or IT Resources, that have the potential to process, store, or access non-public information, must be assigned a unique identification (ID) with the minimum necessary access required to perform their duties. The Workforce is responsible ~~for,~~ and can be held accountable for, the actions conducted with their user ID and are required to secure their IDs from unauthorized use. It is the responsibility of Management to ensure that only minimum necessary access is provided within their department. Each user requiring access to the State network, with the potential to process, store, or access non-Public information, has an individual user ID issued to them.

8-304. Privilege Access Accounts

Privileged Accounts include administrator accounts, embedded accounts used by one system to connect to another, and accounts used to run service programs. These accounts are used by systems and personnel to access sensitive files, execute software, load and configure policies and configuration settings, and set up or maintain accounts.

Due to the elevated access levels these accounts typically have, the State of Nebraska requires the following standards and procedures to be followed to minimize the risk of incidents caused by these accounts:

- Default system account credentials for hardware and software must be either disabled, or the password shall be changed immediately. Use of anonymous accounts is prohibited, and

unassigned accounts must be assigned to an individual prior to use. When no longer needed, the account shall be disabled and password changed. At all times, the State requires individual accountability for use of privilege accounts.

- Accounts with privileged access will have enhanced activity logging enabled, pursuant to *8-708 Audit Requirements*. The OCIO and all applicable Agencies will perform a quarterly review of privileged access account activity;
- All privileged access accounts must be assigned to an individual with an approved business need for the privileged access. These accounts will not be shared.
- Privileged access through remote channels will be allowed for authorized purposes only and must include Multi-Factor Authentication.
- Passwords for these accounts must be changed every 60 days;
- The password change process shall support recovery of managed systems from backup media. Historical passwords should remain accessible in a history table in the event that they are needed to activate a backup copy of a system; and,
- Requests for privileged access accounts must include approval from the OCIO and must be provisioned and maintained by the OCIO.

8-**305. Account Termination**

Accounts that have been inactive for 45 consecutive days will be disabled. Accounts that have been inactive for thirteen (13) months will be deleted. Activity logs and records related to all accounts shall be maintained for a minimum of five (5) years after the account is deleted. These logs and records will be classified as Privileged information and secured appropriately. Deleted accounts will not be reused. Temporary accounts for the Workforce and Vendors will be terminated or renewed annually, and records will be kept on this activity. Records shall be maintained for five (5) years. Staff that has terminated employment will have their credentials disabled immediately, but no later than 24 hours of their departure.

ARTICLE 4

NETWORK SECURITY

The OCIO and agencies will implement a range of network controls to ensure the confidentiality, integrity, and availability of the data flowing across its trusted, internal network, and ensure the protection of connected services and networks. The OCIO ensures that measures are in place to mitigate security risks created by connecting the state network to a third party network. All direct connections to the State network and direct connections between agencies must be authorized by the Office of the Chief Information Officer.

Where an agency has outsourced a server or application to a third party service (such as a web application), the agency must perform or have performed a security review of the outsourced environment to ensure the confidentiality, integrity, and availability of the state's information and application is maintained. For applications hosted by Nebraska.gov, the Nebraska State Records Board or designee will perform the security review on behalf of all Agencies.

Additions or changes to network configurations, including through the use of third party service providers, must be reviewed and approved through the OCIO change management process.

8-401. Network Documentation

The State of Nebraska encourages the use of its electronic communications infrastructure in support of its mission. However, this infrastructure must be well-managed and protected to ensure the security of Agency information. Therefore, all network devices that access the State of Nebraska internal network are required to adhere to these standards.

All publicly accessible devices attached to the State network must be registered and documented in the IT Inventory system. Publicly accessible devices must reside in the OCIO DeMilitarized Zone (DMZ) unless approved by the OCIO for legitimate business purposes.

8-402. Network Transmission Security

1 All encryption must be approved by the OCIO or SISO. Any transmissions over unsecured networks (such as the Internet) that contain Confidential or Highly Restricted information must be encrypted using technology that is FIPS 140-2 Compliant, or approved by the SISO.

2 Network scanning and monitoring is prohibited, unless prior approval is obtained by OCIO or IT management. If approved, scanning must be restricted to authorized and registered IP addresses only, and conducted by authorized personnel only.

3 OCIO shall ensure that all networks and systems are monitored 24x7 with authorized tools (such as Network Based Intrusion Detection and Prevention Systems) and personnel to detect system anomalies or security events.

4 Passwords and SNMP community names may not be sent in clear text over open networks. All devices must use IT authorized encryption for access authorization to the internal network. Access to the DMZ applications is exempt from this requirement.

8-403. Network Architecture Requirements

1 All devices that store, access, or process Confidential or Highly Restricted information shall not reside in the public tier, and must be protected by at least two firewalls. Firewalls shall be placed at perimeter locations so that all critical systems are protected by multiple firewalls and monitoring systems.

2 All publicly accessible devices must be located in an access-controlled environment, and access credentials must be managed by authorized personnel.

3 All network devices that contain or process Confidential or Restricted data must be secured with a password-protected screen saver that automatically locks the session after 15 minutes of inactivity.

4 Devices that include native host-based firewall software in the operating system shall have the firewall activated and properly configured, unless the active firewall software compromises the usability of critical applications, or lessens the posture of other security systems.

5 The State of Nebraska network shall have an annual verification of all open ports, protocols, and services for publicly accessible systems. Any requests for public IP addresses or for additional open ports must be approved by the SISO.

6 Staff will follow approved change control and configuration management procedures for Network devices. Patches and hot-fixes recommended by network hardware or software vendors must be installed as soon as practical after testing.

7 Services and applications that will not be used must be disabled or removed if such action will not negatively impact operations. Protocols such as telnet, VNC, RDP, or others that do not actively support approved encryption should only be used if they are performed over a secondary encryption channel, such as SSL or IPSEC.

8-404. External Connections

Direct connections between the State network and external networks must be implemented in accordance with these policies and standards. Connections will be allowed only when external networks have been reviewed and found to have acceptable security controls and procedures, or appropriate security measures have been implemented to protect state resources. A risk analysis should be performed to ensure that the connection to the external network would not compromise the state's private network. Additional controls, such as the establishment of firewalls and a DMZ may be implemented between any third party and the state. All external connections will be reviewed on an annual basis.

Third party network and/or workstation connection(s) to the state network must have an agency sponsor and a business need for the network connection. An agency non-disclosure agreement may be required to be signed by a legally authorized representative from the third-party organization. In addition to the agreement, the third party's equipment must also conform to the state's security policies and standards, and be approved for connection by the OCIO.

Any connection between agency firewalls over public networks that involves sensitive information must use encryption to ensure the confidentiality and integrity of the data passing over the external network.

8-405. Wireless Networks

Advances in wireless technology and pervasive devices create opportunities for new and innovative business solutions. However, security risks - if not addressed correctly, could expose state information systems to a loss of service or compromise of sensitive information. Everything transmitted over radio waves (wireless devices) can be intercepted. This represents a potential security issue. Agencies shall take appropriate steps, including the implementation of encryption, user authentication, and virus protection measures, to mitigate risks to the security of State data and information systems associated with the use of wireless network access technologies.

No wireless network or wireless access point will be installed without the written approval of the OCIO.

All wireless networks shall be inspected annually by the SISO and AISO to ensure proper security protocols are in place and operational.

ARTICLE 5

SYSTEM SECURITY

8-501. System Documentation

Only OCIO approved hardware or software is permitted within the State of Nebraska infrastructure and on state-owned devices. Personal devices (e.g. smart phones, tablets, laptops etc.) that connect to the Internal Network for email, must use the State of Nebraska provided interface on that device for this access. Requests for additional software must be submitted as directed by the OCIO. Personal software is not allowed on any state-owned equipment.

1. Documentation of key systems within the State of Nebraska will be maintained and secured as Proprietary information.
2. Staff are prohibited from downloading or installing software on state owned equipment unless this activity is approved as part of work assignment and authorized by the OCIO.
3. The State will create and maintain an inventory of all approved hardware and software that can be connected to the Internal Network. All other devices must be approved and recorded by the OCIO before being connected to the Internal Network. The SISO will perform regular monitoring and tracking to ensure that only approved hardware and software exist within the State of Nebraska environment.
4. All authorized hardware and software shall be inventoried, and documented. Results shall be secured in an auditable fashion.

8-502. Minimum User Account Configuration

User accounts shall be provisioned with the minimum necessary access required to perform duties. Accounts shall not be shared, and users must guard their credentials.

Administrator level access is ~~a~~ privileged and shall be restricted to authorized IT personnel only. All privileged access accounts are subject to additional security, including multi-factor authentication and enhanced auditing/logging of activity.

Local accounts shall be disabled unless required for business purposes, and in those cases, use of these accounts must be approved, tightly controlled and monitored. All use of local accounts are required to be associated with an individual user.

8-504. Minimum Server Configuration and Patch Management

The State of Nebraska recognizes the National Institute of Standards and Technology (NIST) as the adopted author of recommended security requirements that provide minimum baselines of security for servers on the State of Nebraska network.

NIST provides instructions, recommendations, and considerations to assist readers in deploying servers in a secure method. All State of Nebraska System Administrators should examine NIST documents when installing and or configuring servers. The documents are not all inclusive, but rather meant as a means of prompting and guiding Administrators through the installation process.

Purpose and Objectives

Information technology (IT) is a vital resource to the State of Nebraska; therefore, it is critical that services provided by these systems can operate effectively.

The purpose of this standard is to establish base configurations and minimum server standards on internal server equipment that is owned and/or operated by the State of Nebraska. Effective implementation of this policy will reduce the risk of unauthorized access and other IT security related events to the State of Nebraska's information and technology systems.

All state agencies, boards and commissions will comply with NIST standards, guidelines, and checklists as identified below.

- NIST 800-53, Security and Privacy Controls for Federal Information Systems and Organizations
- NIST SP 800-70, The NIST Security Configuration Checklists Program
- NIST SP 800-44, Guidelines on Securing Public Web Servers

Server Hardening

All servers that store, process, or have access to Confidential or Restricted dataare required to be hardened according to these standards. In addition, these servers shall have a published configuration management plan as defined below and approved by the State Information Security Officer.

1. Servers may not be connected to the State network until approved by Agency and OCIO Management. This approval will not be granted for sensitive servers until these hardening standards have been met or risk levels have been officially accepted by Agency Management.
2. The Operating System (OS) must be installed by IT authorized personnel only, and all vendor supplied OS patches must be applied. All software and hardware components should be currently supported. All unsupported hardware and software components must be identified and have a management plan that is approved by the State Information Security Officer.
3. All unnecessary software, system services, accounts and drivers must be removed unless doing so would have a negative impact on the server.
4. Logging of auditable events, as defined in NIST 800-53 control objectives, will be enabled. Audit logs will be secured and only accessible to accounts with privileged access.
5. Security parameters and file protection settings must be established, reviewed, and approved by the State Information Security Officer.
6. All system software must have security updates and patches applied when made available from the vendor. Priority setting of vulnerabilities will be based on impact to Department and as referenced in the National Vulnerability database (HTTP://nvd.nist.gov).
7. Hardened servers will be scanned monthly for unauthorized software or unauthorized changes to the configuration baselines.

8. Hardened servers will be monitored with active intrusion detection, intrusion protection, or end-point security monitoring that has been approved by the State Information Security Officer. This monitoring shall have the capability to alert IT administrative personnel within 1 hour.
9. Servers shall be loaded from standardized processes and software. These processes and software shall be appropriately configured and protected, with integrity controls to ensure only authorized and documented changes are possible.
10. All changes to hardened servers must go through a formal change management and testing process to ensure all the integrity and operability of all security and configuration settings remain intact. Significant changes must have a documented Security Impact Assessment included with the change.
11. Remote management of hardened servers shall be performed over secured channels only. Protocols such as telnet, VNC, RDP, or others that do not actively support approved encryption should only be used if they are performed over a secondary encryption channel, such as SSL or IPSEC.

8-505. Minimum Workstation Configuration

Improperly configured workstations are at risk to be compromised. Without proper adherence to these workstation security standards, the State is at increased risk to have data lost, stolen, or destroyed. This standard is necessary to protect the State from unauthorized data or activity residing or occurring on State equipment. It is also necessary to reduce the likelihood of malicious activity propagating throughout the State networks or launching other attacks. All managed workstations that connect to the State's network are required to meet these standards. The OCIO is responsible for maintaining these standards and for configuring and managing the hardware, software, and imaging processes for all managed workstations. orkstation standards should be securely maintained and stored in a centralized documentation library. In addition to adherence to the required images, the following standards are defined for all workstations that connect to the State network. The degree of protection of the workstation should be commensurate with the information classification of the resources stored, accessed, or processed from this computer.

1. Endpoint security (anti-virus) software, approved by the OCIO, must be installed and enabled.
2. The host-based firewall must be enabled if the workstation is removed from the State internal network.
3. The operating system must be configured to receive automated updates.
4. The system must be configured to enforce password complexity standards on accounts.
5. Application software should only be installed if there is an expectation that it will be used for State business purposes. Application software not in use should be uninstalled.
6. All application software must have security updates applied as defined by patch management standards.

7. Shared login accounts are prohibited unless approved in advance and configured by IT. Shared login accounts are only acceptable if approved through the policy exception process and alternate mechanisms or access layers exist to ensure the ability to individually identify personnel accessing non-public information.
8. Shared login accounts are forbidden on multi-user systems where the manipulation and storage of Confidential or Restricted information takes place.
9. Users need to lock their desktops when not in use. The system shall automatically lock a workstation after 5 minutes of inactivity.
10. Users are required to store all Confidential or Restricted information on IT managed servers, and not the local hard drive of the computer. Local storage can only be used for temporary purposes when the data stored is not sensitive, and where loss of the information will not have any detrimental impact on the State. All State laptops with the ability to store data must be fully encrypted using IT approved technology.
11. All workstations shall be re-imaged with standard load images prior to re-assignment.
12. Equipment scheduled for disposal or recycling shall be cleansed following Department media disposal guidelines

8-506. Minimum Laptop Configuration

All laptops that connect to the State of Nebraska network are required to meet these requirements. Each state agency will be responsible for ensuring that any device connected to State resources contain an operating Anti-Virus monitoring with current signatures and that the computer is free from Spyware, Adware, rootkits, or any other threats that would place State resources in jeopardy.

1. Remote access to Confidential or Restricted information must occur through a State-managed endpoint, using the State VPN or other connections that have been approved by the Office of the CIO.
2. Remote access to any privilege functions, such as administrator accounts, must employ multi-factor authentication and all activity shall be logged for audit purposes.
3. Remote access users are responsible for all actions incurred during their session in accordance with all State of Nebraska and agency standards and policies.
4. All home networks connected to the Internet via a broadband connection should have a firewall installed, updated and operational.
5. Web browsers settings should be selected or disabled as appropriate to increase security and limit vulnerability to intrusion.
6. Operating systems should contain the most current security patches.
7. All home computers must contain an Anti-Virus program with current signatures and that the computer is free from Spyware, Adware, and rootkits.
8. Laptops with remote access to, or the capability to store, Confidential or Restricted are required to be fully encrypted using technology approved by the SISO.

8-507. Minimum Mobile Device Configuration

The purchase and use of all mobile computing devices containing or accessing the State of Nebraska networks and information must be provisioned to meet these security policies and be approved by the OCIO. All devices that will be connected to the network must be logged with device type and approval date. Accessories used on corporate computers must be provided by IT or approved by the OCIO.

1. Mobile computing devices must be shut down or locked when not in use. These devices may not be left unattended in a public access area. They must be locked in a secure cabinet or room, or kept on the person. Devices may not be used by or shared with anyone.
2. Mobile computing devices and mobile storage devices must never be left in a vehicle unattended.
3. Storing Confidential or Restricted information on any mobile device or any removable or portable media (e.g. such as. CD's, thumb drives, DVD's, etc.) is prohibited unless arrangements and mechanisms for securing the data has been explicitly approved by the SISO. In those cases, all mobile computing devices or portable media shall be encrypted using technology that is approved by the SISO.
4. Personally owned mobile devices (e.g. such as smartphones and tablets) may be used for approved State purposes, including email, when configured to access the State of Nebraska Information through a managed interface or sandbox only. Devices that are not configured to use the authorized interface are prohibited from accessing any State information, including email.
5. It is required to lock or secure security settings so users cannot delete or change mandatory settings.
6. Strong passwords are required, and passwords must change regularly per State policy regarding passwords.
7. It is required that the device lock after 15 minutes of inactivity, and cannot be unlocked without the re-entry of a password or PIN code.
8. After 10 unsuccessful password attempts, the device or the State container will be erased. In the event that the device becomes lost or stolen, OCIO must have the capability to remotely locate, lock, and erase the device.
9. The device should have all data backed up at the State of Nebraska internal data center.
10. Devices need to be cleared of all information from the prior user before being issued to a new user.
11. The device OS must be up to date and patched. New versions of the OS must be vetted for security posture and supportability.
12. Devices are required to be properly disposed of using mechanisms approved by the SISO. State data needs to be cleared and devices properly disposed of or recycled. The disposition process is required to be documented and periodically audited.
13. New devices are required to be configured and operate within established security guidelines and help desk support must be established before these devices can be operational. New Devices need to be validated before being made available for users to request.

8-508. System Maintenance

1. All systems using third party software that is involved in the processing, storage, or access to any Confidential or Restricted information shall be maintained per manufacturer specifications. Maintenance personnel shall be approved for activity by the State Information Security Officer and shall be briefed on the requirements for protecting sensitive information.
2. Maintenance activity will be logged to include the date/time of the maintenance, activity performed, the person or organization who performed the maintenance, the name and department of the escort (if applicable), and a detailed list of any equipment removed or replaced during the maintenance. This list should include serial numbers, if applicable.
3. Prior to removing any equipment from any secured environment, the equipment will be approved for release and validated by the State Information Security Officer (or his designate) that all non-public information has been encrypted, secured, or permanently deleted from the equipment. When equipment is returned, it shall be inspected for unauthorized systems, settings, or services to ensure the integrity of the security systems before reloading data or placing back into the environment.
4. All tools used for maintenance shall be tested. The Office of the CIO and each Agency shall maintain a list of approved maintenance tools that is reviewed and updated annually, or when required.
5. Nonlocal or Remote maintenance must be approved in advance by the State Information Security Officer or the OCIO, and must also comply with all Agency and OCIO requirements for remote access.
6. All remote maintenance activity will be logged and reviewed.
7. Maintenance of agency-developed software must follow the State's change management process to ensure changes are authorized, tested and accepted by agency management. All known security patches must be reviewed, evaluated and appropriately prioritized.
8. Critical patches must be applied within 24 hours of receipt. High risk patches must be applied within 7 days of receipt. All other patches must be appropriately applied in a timely manner as defined by the Agency.
9. All third-party software deployed and operational within the State must be currently supported by the Vendor unless an exception has been requested and approved through the Policy Exception Process.

ARTICLE 6

APPLICATION SECURITY

8-601. System Documentation

To ensure that security is built into information systems, security requirements, including the need for rollback arrangements, must be identified during the requirements phase of a project and justified, agreed to, and documented as part of the overall business case for the system. To ensure this activity is performed, the Agency Information Security Officer or designee must be involved in all phases of the System Development Life Cycle (SDLC) from the requirements definition phase, through implementation and eventual application retirement.

Controls in systems and applications can be placed in many places and serve a variety of purposes. The specific control mechanisms must be documented at the application level, and included in the agency's security standards documents. The security measures that are implemented must be based on the threat, vulnerability, and risk assessments of the information being processed and cost/benefit analysis.

Significant changes involving systems that store, access, or process Confidential or Restricted information must go through a formal change management process. For recurring maintenance of these systems, an abbreviated change management process can suffice if that abbreviated process has been approved by the State Information Security Officer and the Office of the CIO.

8-602. Separation of Test and Production Environments

Development software and testing tools can cause serious problems to the production environment if separation of these environments does not exist. Separation of the development, test and production environments is required, either on physically separate machines or separated by access controlled domains or directories. Processes must be documented and implemented to govern the transfer of software from the development environment to the production platform. Each agency must consider the use of a quality assurance environment where user acceptance testing can be conducted. The following controls must be considered:

- Access to compilers, editors and other system utilities must be removed from production systems when not required; and
- Logon procedures and environmental identification must be sufficiently unique for production testing and development.
- Access to systems and business applications must be restricted to those individuals who have a business need to access those resources in the performance of their job responsibilities.
- It is recognized that at times, business or technical requirements dictate the need to test with live data. In those cases, it is mandatory to have approval from the State ISO, and to implement production-class controls in the applicable test environment to protect that information.

8-603. Application Development

The following standards are required to be followed for Department application software systems that create, process, or store Confidential and Restricted data.

1. The Agency will establish application change management processes with assigned responsibilities to ensure all changes to applicable application software are approved and documented. Change management teams will include appropriate application development staff and appropriate staff to represent State Information Security requirements.
2. The change management processes may vary depending on the data application size and configuration, however all processes must include formal procedures with tools to support the documentation, review and approval for each change request.
3. The change management processes will retain a documented history of the change process as it passes through the SDLC with documentation securely stored for audit purposes. Documentation should address a review of the following:
    a. Change summary, justification, and timeline
    b. Functionality, Regression, Integrity, and Security Test plans and results
    c. Security review and impact analysis
    d. Documentation and baseline updates
    e. Implementation timeline and recovery plans
4. Changes to software applications must be controlled and production installations shall be made by personnel assigned to update production libraries. Mechanisms to maintain and ensure the integrity of the application code shall be implemented.
5. Changes to production libraries should not be the same personnel who made the application changes unless documented procedures are in place which ensure the confidentiality, integrity, and availability of the data maintained in the production library.
6. Application development changes that impact Department IT infrastructure must be submitted to the Infrastructure Change Control Team for review, approval, and implementation
7. The security requirements of new systems must be established, documented and tested prior to their acceptance and use. Agency Information Security Officer or designee will ensure that acceptance criteria are utilized for new information systems and upgrades. Acceptance testing will be performed to ensure security requirements are met prior to the system being migrated to the production environment.
8. All applications are required to maintain up-to-date documentation that includes an assessment of security threats and impacts, and a detailed description of the data handling with its accurate classification.
9. Applications that provide user interfaces shall have an appropriate warning banner displayed, applicable to the data being accessed (e.g., PHI, FTI, PII, etc).
10. Application credentials, where possible, should be inherited from the State Managed Authentication Source. If that is not possible, credentials should have the same level of management and approval as other Agency access credentials.

11. Applications must be configured such that Confidential or Restricted data will be encrypted when transmitted outside the Department internal network.

Security Standards for Web Application and Services

Internet-facing systems are diverse to meet a multitude of different needs. Therefore, information exposures by these systems differ, as do threats. Security controls should be implemented to mitigate meaningful risks to an application. Because every system is different, the web application developer is the most knowledgeable about the system and the risks it faces.

This standard establishes a baseline of security requirements for all State websites, web services, and all third-party supported or hosted web applications. All applications that are Internet-facing are required to securely maintain documentation and evidence of compliance levels with this standard.

This standard is based on the research and recommendations from the SysAdmin, Audit, Network, and Security (SANS) Institute and the Open Web Application Security Project (OWASP).

1. Consider the threats, vulnerabilities, and risks to your application. If you are unsure, follow the Threat Risk methodology published by OWASP.

   http://www.owasp.org/index.php/Threat_Risk_Modeling

2. Consider and implement additional security controls to ensure the Confidentiality, Integrity, Availabilityof the information based on the unique threats and exposures that face your application.

3. Implement error-handling in a manner that denies processing on any failure or exception.

4. All input fields must be validated before accepting. Input should be checked to prevent the program from executing malicious code. Input length must be validated to determine if it is within the predetermined minimum and maximum ranges. Input values should be screened for valid data types (e.g., number or character only, no special characters).

5. Output fields must be sanitized to ensure the output does not reveal too much information that could be used by malicious intent (e.g., default system-generated messages should be translated by the application). If invalid user input is encountered, the error message should not reveal the specific component which caused the error. Messages should be general in nature, and not reveal anything more than what is necessary.
6. The identity of the user must be authenticated if the application has access to non-public information. All user credentials and passwords must meet the security policy requirements for strength, change, and history. User access and capability must be limited to the functions required for the authorized access level only.

7. The requesting and granting of user accounts must include an approval process that validates the user and the minimum necessary access levels.

8. Establish security settings commensurate with the type of access.

9. All external systems (including web services), which require access to the application, must be authenticated and permissions checked before the external system becomes trusted.
10. All password entry fields should not "echo" the password in readable text when it is entered. Auto-complete of password fields should be disabled.
11. All sessions should be terminated when the user logs out of the system.
12. If a web application needs to store temporary or session-related information that is Confidential or Restricted outside of the secured Department internal network, that information must be encrypted in all cases – whether stored or in transit. Encryption technology must be approved by OCIO.
13. All web applications are required to have a security scan and test of the application on a recurring basis as determined by the State ISO. Higher risk or impact applications should be tested annually. This test shall be coordinated and supervised by the SISO and ISO and IT management. Some packaged web applications where the package's architecture inherently protects the application from security risks, may have reduced testing requirements versus other web applications.
14. The anonymous public facing environment shall contain publicly approved content only. All non-public data and applications shall be segregated by additional firewalls and network monitoring.

Other application security recommendations and development guides can be reviewed at the OWASP or SANS websites:

https://www.owasp.org/index.php/Category:OWASP_Guide_Project

http://www.sans.org/top25-software-errors/

8-604. External Hosting of State Data and Cloud Security

Accessing online "cloud" storage websites such as Dropbox, Google Drive, etc., is a security risk that will be restricted based on an employee's job functions. Use of these systems for any State purposes is prohibited by unless approved by the employee's supervisor or manager. Even if approved, it is prohibited to process or store any Confidential or Restricted information with these services, unless the storage is encrypted with approved technology, and has been approved in advance by the SISO.

The following standard provides guidance on the acceptable use of cloud computing services by Nebraska state government agencies.

1. DEFINITIONS

The NIST Definition of Cloud Computing:

This standard incorporates the following definition from the National Institute of Standards and Technology (*The NIST Definition of Cloud Computing*, NIST Special Publication 800-145, September 2011 [footnotes omitted]):

Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage,

applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. This cloud model is composed of five essential characteristics, three service models, and four deployment models.

Essential Characteristics:

***On-demand self-service*.** A consumer can unilaterally provision computing capabilities, such as server time and network storage, as needed automatically without requiring human interaction with each service provider.

***Broad network access*.** Capabilities are available over the network and accessed through standard mechanisms that promote use by heterogeneous thin or thick client platforms (e.g., mobile phones, tablets, laptops, and workstations).

***Resource pooling*.** The provider's computing resources are pooled to serve multiple consumers using a multi-tenant model, with different physical and virtual resources dynamically assigned and reassigned according to consumer demand. There is a sense of location independence in that the customer generally has no control or knowledge over the exact location of the provided resources but may be able to specify location at a higher level of abstraction (e.g., country, state, or datacenter). Examples of resources include storage, processing, memory, and network bandwidth.

***Rapid elasticity*.** Capabilities can be elastically provisioned and released, in some cases automatically, to scale rapidly outward and inward commensurate with demand. To the consumer, the capabilities available for provisioning often appear to be unlimited and can be appropriated in any quantity at any time.

***Measured service*.** Cloud systems automatically control and optimize resource use by leveraging a metering capability at some level of abstraction appropriate to the type of service (e.g., storage, processing, bandwidth, and active user accounts). Resource usage can be monitored, controlled, and reported, providing transparency for both the provider and consumer of the utilized service.

Service Models:

***Software as a Service (SaaS)*.** The capability provided to the consumer is to use the provider's applications running on a cloud infrastructure. The applications are accessible from various client devices through either a thin client interface, such as a web browser (e.g., web-based email), or a program interface. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, storage, or even individual application capabilities, with the possible exception of limited user-specific application configuration settings.

***Platform as a Service (PaaS)*.** The capability provided to the consumer is to deploy onto the cloud infrastructure consumer-created or acquired applications created using programming languages, libraries, services, and tools supported by the provider. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, or storage, but has control over the deployed applications and possibly configuration settings for the application-hosting environment.

***Infrastructure as a Service (IaaS)*.** The capability provided to the consumer is to provision processing, storage, networks, and other fundamental computing resources where the consumer is able to deploy and run arbitrary software, which can include operating systems and applications. The consumer does not manage or control the underlying cloud infrastructure but has control over operating systems, storage, and deployed applications; and possibly limited control of select networking components (e.g., host firewalls).

Deployment Models:

***Private cloud*.** The cloud infrastructure is provisioned for exclusive use by a single organization comprised of multiple consumers (e.g., business units). It may be owned, managed, and operated by the organization, a third party, or some combination of them, and it may exist on or off premises.

***Community cloud*.** The cloud infrastructure is provisioned for exclusive use by a specific community of consumers from organizations that have shared concerns (e.g., mission, security requirements, policy, and compliance considerations). It may be owned, managed, and operated by one or more of the organizations in the community, a third party, or some combination of them, and it may exist on or off premises.

***Public cloud*.** The cloud infrastructure is provisioned for open use by the general public. It may be owned, managed, and operated by a business, academic, or government organization, or some combination of them. It exists on the premises of the cloud provider.

***Hybrid cloud*.** The cloud infrastructure is a composition of two or more distinct cloud infrastructures (private, community, or public) that remain unique entities, but are bound together by standardized or proprietary technology that enables data and application portability (e.g., cloud bursting for load balancing between clouds).

Other Deployment Models

Government community cloud. A community cloud infrastructure provisioned solely for use by federal, state, and/or local government.

State cloud. The private cloud infrastructure provided by the State of Nebraska, Office of the Chief Information Officer.

Other Definitions

Data classification. The data classification system created in the Information Security Policy (NITC 8-101, § 4.6).

2. STANDARD

The following table contains the acceptable uses of cloud computing by Nebraska state government agencies. The classification of the data to be processed or stored using cloud computing determines the acceptable options. If there is a mix of data classifications, the most restrictive data classification will be used.

Data Classification	Cloud Deployment Models					
	State Cloud	Private Cloud	Government Community Cloud	Community Cloud	Public Cloud	Hybrid Cloud
Restricted	✓	△	△	△	⊘	△
Confidential	✓	△	✓	△	⊘	△
Managed Access Public	✓	✓	✓	✓	✓	✓
Public	✓	✓	✓	✓	✓	✓

(✓) means an approved deployment model for cloud computing;
(⊘) means an unapproved deployment model for cloud computing; and
(△) means prior approval by the OCIO is required.

2.1 **Prior Approval Process**

An agency requesting prior approval of a cloud computing service must submit a Service Request to the OCIO Service Desk. The request should provide detailed information about the cloud deployment model and data to be processed or stored using cloud computing. The OCIO will respond to the request within four business days. The OCIO may approve the request, approve the request with conditions, deny the request, or request additional information.

3. EXEMPTION FOR EXISTING SERVICES

Cloud computing services in use on December 31, 2016, are exempt from the requirements of this standard. The exemption for an existing service ends when either: (1) the current term of the agreement for such service expires; or (2) there are significant changes to the service.

4. FedRAMP COMPLIANCE

If the Cloud Service Providers (CSP's) does not have an official FedRAMP certification by an accredited third-Party Assessor Organization (3PAO), and the CSP is being considered for use by the State, the following conditions must be met or addressed via agreement with the service provider before engaging any cloud service providers when that cloud service may store or process any Confidential or Restricted data:

1. The Cloud Service Provider or third-party host (CSP/3PH) must provide evidence of secure storage of access credentials that are at least equal to that of State internal systems.
2. Access to the cloud service will require multi-factor authentication based on data classification levels.
3. De-provisioning of credentials must occur within two (2) hours of de-provisioning of the internal system credentials.
4. Information will be encrypted using IT approved technology for information in transit as well as information stored or at rest.
5. Encryption key management will be controlled and managed by the State unless explicit approval for key management is provided to CSP/3PH by IT. This may require an escrow service for key storage.

6. All equipment removed from service, information storage areas, or electronic media that contained State of Nebraska information must have all this information purged using appropriate means. Data destruction must be verified by the State before allowing that equipment, information storage space, or media to be destroyed or assigned for reuse. A Certificate of Destruction must be provided for equipment that has been destroyed.
7. CSP/3PH will provide vulnerability scanning and testing on a schedule approved by the State ISO. Results will be provided to Department.
8. Patch management of hardware and software at the CSP/3PH are required to meet the same standards that are required at State.
9. CSP/3PH will meet all State of Nebraska requirements for chain of custody and Confidential / Restricted information breach notification if State requires forensic analysis. CSP/3PH will maintain an incident management program that notifies State within one (1) hour of a breach.
10. CSP/3PH will provide evidence of audit and assessment of the security of the service environment, and will agree to reasonable inspection of such security by Department-authorized parties.
11. CSP/3PH is required to advise the State on all geographic locations of stored State information. CSP/3PH will not allow State information to be stored or accessed outside the USA without explicit approval by the OCIO. This includes both primary and alternate sites.
12. Privileged access roles at the CSP/3PH are required to meet the same vetting standards of privileged access personnel at the State, such as background checks, etc.
13. Contracts with CSP/3PH's shall have SLAs in place that clearly define security and performance standards. Contracts will address how performance and security will be measured, monitored, and reported. Contracts will also establish an enforcement mechanism for SLA compliance.
14. . CSP/3PH will provide adequate security and privacy training to its associates, and provide the SISO with adequate evidence of this training.
15. CSP/3PH will provide the State with the ability to conduct a reasonable search to meet Nebraska Public Records Law.
16. Before contracting with a CSP/3PH, the State shall have proactive records planning in place to ensure the ability to have timely and actual destruction of records in accordance with Department record retention policies.
17. CSP/3PH will provide documentation, evidence, or reasonable access by the OCIO and SISO to ensure compliance with these standards.

ARTICLE 7

AUDITING AND COMPLIANCE

8-700. Auditing and Compliance Security Standard

It is the responsibility of the SISO to ensure an appropriate level of Security oversight is occurring at all potential exposure points of State and Agency systems and operations so that the State has reasonable assurance that the overall security posture continuously remains intact. The SISO and AISO have the responsibility to ensure the overall security program meets state and federal statutes as they apply to the State of Nebraska and its Agency operations and resources.

The SISO will establish and manage an entity-wide oversight and compliance function. This will include, at a minimum, appropriate information security oversight at key points within the Technology Acquisition Process, Hardware and Software Change Management Process, and the Contract Management Process when changes involve access to or potential exposure of Confidential or Restricted information.

Compliance with this policy is mandatory. Any compromise or suspected compromise of this policy must be reported as soon as reasonably possible to appropriate agency management and the State Information Security Officer. The failure to comply with this or any other security policy that may or may not result in the compromise of State information confidentiality, integrity, and/or availability may result in action as permitted by law, rule, regulation or negotiated agreement. Each agency will take appropriate steps necessary, including legal and administrative measures, to protect its assets and monitor compliance with this policy.

An agency review to ensure compliance with this policy and applicable NIST 800-53 security guidelines must be conducted at least annually and each Agency management will certify and report the agency's level of compliance with this policy

The SISO may periodically review Agency compliance with this policy and the related NIST control framework. Such reviews may include:

- Reviews of the technical and business analyses required to be developed pursuant to this policy
- Project documentation, technologies or systems which are the subject of the published policy or standard.

These additional reviews may occur due to significant changes in technical infrastructure, or to validate corrective actions after a security incident. All identified gaps or deficiencies shall be documented in an Agency Security Corrective Action Plan that shall be made available to the State Information Security Officer as necessary. The Security Corrective Action plan is classified as a Restricted information document, and should contain detailed descriptions of the security deficiencies, recommended remediation or mitigation activity, key milestones and target dates, and responsible parties. This plan should be a regular item for review by senior Agency and OCIO management to ensure acceptable progress is being made on mitigating or remediating security gaps.

8-701. Awareness and Training

The State of Nebraska provides information technology resources to authorized Users to facilitate the efficient and effective performance of their duties. The use of such resources imposes certain responsibilities and obligations subject to state government policies and applicable state and federal laws. It is the responsibility of all staff to protect information resources and ensure that such resources are not misused.

An information security awareness program must be developed, implemented, documented, and maintained that addresses the security education needs of the State. To ensure staff is knowledgeable of security procedures, their role and responsibilities regarding the protection of agency information and the proper use of information processing to minimize security risks, all staff with access to agency information must receive security awareness training, which must be reinforced at least annually. Technical staff must be trained to a level of competence in information security that matches their duties and responsibilities.

New Hire and Refresher Training

Every member of the Staff is required to attend security training as part of their new-hire orientation. On an annual basis, every member of the Workforce is required to complete a security and privacy training session. The State will maintain records of all attendance for new hire and refresher training.

Periodic Briefings

Management shall periodically incorporate Information Security topics into their meetings with Workforce. The SISO and/or agency AISO shall be available to conduct periodic briefings on various security topics as requested. Additionally, the SISO shall require periodic security briefings to selected audiences when circumstances require, such as responding to a gap in security policy or addressing recurrence of security incidents.

Annual Employee Acknowledgement

New members of the Workforce will sign an acknowledgement of understanding of the Policy and their obligations to comply with the Policy no later than one (1) week after their hire date. Members of the Workforce are required to sign an understanding of the Policy and agreement to comply with the Policy annually.

8-702. Security Reviews and Risk Management

This Policy is based on the NIST 800-53 *Security Controls* framework. As such, the State is required to conduct an annual review of the information technology environment to ensure compliance with these standards. The security controls that are to be inspected are organized into control families within three classes (management, operational, and technical).

The SISO will facilitate and oversee an annual security control assessment. This assessment will cover at least 1/3 of the control areas defined in the NIST 800-53 Security Controls, such that over a three-year timeframe all control areas will have been assessed.

This review shall be conducted for each major system used within the State, and shall include all infrastructure and peripheral processes that are used to support State business processes.

Unscheduled Risk Assessments

Unscheduled risk assessments will be performed at the discretion of the SISO or AISO, typically when circumstances require additional oversight, such as after a security incident, increased security threat, or significant changes to the IT infrastructure. These assessments are flexible in nature, and are intended to review specific elements that have been identified as exception-based or high priority. These reviews can also be performed to validate the appropriate remediation or mitigation of a previous finding.

The Security Officer shall document the business area, reason for the review, scope of inspection, and dates of the review in the Corrective Action Planning documentation. All findings and results will also be documented in the Security Corrective Action Plan.

8-703. Logging and Review of Auditable Events

All systems that handle Confidential or Restricted information, allow interconnectivity with or from other systems, or make access control (authentication and authorization) decisions, shall record and retain audit-logging information sufficient to answer the following questions:

- What activity was performed?
- Who or what performed the activity, including on what system the activity was performed.
- What the activity was performed on (object)?
- When was the activity performed?
- What tool(s) was the activity performed with?
- What was the status (such as success vs. failure), outcome, or result of the activity?

Log Format, *S*torage, and Retention

The State of Nebraska is required to ensure availability of audit log information by allocating sufficient audit record storage capacity to meet policy requirements. OCIO and the Agency IT teams shall perform annual capacity planning and trend analysis to reduce the likelihood of such capacity being exceeded. The capacity and utilization of log files shall be regularly monitored and reported, and action will be taken to keep an approved level of freespace available for use. Automated notification of Agency or OCIO personnel shall occur if the capacity of log files reaches defined threshold levels, or the audit logging system fails for any reason.

The Audit Logging process is required to provide system alerts to appropriate Agency or OCIO personnel in the event of an audit processing failure (e.g., shut down information system, unintended overwriting of the oldest audit records, stop generating audit records, etc.). It is required that all system logs shall be sent to a central log review system that is protected from unauthorized access and is backed up for availability and integrity purposes. All log files shall be retained or recoverable for seven years.

Auditable Events

The State System and Network infrastructure are defined as “the LAN, WAN, Servers, firewalls, and Routers/Switches use to provide electronic communication and data /information processing, whether supported by the Agency directly or the OCIO”.

Security safeguard regulations require logging and reviewing events that are determined to have a moderate or above level of risk. Auditable events may be incorporated into system auto logs and change management documents. The following System and Network Infrastructure events should be logged and reviewed on a weekly basis:

- Log on and off the system;
- Change of password;
- All system administrator commands, while logged on as system administrator;
- Switching accounts or running privileged actions from another account, (e.g., Linux/Unix SU or Windows RUNAS);
- Creation or modification of super-user groups;
- Subset of security administrator commands, while logged on in the security administrator role;
- Subset of system administrator commands, while logged on in the user role;
- Clearing of the audit log file;
- Startup and shutdown of audit functions;
- Use of identification and authentication mechanisms (e.g., user ID and password);
- Change of file or user permissions or privileges (e.g., use of suid/guid, chown, su);
- Remote access outside of the corporate network communication channels (e.g., modems, dedicated VPN) and all dial-in access to the system;
- Changes made to an application or database by a batch file;
- Application-critical record changes;
- Changes to database or application records, where the application has been bypassed to produce the change (via a file or other database utility);
- All system and data interactions concerning FTI;
- Additional platform-specific events, as defined by Agency needs or requirements;
- Detection of suspicious/malicious activity such as from an Intrusion Detection or Prevention System (IDS/IPS), anti-virus system, or anti-spyware system
- Physical entrance or access to secured and restricted areas or facilities where system and network infrastructure reside.

Audit Log Contents

Audit logs shall contain sufficient information to establish what events occurred, the sources of the events, and the outcomes of the events. The logs shall identify or contain at least the following elements, or enough information in which to infer the following elements with reasonable assurance.

- Type of action; Examples include authorize, create, read, update, delete, and accept network connection.
- Subsystem performing the action; Examples includes process or transaction name, process or transaction identifier.
- Identifiers (as many as available) for the subject requesting the action; Examples include user name, computer name, IP address, and MAC address. Note that such identifiers should be standardized to facilitate log correlation.
- Date and time the action was performed, including relevant time-zone information if not in Coordinated Universal Time;
- Whether the action was allowed or denied by access-control mechanisms;
- Description and/or reason-codes of why the action was denied by the access-control mechanism, if applicable;
- Depending on the nature of the event that is logged, there may be other information necessary to collect.

Audit Review, Monitoring, Findings and Remediation

Security safeguard regulations require regular inspections of system audit logs for indications of inappropriate or unusual activity. Additionally, these logs shall be reviewed by authorized personnel to facilitate investigations of suspicious activity or suspected violations. All reports of findings shall be reported to appropriate officials who will prescribe the appropriate and necessary actions.

- Logs of suspicious activity shall be reviewed as soon as possible.
- Logs of system capacity and log integrity shall be reviewed on a weekly basis.
- Logs of privilege access account creation or modification shall be reviewed on a weekly basis
- All other logs shall be reviewed at monthly at a minimum

When possible, the Agency or OCIO will employ automated mechanisms to alert the OCIO, SISO, or AISO when inappropriate or unusual activities with security implications are discovered. Any automation used for log analysis will not change the underlying log structure. It is acceptable for log analysis tools to extract data for analytical review, if the original audit logs remain unchanged and secured.

All relevant findings discovered because of an audit log review shall be listed in the appropriate problem tracking system or the Corrective Action Planning (CAP) process to ensure prompt resolution or appropriate mitigating controls. All results and findings generated by the audit or review process must be provided to appropriate Department management within one week of project/task completion. This report will be considered Confidential Information.

Application Logging Review and Monitoring

The State requires that application development or acquisition activity include applicable application logging for security events. Application logs are invaluable data for identifying security incidents, monitoring policy violations, establishing baselines, providing information about problems and unusual conditions, contributing additional application-specific data for incident investigation which is lacking in other log sources, and helping defend against vulnerability identification and exploitation through attack detection.

Application logging might also be used to record other types of events too. Application logging content must be part of the overall system analysis and design activity, and should consider:

1. Application process startup, shutdown, or restart;
2. Application process abort, failure, or abnormal end;
3. Significant input and output validation failures;
4. Business process monitoring (e.g., activity abandonment, transactions, connections, information requests);
5. Audit trails (e.g., data addition, modification and deletion, data exports);
6. Performance monitoring (e.g., data load time, page timeouts);
7. Compliance monitoring and regulatory, legal, or court ordered actions;
8. Authentication and authorization successes and failures;
9. Session management failures;
10. Use of higher-risk functionality (e.g., addition or deletion of application credentials, changes to privileges, assigning users to tokens, adding or deleting tokens, submission of user-generated content - especially file uploads); and
11. Suspicious, unacceptable or unexpected behavior.

Application logs will be reviewed at least monthly. Corrective actions to address application deficiencies will be managed through the application development process or the applicable Security CAP process.

8-704 Security Requirements for Third Parties and Vendors

All third-party organizations who have access to Confidential or Restricted information are required to have documented agreements and/or Memorandums of Understanding that describes the minimum security requirements they must follow to appropriately protect this information. This includes vendors who have access to equipment or infrastructure that stores, accesses, or processes Confidential or Restricted Information. All technology contracts with vendors or third parties who have access to non-public information are required to include information security requirements. The required language must describe the Confidentiality, Integrity, Availability, and Privacy controls required for the third party to follow.

Any discrepancies or inability to follow these requirements must be documented and approved by the Office of the CIO and the State Information Security Officer so that mitigating or alternative plans may be considered. The State Information Security Officer will have the

authority to inspect these third-party arrangements to ensure compliance to State Policies and requirements.

For information to be released outside an agency or shared between agencies, a process must be established that, at a minimum:

- evaluates and documents the sensitivity of the information to be released or shared;
- identifies the responsibilities of each party for protecting the information;
- defines the minimum controls required to transmit and use the information;
- records the measures that each party has in place to protect the information;
- defines a method for compliance measurement;
- provides a signoff procedure for each party to accept responsibilities;
- establishes a schedule and procedure for reviewing the controls (Refer to Section 4.6. Data Classification).

Non-public State information must not be made available through a public network without appropriate safeguards approved by the data owner(s). The agency must implement safeguards to ensure access control, and data protection measures are adequately protecting State information and logs are collected and protected against unauthorized access. Non-public information includes, but is not limited to:

- critical infrastructure assets which are so vital that their infiltration, incapacitation, destruction or misuse could have a debilitating impact on health, welfare or economic security of the citizens and businesses of the State of Nebraska
- data that identifies specific structural, operational, or technical information, such as: 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;
- personally identifiable information (PII) as defined under Neb. Rev. Stat. § 87-802;
- protected health information (PHI) as defined at 45 CFR § 160.103;
- federal tax information (FTI) as defined at 26 U.S. Code § 6103

ARTICLE 8

VULNERABILITY AND INCIDENT MANAGEMENT

8-801. Incident Response

Computer systems are subject to a wide range of mishaps; from corrupted data files, to viruses, to natural disasters. These incidents can occur at any time of the day or night. Many mishaps are fixed through day-to-day operating procedures, while more severe mishaps are addressed in other ways (e.g., Disaster Recovery plans). Responses to an incident can range from recovering compromised systems to the collection of evidence for a variety of forensic requirements. Preparation and planning for incidents, and ensuring the right resources are available, are critical to the State of Nebraska's ability to adequately detect, respond and recover from security incidents.

The State of Nebraska and all Agencies that process, store, or access Confidential or Restricted information are required to maintain an Incident Response Plan per this policy. This plan shall include operational and technical components, which provide the necessary functions to support all the fundamental steps within the Incident Management Life Cycle - including the following:

1. Preparation
2. Incident Triage and Identification
3. Containment
4. Incident Communication
5. Preservation of Evidence
6. Root Cause Analysis
7. Recovery and Permanent Remediation

The security policy requires the establishment and maintenance of a computer security incident response capability that is in effect 24x7. This document identifies key steps for reporting security incidents and establishes formal reporting requirements for all such instances to the State's Senior Management and Agency officials responsible for reporting to federal offices,.

These procedures also describe the way OCIO or Agency technical staff will aid the in the eradication, recovery, and permanent remediation of the root cause of the incident. This is important to preserve as much evidence as practical while keeping in mind that prevention of damage is of the highest priority.

A. <u>Preparation - Scope and Responsibilities</u>

A security incident is any adverse event whereby some aspect of the State infrastructure is threatened (e.g., personal violation, loss of data confidentiality, disruption of data integrity, denial of service, security breach, etc.). It is important to note that even if there is no evidence of information being accessed by unauthorized personnel, exposing sensitive information in an unsecure manner is considered a security incident. For example, any unencrypted e-mail containing Confidential or Restricted information (e.g. Federal Tax Information, Personally Identifiable Information, etc.) sent outside the secured State of Nebraska network is a security incident and should be reported as such.

All security incidents must be reported to the State Information Security Officer, Department Management, or the OCIO Help Desk **IMMEDIATELY**. Security incidents will be tracked by the SISO. Any State employee or contractor who observe, experience, or are notified of a security incident, should immediately report the situation to the AISO, SISO or the OCIO Help Desk, but at the very least to their supervisor. All State of Nebraska management are responsible to ensure that their employees and contractors understand that awareness of the incident are to be reported immediately to the SISO, Department Management, or the OCIO Help Desk.

State and Agency Legal and/or Privacy Office

These departments are required to work with the Information Technology teams and the SISO/AISO during triage to assess reportable conditions. They are responsible for crafting any communications for customers, government officials and the public in the event of a reportable breach. They are also responsible for ensuring all third-party agreements have requirements to comply with the State's Incident Management requirements.

State Information Security Officer and Agency Information Security Officer

The Security Officers are responsible for assembling, engaging, and overseeing the applicable Incident Response Team. They will coordinate the management of security incidents and any identified follow-up activity, remediation, or countermeasures. They are also responsible for taking lead with Information Technology personnel to perform analysis and triage of incident impact and reportable conditions.

The Security Officers will finalize and sign off on any Security Incident Reports, and determine follow-up activity, root cause analysis, long term mitigation, and updates to the security awareness training. They are also responsible for ensuring that all technical areas within the State have an understanding and ability to meet this standard. They are required to perform education and training of this standard to all applicable Department personnel, and then test the Incident Response Process annually.

Incident Response Team

The State shall identify key personnel who will serve as members of the Incident Response Team. Agencies may also identify additional Incident Response teams for their specific environment. This team will be made up of knowledgeable staff that can rapidly respond to, manage, and support any suspected incident to minimize damage to State information systems, networks and data by identifying and controlling the incident, properly preserving evidence, and reporting to appropriate entities. This team can change from time to time, depending on the nature of the incident and the skills necessary to recover from it. The SISO or AISO will maintain a contact list which includes the names, telephone numbers, pager numbers, mobile telephone numbers, email addresses, organization names, titles, and roles and responsibilities for all potential key incident response resources. Key responsibilities for the Incident Response team include:

- The State of Nebraska direction is "Prevention over Forensics". In other words, do not allow a damaging incident to continue so that additional evidence may be collected.
- Conduct the initial triage. Perform a damage and impact assessment and document the findings.

- Report to State of Agency management on a regular schedule with status and action plans.
- Maintain confidentiality of the circumstances around the incident.
- Follow procedures to maintain a chain of trust and to preserve evidence.
- Initiate the Root Cause analysis, bring in other resources as necessary.
- Initiate return to normal operations, bring in other resources as necessary.

B. Incident Management Procedures

Incident Management procedures require, first and foremost, prevention of damage from the incident over forensics. This means that the priority is to shut off or terminate any potential damaging threat. It is strongly desired to perform this action in a manner that allows for detailed forensics or preservation of evidence, but if there is ANY doubt, all State personnel, whether employees or contractors, are required to disable the threat immediately. Following the assessment and termination of the threat, the next priority is containment, followed by recovery actions, damage determination, report documentation, lessons learned, and implementation of corrective actions.

All communication related to the incident shall be carefully managed and controlled by the OCIO and Agency Senior Management. Only previously identified officials are authorized to communicate to other State of Nebraska officials, the public/press, or any other government agency. All personnel involved any incident management support activity will communicate only with the parties necessary for incident analysis or recovery activity, and to the SISO, OCIO, or the Agency Information Technology team. No other communication, unless explicitly authorized, is allowed.

A Security Incident Report information is classified as Restricted Information. Sharing or distribution of the information will be limited to only those individuals with a valid need-to-know. The OCIO or Agency management, with consultation from the SISO/AISO, will review all requests for the release of security incident information and make determinations regarding its release, ensuring that it is consistent with applicable policies, regulations, and external customer requirements. Overall questions regarding this procedure should be directed to the SISO and AISO.

C. Incident Management Training and Testing

The State and/or Agency shall provide annual training on incident recognition and reporting requirements to all staff and contractors. More in depth training and awareness will be given to all applicable staff in incident response and recovery procedures and reporting methods. Annually, the SISO and AISO shall provide training for appropriate identification, management, and remediation of an incident and shall facilitate a simulated incident response and recovery test for the State or Agency Security Incident Response team. This test shall simulate a variety of security related incidents.

D. Incident Triage and Identification

As soon as an incident is suspected, personnel qualified and designated to respond shall be notified to take immediate action, determine incident impact, file a ticket, or prepare a report.

Initial triage shall be conducted by the SISO/AISO, OCIO Help Desk, or the Information Technology team to understand the scope and impact of the incident and initiate appropriate action. Once an incident has been identified and reported, the SISO/AISO (or designate) will assume oversight of the incident response and will continually assess the incident conditions and determine if escalation of response actions is appropriate. Prevention of damage is given priority over forensics of incident source. Therefore, the SISO/AISO and IT Management reserve the right to quarantine any potentially threatening system and terminate any threatening activity using all means necessary. The SISO will ensure that a Security Incident Report is completed for all incidents.

For more complicated incidents that may require further analysis, the Incident Response team will be assembled via direction from the SISO, OCIO, AISO, or Agency IT Management. This team will take over the triage and impact assessment process.

A damage analysis of security incidents is to be initiated immediately after assessment by the SISO and/or the Incident Response Team. They will determine if the incident impacts organizations outside of the Department's internal network. They will also determine if any reportable conditions, such as unauthorized disclosure of Confidential or Restricted information exists. If the incident appears to have ANY citizen information compromised, immediate notification to the Senior Management, SISO, AISO, or OCIO is REQUIRED. This person will then notify other appropriate senior State officials ore relevant parties and will determine the communication plan for any government agencies or the public and press. Senior Management or designates will oversee and coordinate all communication actions.

All forms of unauthorized disclosure of Confidential or Restricted information, including the potential for unauthorized disclosure (such as information spillage), shall be considered Incidents. Information spillage refers to instances where either Confidential or Restricted information is inadvertently placed on information systems that are not authorized to process such information. Such information spills often occur when information that is initially thought to be of lower sensitivity is transmitted to an information system and then is subsequently determined to be of higher sensitivity. At that point, an Incident has occurred and corrective action is required.

All compromised systems will be disconnected from external communications immediately upon discovery. Senior Management will be notified of analysis results and citizen impact immediately upon discovery, and shall be kept abreast of all analysis findings, impact assessments, and remediation progress.

E. <u>Incident Containment and Recovery</u>

Any IT resources that are engaged in active attacks against other IT resources must be isolated and taken off the State network immediately. Incidents involving the exposure (or POTENTIAL exposure) of Confidential or Restricted information to unauthorized parties must also be contained immediately. Other compromises must be contained as soon as practical, considering impacts of service interruptions, recovery of equipment, and potential impacts of the incident itself.

Containment can be achieved by immediately disconnecting the resource from the network, revoking user access, or other means as appropriate. The SISO has the authority to coordinate with the OCIO to block compromised services and hosts that present a threat to the rest of the State network. Notifications of outages or service interruptions will follow normal OCIO or Agency procedures if possible, but will not delay the outage or interruption if an attack or breach is underway or if the threat of an attack or breach is imminent.

Once the incident has been verified and contained, the OCIO or the Agency IT Department can begin carefully bringing resources back on line and operational.

F. Incident Communication

Reportable conditions, such as the breach of PHI, PII or FTI, require notification within specific timeframes (as defined in state and federal regulations). It is the responsibility of the SISO and AISOs to understand these requirements and ensure the State and/or Agency remains compliant in the event of a reportable incident.

Additionally, communication during a security incident must be carefully controlled to ensure that information that is disclosed is accurate, timely, and provided only to appropriate audiences.

It is the responsibility of the SISO, AISO, OCIO, and Agency management to ensure that all communication regarding any security incident is managed and controlled.

G. Preservation of Evidence

In the event of a discovery of a breach of system security protections, an internal security investigation must be properly performed to preserve evidence. If the incident involves any type of law enforcement, the Incident Response team shall secure the potential evidence without reviewing additional content. Network hardware, software or data may be considered potential evidence.

A subpoena, warrant or other official request must be issued before any data is released to law enforcement. Only senior State and Agency Officials are authorized to release any evidence to law enforcement. Evidence from incidents that involve an immediate threat to persons or property may be provided to law enforcement in advance of a public records request, subpoena or warrant, but may only be provided by authorized parties.

The chain of custody steps that should be taken to preserve all potential evidence in the event of a security breach are as follows:

a. If possible, isolate the system from the network, either physically (unplug the network cable), or logically. Do NOT power the system off. Evidence in system memory may be lost.

b. If the system cannot be taken off the network, take pictures and screenshots.

c. Notify the Department IT Security Officer immediately after initial steps, but NO LATER than one hour after becoming aware of the possible incident.

d. Make a bit copy of the drive before investigating (i.e., opening files, deleting, rebooting).

e. Dump memory contents to a file.

f. Label all evidence.

g. Log all steps.

H. Incident Documentation and Root Cause Analysis

An incident report is required for all incidents except those classified as having a low impact to the State network. The incident report should include entry of the root cause, actions taken and any remediation or mitigation strategy to reduce the risk of recurrence. Depending on the nature of the security incident, a post-mortem meeting may be conducted.

Documentation of information is critical in situations that may eventually involve authorities as well as provides documentation of the actions taken to resolve the event. Incident reports are Restricted Information, and copies will only be distributed under direction of State or Agency management.

A formal Root Cause Analysis shall be performed within two weeks of the occurrence of the Security Incident. This analysis shall identify the core issues of the incident in the affected environment and actions that can be taken to address these issues. This can include physical, logical, or environmental changes, operational or administrative control changes, or enhanced training, education, or awareness programs.

I. Incident Recovery and Permanent Remediation

The Incident Response team working with technology, application and data owners shall evaluate and determine when to return compromised systems to normal operations. Access to compromised systems shall be limited to authorized personnel until the security incident has been contained and root cause mitigated. Analysis and mitigation procedures shall be completed as soon as possible, recognizing State systems are vulnerable to other occurrences of the same type.

The OCIO, SISO, and AISO shall define and prioritize the requirements to be met before returning an affected or compromised system to normal operations. Recovery procedures shall include:

- Reinstalling compromised systems from trusted backup-ups, if required;
- Reinstalling system user files, startup routines, or settings from trusted versions or sources, if required;
- Validating Restored Systems through system or application regression tests, user verification, penetration tests, and vulnerability testing and test result comparisons;
- Increasing Security monitoring and heighten awareness for a recurrence of the incident.

8-802. Penetration Testing

Systems that provide information through a public network, either directly or through another service that provide information externally (such as the World Wide Web), will be subjected to State penetration testing and intrusion testing. Penetration and intrusion testing will be conducted at the request of the agency or data owner(s) to determine if unauthorized access and or changes to an application can be made.

The results of the penetration and intrusion testing will be reviewed in a timely manner by the State Information Security Officer. Any vulnerability detected will be evaluated for risk by the agency and a mitigation plan will be created and forwarded to the State Information Security Officer. The tools used to perform these tasks will be updated periodically to ensure that recently discovered vulnerabilities are included.

Where an agency has outsourced a server, application or network services to another entity, responsibility for penetration and intrusion testing must be coordinated by both entities.

Any penetration or intrusion testing must be performed by individuals who are authorized by the State Information Security Officer and who have requested and received written consent from the Office of the Chief Information Officer at least 24 hours prior to any testing or scanning. Agencies authorized to perform penetration and intrusion testing or vulnerability scanning must have a process defined, tested and followed always to minimize the possibility of

disruption. Any other attempts to perform tests or scans will be deemed an unauthorized access attempt.

8-803. Vulnerability Scanning

Systems that provide information through a public network, either directly or through another service that provide information externally (such as the World Wide Web), will be subjected to vulnerability scanning.

All servers will be scanned for vulnerabilities and weaknesses by the Office of the Chief Information Officer before being installed on the State network. For both internal and external systems, scans will be performed at least monthly or after any major software or configuration changes have been made, to ensure that no major vulnerabilities have been introduced. Priority setting of vulnerabilities will be based on impact to the State and as referenced in the National Vulnerability database (HTTP://nvd.nist.gov).

All web-based applications will be scanned for vulnerabilities and weaknesses before being promoted to a production environment or after any major upgrades or changes have occurred. Results of the vulnerability scan will be reviewed in a timely manner by the State Information Security Officer. Any vulnerability detected will be evaluated for risk by the OCIO or Agency and a mitigation plan will be created as required and forwarded to the State Information Security Officer. The tools used to perform these tasks will be updated periodically to ensure that recently discovered vulnerabilities are included.

Where an agency has outsourced a server, application or network services to another entity, responsibility for vulnerability scanning must be coordinated by both entities and the scanning must meet State of Nebraska policy.

8-804. Malicious Software Protection

Software and associated controls must be implemented across agency systems, and logs monitored, to detect and prevent the introduction of malicious code into the State environment. The introduction of malicious code such as a computer virus, worm or Trojan horse can cause serious damage to networks, workstations and state data. Users must be made aware of the dangers of malicious code. The types of controls and frequency of updating signature files, is dependent on the value and sensitivity of the information that could be potentially at risk.

For workstations, virus signature files must be updated at least weekly. On host systems or servers, the signature files must be updated daily or when the virus software vendor's signature files are updated and published. Security patches for software will be applied as defined by the Change Management Process, but all software must have security patches applied as soon as possible.

8-805. Security Deficiencies

All security deficiencies reported or identified in any security review, scan, assessment, or analysis shall be documented in the State or Agency Security POAM per policy 8-100. These gaps shall be managed to mitigation, remediation, or approved risk acceptance.

ARTICLE 9

DATA SECURITY

8-901. State of Nebraska Information Sharing

It is critical that Agencies that share information and systems learn as much as possible about the risks associated with the planned or current interconnection and the security controls that they can implement to mitigate those risks. It also is critical that they establish formally documented agreements regarding the management, operation and use of interconnections, as required. The agreement should be reviewed and approved by appropriate senior staff from each organization.

All Agencies that share connectivity and information between the Agency and the OCIO are required to have a security program that meets this information security policy. The AISO shall develop a System Security Plan that must be approved by the SISO. All Agencies shall perform a security control assessment that identifies the adequacy of security controls and precautions for protecting State information. If the Agency performs this assessment independent of the SISO, an approved and signed Interconnection System Agreement (ISA) that describes the security controls and plans will be in place to protect State information.

8-902. Data Inventory

Each Agency shall identify and classify all information according to this policy. Agencies are required to perform a Security Control Assessment (SCA) that assesses the adequacy of security controls commensurate with its Data Classification as well as the Agency's level of compliance with this policy and/or applicable security frameworks (such as NIST, PCI, CMS, IRS, etc.) . The assessment can be performed internally by the AISO or with the assistance of the SISO, but each Agency is required to have an assessment at least once every three years, covering at least 1/3 of the applicable controls such that all control areas have been assessed over a three-year period. Agencies are also required to perform an assessment anytime significant changes to the technical environment occur.

To aid in this assessment, agencies are required to maintain an inventory of where Confidential and Restricted information reside, so those environments can be assessed for security adequacy.

8-903. Data Classification

Data is a critical asset of the State of Nebraska. All staff have a responsibility to protect the confidentiality, integrity, availability of data generated, accessed, modified, transmitted, stored or used by the State of Nebraska, irrespective of the medium on which the data resides and regardless of format (such as in electronic, paper or other physical form).

Agencies are responsible for establishing and implementing appropriate managerial, operational, physical, and technical controls for access to, use of, handling of, transmission of, and disposal of State data in compliance with this policy, federal requirements, and the agency Records Retention schedule. The agency data owner should carefully evaluate and determine the appropriate data sensitivity or classification category for their information. Assigning classifications determines day-to-day practices with information: how it is handled, who handles it, how it is transported, stored, who has access, where it can go, etc.

Data owned, used, created or maintained by the State is classified into the following four categories:

- **Restricted.** This classification level is for sensitive information intended for use by a limited number of authorized staff with an explicit “need to know” and controlled by special rules to specific personnel. Examples of this privileged access information include attorney/client privilege information, Agency strategies or reports that have not been approved for release, audit records, network diagrams with IP addresses specified, privileged administrator credentials, etc., This level requires internal security protections and could have a high impact in the event of an unauthorized data disclosure.
- **Confidential.** This classification level is for sensitive information intended for use within an Agency and controlled by special rules to specific personnel. Examples of this type of data include Federal Tax Information (FTI), Protected Health Information (PHI) and other Patient Medical Records covered by Health Insurance Portability and Accountability Act (HIPAA), Payment Card Industry (PCI) information, Personally Identifiable Information (PII) and any other information regulated by State or Federal regulations..
- **Managed Access Public**. This classification level is for information that is public in nature but may require authorization to receive it. This type of information requires a minimal level of security and would not have a significant impact in the event of data disclosure. This type of information does not include personal information but may carry special regulations related to its use or dissemination. Managed Access Public data may also be data that is sold as a product or service requiring users to subscribe to this service.
- **Public**. This classification is for information that requires no security and can be handled in the public domain.

8-904. Information Retention and Destruction

All information, created, acquired or used in support of State of Nebraska's business activities, must be used for official business only. Agency information is an asset and must be protected from its creation through its useful life, and to its authorized disposal in accordance with the Records Management Act and your agency's retention schedule. State information must be maintained in a secure, accurate, and reliable manner and be readily available for authorized use.

Disclosure of sensitive information through careless disposal or re-use of equipment presents a risk to the State of Nebraska. Formal procedures must be established to minimize this risk. Storage devices such as hard disk drives, paper or other storage media (e.g. tape, diskette, CDs, DVDs, USB drives, cell phones, memory sticks,) regardless of physical form or format containing confidential or restricted information must be physically destroyed or securely overwritten when the data contained on the device is no longer required under the provisions of the Records Management Act. These events should include certificates of destruction. State and agency asset management records must be updated to reflect the current location and status of physical assets (e.g., in service, returned to inventory, removed from inventory, destroyed, etc.) when any significant change occurs.

Sec.2. In section 5-204(2.2.6), strike the sentence beginning with “Section”.

Sec.3. Strike section 5-204(4) in its entirety.

Sec.4. In Attachment A to section 5-204, strike the sentence beginning with “See NITC 8-101”; strike the bulleted sentence beginning with “Approved remote access”; and strike the subsection titled: “Identified NITC policies that apply to use, access and protecting information:” in its entirety.

Sec.5. In Attachment B to section 5-204, strike the sentence beginning with “See NITC 8-101”; strike the bulleted sentence beginning with “Approved remote access”; and strike the subsection titled: “Identified NITC policies that apply to use, access and protecting information:” in its entirety.

Sec.6. Staff shall reformat and re-enumerate the provisions of this proposal for consistency prior to final publication.

Sec.7. Original sections 5-204, 8-101, 8-102, 8-103, 8-201, 8-301, 8-302, 8-303, 8-304, and 8-401 are repealed. Resource documents 8-RD-01, 8-RD-02, 8-RD-03, 8-RD-04, 8-RD-05, and 8-RD-06 are repealed.

Sec.8. This proposal becomes operative on xxx xx, xxxx.