CHAPTER 8

INFORMATION SECURITY POLICY

Article.

1. Purpose; Scope; Roles and Responsibilities; 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; POLICY EXCEPTION PROCESS

Section.

8-101. Purpose.

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. This Information Security Policy contains the safeguards, responsibilities and acceptable behaviors required to establish and maintain a secure environment.

--

History: Adopted on July 12, 2017.
URL: https://nitc.nebraska.gov/standards/8-101.pdf

8-102. Scope.

(1) This policy applies to all information technology systems for which the state has administrative responsibility, including systems managed or hosted by third parties on behalf of an agency. In the event an agency has developed policies or additional requirements for information security, the more restrictive policy will apply.

(2) Portions of this policy are based on the standards, guidelines, and best practices developed by the National Institute of Standards and Technology (NIST), including the NIST Cybersecurity Framework (https://www.nist.gov/cyberframework) and related publications (https://csrc.nist.gov/publications). Additional items contained in these NIST publications—that are not included in this policy—should be treated as guidance and best practices to be followed by agencies as appropriate.

--

History: Adopted on July 12, 2017. Amended on March 12, 2020.
URL: https://nitc.nebraska.gov/standards/8-102.pdf

8-103. Roles and responsibilities.

(1) State Agencies. Agencies that create, use, or maintain information systems for the state must establish and manage an information security program consistent with this policy to ensure the confidentiality, availability, and integrity of the state's information assets. Agencies may work with the Office of the Chief Information Officer for assistance with implementing an information security program.

(2) Office of the Chief Information Officer. The Office of the Chief Information Officer is responsible for recommending policies and guidelines for acceptable and cost-effective use of information technology in noneducation state government.

(3) State Information Security Officer. The state information security officer serves as a security consultant to agencies and agency information security officers to assist the agencies in meeting the requirements of this policy and other policies. The state information security officer may also perform assessments of agency security for risk and compliance with this policy and other security related policies and frameworks as applicable.

(4) Agency Information Security Officer. An agency information security officer may be designated at the discretion of the agency. The agency information security officer has the responsibility for ensuring implementation, enhancement, monitoring, and enforcement of information security policies and standards for their agency. The agency information security officer may collaborate with the Office of the CIO on information security initiatives within the agency.

(5) Nebraska Information Technology Commission. The Nebraska Information Technology Commission is the owner of this policy with statutory responsibility to adopt minimum technical standards, guidelines, and architectures.

(6) Technical Panel. The Technical Panel is responsible for recommending technical standards and guidelines to be considered for adoption by the Nebraska Information Technology Commission.

(7) State Government Council. The State Government Council is an advisory group chartered by the Nebraska Information Technology Commission to provide recommendations relating to state government agencies.

(8) Security Architecture Workgroup. The Security Architecture Workgroup is chartered by the State Government Council to 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 real or potential security threats or

vulnerabilities that could impact state business; document and communicate existing problems, potential points of vulnerability, and related risks; and determine security requirements of state agencies stemming from state and federal laws, regulations, and other applicable standards.

--

History: Adopted on July 12, 2017. Amended on March 12, 2020 and July 8, 2021.
URL: https://nitc.nebraska.gov/standards/8-103.pdf

8-104. Policy exception process.

This policy establishes the controls and activities necessary to appropriately protect information and information technology resources. While every exception to a policy or standard weakens the protection for state 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 this policy, the agency may request an exemption by following the procedure outlined in section 1-103.

--

History: Adopted on July 12, 2017.
URL: https://nitc.nebraska.gov/standards/8-104.pdf

ARTICLE 2

GENERAL PROVISIONS

Section.

8-201. Acceptable use.

Subject to additional requirements contained in state law, the following are the policies and provisions governing the acceptable use of information technology resources in state government: (1) section 7-101 is the acceptable use policy for the state network; (2) Neb. Rev. Stat. § 49-14,101.01 establishes certain statutorily prohibited uses of public resources; and (3) the following additional requirements established by this section: (a) all state electronic business must be conducted on approved IT devices; (b) accessing or attempting to access CONFIDENTIAL or RESTRICTED information for other than a required business "need to know" is prohibited; and (c) misrepresenting yourself as another individual or organization is prohibited.

Use of state information technology resources may be monitored to verify compliance with this policy.

--

History: Adopted on July 12, 2017.
URL: https://nitc.nebraska.gov/standards/8-201.pdf

8-202. 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.

The change management process may 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.

(1) IT Infrastructure. The following change management standards are required to be followed for all IT infrastructure:

(a) The Office of the CIO 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 Office of the CIO, agency, 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;

(b) All records, meetings, decisions, and rationale of the change control group must 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: (1) change summary, justification and timeline; (2) functionality, regression, integrity, and security test plans and results; (3) security review and impact analysis; (4) documentation and baseline updates; and (5) implementation timeline and recovery plans;

(c) The 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; and

(d) 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.

(2) 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:

(a) Application change management processes must be performed with assigned responsibilities to ensure all changes to application software are approved and documented. Change management teams will include appropriate application development staff and appropriate staff to represent state information security requirements;

(b) 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;

(c) The change management processes will retain a documented history of the change process as it passes through the software development life cycle with documentation securely stored for audit purposes. Documentation should address a review of the following: (1) change summary, justification, and timeline; (2) functionality, regression, customer acceptance, and security test plans; (3) security review and impact analysis; (4) documentation and baseline updates; and (5) implementation timeline and recovery plans;

(d) Changes to software applications must be controlled and production installations must be made by personnel assigned to update production libraries. Mechanisms to maintain and ensure the integrity of the application code must be implemented;

(e) Changes to production libraries should not be the same personnel who made the application changes unless documented procedures are in place that ensure the confidentiality, integrity, and availability of the data maintained in the production library; and

(f) Application development changes that impact IT infrastructure must be submitted to the infrastructure change management process for review, approval, and implementation coordination.

--

History: Adopted on July 12, 2017.
URL: https://nitc.nebraska.gov/standards/8-202.pdf

8-203. Multi-function devices.

All multi-function devices used to process, store, or transmit data must be approved by the state information security officer or agency information security officer. The device must be configured and managed to adequately protect sensitive information.

Configuration and management of multi-function devices must include minimum necessary access to the processing, storing, or transmitting functions. All unnecessary network protocols and services must be disabled. Access controls must be in place, and administrator privileges must be controlled and monitored. Auditing and logging must be enabled. Access to the internal storage must be physically controlled. The devices must be securely disposed or cleansed when no longer needed. Software and firmware must be updated to the latest version supported by the vendor. All CONFIDENTIAL or RESTRICTED information must be encrypted in transit when moving across a WAN as well as when stored on the internal storage unit of the device. If the device 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 state information security officer or agency information security officer.

--

History: Adopted on July 12, 2017.
URL: https://nitc.nebraska.gov/standards/8-203.pdf

8-204. Email.

(1) Users 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 network unless approved by the state information security officer and, if applicable, the agency information security officer.

(2) CONFIDENTIAL or RESTRICTED data must not be sent by email, or stored in the email system, unless it has been encrypted using technology approved by the state information security officer and, if applicable, the agency information security officer.

--

History: Adopted on July 12, 2017. Amended on March 12, 2020.
URL: https://nitc.nebraska.gov/standards/8-204.pdf

8-205. Portable IT devices.

CONFIDENTIAL or RESTRICED data must not be stored on portable IT devices unless it has been encrypted using technology approved by the state information security officer or the agency information security officer.

--

History: Adopted on July 12, 2017.
URL: https://nitc.nebraska.gov/standards/8-205.pdf

8-206. Facilities; physical security requirements.

Agencies must 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.

--

History: Adopted on July 12, 2017.
URL: https://nitc.nebraska.gov/standards/8-206.pdf

8-207. Facilities; identification badges; visitors.

Only authorized individuals are allowed to enter secure areas of state facilities that contain information technology infrastructure. Those individuals will be issued an electronic ID badge. All authorized individuals are required to scan their ID badge before entry into these secure areas. ID badges must be visible, 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 the following information: 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 secure areas such as data centers. If it is necessary for a visitor to enter a secure 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.

--

History: Adopted on July 12, 2017.
URL: https://nitc.nebraska.gov/standards/8-207.pdf

8-208. External service providers.

All external service providers with access to CONFIDENTIAL or RESTRICTED information must have a written agreement that includes the minimum security requirements necessary for the protection of this information. The state information security officer may inspect these external service provider arrangements to ensure compliance with state policies and requirements.

--

History: Adopted on July 12, 2017.
URL: https://nitc.nebraska.gov/standards/8-208.pdf

8-209. Agency security planning and reporting.

Pursuant to the terms of certain federal data exchange agreements, state agencies may be required to maintain the following documentation:

(1) Information security strategic plan (section 8-210);

(2) System security plan (section 8-211); and

(3) Other information security documentation not covered by this section.

For agencies not subject to federal data exchange agreements, these planning documents are considered guidelines and recommended as best practice.

--

History: Adopted on July 12, 2017. Amended on July 8, 2021.
URL: https://nitc.nebraska.gov/standards/8-209.pdf

8-210. Information security strategic plan.

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 should be given the same level of executive scrutiny at the state as planning for information technology changes. This plan should be updated and published on a biennial basis, and should include a two-year projection of key security business drivers and planned security infrastructure implementation. This plan is necessary to ensure that information security is viewed as a strategic priority, and is included as part of the overall planning process.

Contents of the information security strategic plan:

(1) Summary of the information security, mission, scope, and guiding principles;

(2) Analysis of the current and planned technology and infrastructure design, and the corresponding changes required for information security to stay aligned with these plans;

(3) Summary of the overall information risks assessments and current risk levels;

(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 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 if the agency is required to maintain these documents by other requirement or policy;

(8) Analysis of the regulatory and contractual compliance environment, including potential new regulations or pending contractual requirements that will affect information security; and

(9) Proposed two-year timeline of events and key deliverables or milestones.

--

History: Adopted on July 12, 2017. Amended on July 8, 2021.
URL: https://nitc.nebraska.gov/standards/8-210.pdf

8-211. System security plan.

The system security plan (SSP) provides an overview of the security requirements of the information system including all 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 describe the current controls in place to protect information at a level commensurate with the sensitivity level of the system.

The agency information security officer should develop or update the SSP in response to each of the following events: new system; significant system modification; increase in security risks/exposure; increase of overall system security level; serious security violation(s); or 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. 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 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) 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;

(8) Review of security controls and assessment results that have been conducted within the past three years; and

(9) 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.

--

History: Adopted on July 12, 2017. Amended on July 8, 2021.
URL: https://nitc.nebraska.gov/standards/8-211.pdf

8-212. [Repealed.]

--

History: Adopted on July 12, 2017. Repealed on July 8, 2021.
URL: https://nitc.nebraska.gov/standards/8-212.pdf

ARTICLE 3

ACCESS CONTROL

Section.

8-301. Remote access.

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

The following are the requirements for remote access:

(1) Requests for remote access must be reviewed and approved by the agency and the Office of the CIO;

(2) All remote sessions must use access control credentials and an OCIO-approved form of multi-factor authentication;

(3) All remote sessions must utilize OCIO-approved cryptographic mechanisms as defined by NIST 800-140 to protect the confidentiality and integrity of remote access sessions;

(4) All remote sessions over open public networks must use a VPN when connecting to the state network;

(5) All 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;

(6) All remote state owned or managed devices must be password protected and full-disk encrypted using OCIO-approved technology;

(7) All remote access sessions must be logged. The Office of the CIO or the agency will perform periodic monitoring of remote access sessions with random inspections of the user security settings and protocols to ensure compliance with this policy;

(8) Remote access logon failures must be logged. Credentials must be disabled after three (3) consecutive failed login attempts;

(9) Remote sessions must be locked after no more than 15 minutes of inactivity until the user re-establishes access with the appropriate credentials and authentication procedures;

(10) Mechanisms must be employed to ensure personally identifiable information, or other sensitive information (e.g., SSA, FTI, PII, PHI) cannot be downloaded or remotely stored; and

(11) Restricted data types cannot be accessed by agency employees, agents, representatives, or contractors located offshore—outside of the United States territories, embassies, or military installations.

--

History: Adopted on July 12, 2017. Amended on November 4, 2021.
URL: https://nitc.nebraska.gov/standards/8-301.pdf

8-302. Passwords.

(1) Minimum Password Requirements. The following are the minimum password requirements for state government passwords:

(a) Must contain a minimum of eight characters;

(b) Must contain at least three of the following four: at least one uppercase character; at least one lowercase character; at least one numeric character; or, at least one symbol (!@#$%^&); and

(c) 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 shall use a password that follows at least a confidential level of authentication when logging into a state network or application.

(2) Additional Access Requirements for RESTRICTED Information. Information that is classified as 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 subsection (1), and must contain the following additional requirements:

(a) Multi-factor authentication;

(b) Expire after 60 days;

(c) Minimum password age set to 15 days; and

(d) Accounts will automatically be disabled after three unsuccessful password attempts.

(3) Additional Access Requirements for CONFIDENTIAL Information. Information that is classified as CONFIDENTIAL requires a high level of security. A password used to access CONFIDENTIAL information must follow the password complexity rules outlined in subsection (1), and must contain the following additional requirements:

(a) Expire after 90 days; and

(b) Accounts will automatically lock after three consecutive unsuccessful password attempts.

(4) Password Requirements for MANAGED ACCESS PUBLIC Information. Information that is classified as MANAGED ACCESS PUBLIC requires minimal level of security and need

not comply with subsection (1). 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.

(5) Password Requirements for Accessing PUBLIC Information. Information that is classified as PUBLIC requires no additional password security and need not comply with subsection (1).

(6) 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 subsection (1). The additional requirements for access to CONFIDENTIAL or RESTICTED data with a non-expiring password are:

(a) Extended password length to 10 characters;

(b) Independent remote identity proofing may be required;

(c) Personal security question may be asked;

(d) Multi-factor authentication; and

(e) Any feature not included on this list may also be utilized upon approval of the state information security officer.

(7) 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.

(8) 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 RESTRICTED information.

(9) 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.

--

History: Adopted on July 12, 2017.
URL: https://nitc.nebraska.gov/standards/8-302.pdf

8-302.1. Public accounts; passwords.

This section sets forth the format, minimum requirements, and review procedures for public accounts accessing state resources. This section applies to all public accounts created for use within the State of Nebraska domain namespaces. Public accounts are accounts on state managed systems that are to be used by the general public and are not to be used by state employees or contractors to conduct state business.

(1) Information Access. A public account may only be used by the user to access their own information.

(2) Passwords. The following are the minimum requirements for public account passwords:

(a) Must contain a minimum of 12 characters;

(b) Must contain at least three of the following four complexity requirements: at least one uppercase letter; at least one lowercase letter; at least one numeric value; or, at least one special character; and

(c) Accounts must be locked temporarily after five failed password attempts.

(3) Review Process. Accounts with no successful login activity for a period of 24 months will be disabled. Accounts with no successful login activity for 26 months will be deleted.

(4) Misuse or Abuse. Any misuse or abuse of a public accounts will cause the account in question to be terminated.

--

History: Adopted on July 8, 2021.
URL: https://nitc.nebraska.gov/standards/8-302.1.pdf

8-303. Identification and authorization.

(1) All employees and other persons performing work on behalf of the state, authorized to access any state information or IT resources, that have the potential to process, store, or access non-public information, must be assigned a unique State of Nebraska user ID which resides in the State of Nebraska Active Directory domain with the minimum necessary access required to perform their duties.

(2) Staff are required to secure their user IDs from unauthorized use.

(3) Sharing user IDs is prohibited.

(4) 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.

--

History: Adopted on July 12, 2017.
URL: https://nitc.nebraska.gov/standards/8-303.pdf

8-304. Privileged access accounts.

Privileged access 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 following standards and procedures must be followed to minimize the risk of incidents caused by these accounts:

(1) All privileged access accounts must be assigned to an individual with an approved business need for the privileged access. These accounts must not be shared;

(2) Default administrator accounts must be renamed, removed or disabled. Default passwords for renamed or disabled default administrator accounts must be changed;

(3) Default system account credentials for hardware and software must be either disabled, or the password must be changed. Use of anonymous accounts is prohibited, and unassigned accounts must be assigned to an individual prior to use. When no longer needed, the account must be disabled. At all times, the state requires individual accountability for use of privileged access accounts;

(4) Privileged access accounts will have enhanced activity logging enabled. The Office of the CIO and all applicable agencies will perform a quarterly review of privileged access account activity;

(5) Privileged access through remote channels will be allowed for authorized purposes only and must include multi-factor authentication;

(6) Passwords for these accounts must be changed every 60 days;

(7) The password change process must 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

(8) Privileged access accounts must be approved, provisioned, and maintained by the Office of the CIO.

--

History: Adopted on July 12, 2017.
URL: https://nitc.nebraska.gov/standards/8-304.pdf

ARTICLE 4

NETWORK SECURITY

Section.

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 internal network are required to adhere to these standards.

The Office of the CIO 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 Office of the CIO 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 CIO.

Where an agency has outsourced a server or application to an external service provider (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 will perform the security review on behalf of all agencies.

All publicly accessible devices attached to the state network must be registered and documented in the IT inventory system. Additions or changes to network configurations, including through the use of external service providers, must be reviewed and approved through the Office of the CIO's change management process. Publicly accessible devices must reside in the Office of the CIO's DMZ unless approved by the Office of the CIO for legitimate business purposes.

--

History: Adopted on July 12, 2017.
URL: https://nitc.nebraska.gov/standards/8-401.pdf

8-402. Network transmission security.

The following are network transmission security requirements:

(1) All encryption must be approved by the state information security officer. Any transmissions over unsecured networks (such as the Internet) that contain CONFIDENTIAL or RESTRICTED information must be encrypted using technology that is FIPS 140-2 compliant;

(2) Network scanning and monitoring is prohibited, unless prior approval is obtained from the Office of the CIO. If approved, scanning must be restricted to authorized and registered IP addresses only, and conducted by authorized personnel only;

(3) The Office of the CIO 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; and

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

--

History: Adopted on July 12, 2017.
URL: https://nitc.nebraska.gov/standards/8-402.pdf

8-403. Network architecture requirements.

The following are network architecture requirements:

(1) All devices that store, access, or process CONFIDENTIAL or RESTRICTED information must not reside in the public tier, and must be protected by at least two firewalls. Firewalls must 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 no more than 15 minutes of inactivity;

(4) Devices that include native host-based firewall software in the operating system must 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 network will have an annual verification of all open ports, protocols, and services for publicly accessible systems;

(6) Any requests for public IP addresses or for additional open ports must be approved by the state information security officer;

(7) 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; and

(8) 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.

--

History: Adopted on July 12, 2017.
URL: https://nitc.nebraska.gov/standards/8-403.pdf

8-404. External connections.

Direct connections between the state network and external networks must be implemented in accordance with these policies and standards:

(1) 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 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;

(2) External network and workstation connections to the state network must have an agency sponsor and a business need for the network connection. The external network equipment must also conform to the state's security policies and standards, and be approved by the Office of the CIO; and

(3) 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.

--

History: Adopted on July 12, 2017.
URL: https://nitc.nebraska.gov/standards/8-404.pdf

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.

The following are wireless network requirements:

(1) 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;

(2) No wireless network or wireless access point will be installed without the written approval of the Office of the CIO; and

(3) All wireless networks will be inspected annually by the state information security officer and agency information security officer to ensure proper security protocols are in place and operational.

--

History: Adopted on July 12, 2017.
URL: https://nitc.nebraska.gov/standards/8-405.pdf

ARTICLE 5

SYSTEM SECURITY

Section.

8-501. System security; approved hardware and software; documentation.

(1) Only Office of the CIO approved hardware or software is permitted within the state's information technology infrastructure.

(2) All authorized hardware and software shall be inventoried and documented. Results shall be secured in an auditable fashion.

--

History: Adopted on July 12, 2017.
URL: https://nitc.nebraska.gov/standards/8-501.pdf

8-502. Minimum user account configuration.

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

(2) Administrator level access is privileged and must be restricted to authorized IT personnel only. All privileged access accounts are subject to additional security, including multi-factor authentication, and enhanced auditing and logging of activity.

(3) Local accounts must 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.

--

History: Adopted on July 12, 2017.
URL: https://nitc.nebraska.gov/standards/8-502.pdf

8-503. Minimum server configuration.

The state recognizes the National Institute of Standards and Technology (NIST) along with Center for Internet Security (CIS) Controls and Benchmarks as sources for recommended security requirements that provide minimum baselines of security for servers.

NIST and CIS provide instructions, recommendations, and considerations to assist readers in deploying servers in a secure method. All state system administrators should examine NIST and CIS Control documents when installing or configuring servers. The documents are not all inclusive, but rather meant as a means of prompting and guiding administrators through the installation process.

Agencies must comply with the following NIST standards, guidelines, and checklists: NIST SP 800-53, Security and Privacy Controls for Information Systems and Organizations; NIST SP 800-70, National Checklist Program for IT Products; and NIST SP 800-44, Guidelines on Securing Public Web Servers. Agencies should also strive to implement the highest tier possible for the CIS Controls and Benchmarks.

Server Hardening. All State of Nebraska servers are required to be hardened according to these standards. In addition, these servers must have a published configuration management plan as defined below and approved by the Office of the CIO. The following are server hardening standards:

(1) Servers may not be connected to the state network until approved by the Office of the CIO. This approval will not be granted for servers until these hardening standards have been met or risk levels have been accepted by agency management;

(2) The operating system must be installed by authorized IT personnel only, and all vendor supplied patches must be applied. All software and hardware components must be currently supported by the vendor. All unsupported hardware and software components must be identified and have a management plan for replacement that is approved by the Office of the CIO;

(3) All unnecessary software, system services, system and admin accounts, and drivers must be removed or disabled unless doing so would have a negative impact on the server;

(4) Logging of auditable events, as defined in NIST SP 800-53 control objectives, will be enabled. Audit logs will be secured and only accessible to accounts with privileged access and retained for a minimum of one year or be retained in accordance with federal and state guidance;

(5) Security parameters and file protection settings must be established, reviewed, and approved by the Office of the CIO;

(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 the agency and as referenced in the National Vulnerability Database (https://nvd.nist.gov);

(7) Servers will be scanned monthly for unauthorized software or unauthorized changes to the configuration baselines;

(8) Servers will be monitored with active intrusion detection, intrusion protection, and end-point security monitoring that has been approved by the state information security officer. This monitoring must have the capability to alert IT administrative personnel within 1 hour;

(9) Servers must 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 significant changes to servers must go through a formal change management and testing process to ensure the integrity and operability of all security and configuration settings. Significant changes must have a documented security impact assessment included with the change;

(11) Remote management of servers must be performed over secured channels only. Protocols that do not actively support approved encryption, such as telnet, VNC, and RDP, should only be used if they are performed over a secondary encryption channel, such as TLS; and

(12) Agencies must implement prevention techniques to protect against unauthorized data mining of information from public facing systems (e.g. Captcha).

--

History: Adopted on July 12, 2017. Amended on July 8, 2021.
URL: https://nitc.nebraska.gov/standards/8-503.pdf

8-504. 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 Office of the CIO is responsible for maintaining these standards and for configuring and managing the hardware, software, and imaging processes for all managed workstations. Workstation standards should be securely maintained and stored in a centralized documentation library. The degree of protection of the workstation should be commensurate with the data classification of the resources stored, accessed, or processed from this computer. The following are minimum workstation configuration standards:

(1) Endpoint security (anti-virus) software, approved by the Office of the CIO, must be installed and enabled;

(2) The host-based firewall must be enabled if the workstation is removed from the state 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) Web browsers settings should be selected or disabled as appropriate to increase security and limit vulnerability to intrusion;

(8) 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;

(9) Shared login accounts are forbidden on multi-user systems where the manipulation and storage of CONFIDENTIAL or RESTRICTED information takes place;

(10) Users need to lock their desktops when not in use. The system must automatically lock a workstation after 5 minutes of inactivity;

(11) 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 may 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;

(12) All workstations shall be re-imaged with standard load images prior to re-assignment; and

(13) Equipment scheduled for disposal or recycling must be cleansed following agency media disposal guidelines.

--

History: Adopted on July 12, 2017.
URL: https://nitc.nebraska.gov/standards/8-504.pdf

8-505. Minimum laptop configuration.

In addition to the requirements contained in section 8-504, all laptops that connect to the state network are required to meet the following requirements:

(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 must be logged for audit purposes;

(3) Remote access users are responsible for all actions incurred during their session in accordance with all state 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; and

(5) Laptops with remote access to, or the capability to store, CONFIDENTIAL or RESTRICTED data are required to be fully encrypted using technology approved by the state information security officer.

--

History: Adopted on July 12, 2017.
URL: https://nitc.nebraska.gov/standards/8-505.pdf

8-506. Minimum mobile device configuration.

All mobile computing devices accessing the state network or containing state information must be provisioned to meet these security policies and be approved by the Office of the CIO. All devices that will be connected to the state network must be logged with device type and approval date. The following are minimum mobile device configuration standards:

(1) Mobile computing devices must be shut down or locked when not in use. These devices must 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 should not be shared;

(2) Mobile computing devices and mobile storage devices must not be left in a vehicle unattended;

(3) Storing CONFIDENTIAL or RESTRICTED information on any mobile device or any removable or portable media (e.g., CDs, thumb drives, DVDs) is prohibited unless arrangements and mechanisms for securing the data has been explicitly approved by the state information security officer. In those cases, all mobile computing devices or portable media shall be encrypted using technology that is approved by the state information security officer;

(4) Personally owned mobile devices (e.g., smartphones and tablets) may be used for approved state purposes, including email, when configured to access the state 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) The device must have security settings that block users from changing mandatory settings;

(6) Strong passwords are required, and passwords must change regularly per state policy regarding passwords;

(7) The device must lock after no more than 5 minutes of inactivity and must require the re-entry of a password or PIN code to unlock;

(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, the Office of the CIO must have the capability to remotely locate, lock, and erase the device;

(9) The device should have all data backed up at the state 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 must be properly disposed of using mechanisms approved by the state information security officer. State data must be cleared and devices properly disposed of or recycled. The disposition process is required to be documented and periodically audited; and

(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.

--

History: Adopted on July 12, 2017.
URL: https://nitc.nebraska.gov/standards/8-506.pdf

8-507. System maintenance.

The following are system maintenance standards:

(1) All systems involved in the processing, storage, or access to any CONFIDENTIAL or RESTRICTED information must be maintained per manufacturer specifications. Maintenance personnel must be approved for this activity by the state information security officer and must be briefed on the requirements for protecting sensitive information;

(2) Maintenance activity must 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 the secured environment to which it is assigned, the equipment must be approved for release and validated by the state information security officer that all non-public information has been encrypted, secured, or permanently deleted from the equipment. When equipment is returned, it must 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 must be tested. The Office of the CIO must maintain a list of approved maintenance tools that is reviewed and updated at least annually;

(5) Nonlocal or remote maintenance must be approved in advance by the state information security officer or the Office of the CIO, and must also comply with all agency and Office of the CIO requirements for remote access;

(6) All remote maintenance activity must 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 determined by the agency; and

(9) All vendor supplied software deployed and operational must be currently supported by the vendor.

--

History: Adopted on July 12, 2017.

URL: https://nitc.nebraska.gov/standards/8-507.pdf

ARTICLE 6

APPLICATION SECURITY

Section.

8-601. Application documentation.

To ensure that security is built into applications, 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 must be involved in all phases of the application development life cycle from the requirements definition phase, through implementation and eventual application retirement.

Controls in applications may 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 applications that store, access, or process CONFIDENTIAL or RESTRICTED information must go through a formal change management process. For recurring maintenance of these applications, an abbreviated change management process may suffice if that abbreviated process has been approved by the state information security officer.

--

History: Adopted on July 12, 2017.
URL: https://nitc.nebraska.gov/standards/8-601.pdf

8-602. 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 must be backed up and access restricted to authorized personnel only. Application changes are required to go through a software development life cycle process that ensures the confidentiality of information, and integrity and availability of source and executable code. Application changes must follow the change management process as defined in section 8-202.

--

History: Adopted on July 12, 2017.
URL: https://nitc.nebraska.gov/standards/8-602.pdf

8-603. 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:

(1) Access to compilers, editors and other system utilities must be removed from production systems when not required;

(2) Logon procedures and environmental identification must be sufficiently unique for production testing and development;

(3) 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; and

(4) 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 information security officer, and to implement production-class controls in the applicable test environment to protect that information.

--

History: Adopted on July 12, 2017.
URL: https://nitc.nebraska.gov/standards/8-603.pdf

8-604. Application development.

The following standards are required to be followed for agency developed application software that create, process, or store CONFIDENTIAL or RESTRICTED data:

(1) The agency must establish an 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 must retain a documented history of the change process as it passes through the application development life cycle with documentation securely stored for audit purposes. Documentation should address a review of the following: change summary, justification, and timeline; functionality, regression, integrity, and security test plans and results; security review and impact analysis; documentation and baseline updates; and implementation timeline and recovery plans;

(4) Changes to software applications must be controlled and production installations must be made by personnel assigned to update production libraries. Mechanisms to maintain and ensure the integrity of the application code must 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 agency IT infrastructure must be submitted to the Infrastructure Change Control Team for review, approval, and implementation;

(7) The security requirements of new applications must be established, documented and tested prior to their acceptance and use. The agency information security officer must ensure that acceptance criteria are utilized for new applications and upgrades. Acceptance testing must be performed to ensure security requirements are met prior to the application 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 must have an appropriate warning banner displayed, applicable to the data being accessed (e.g., PHI, FTI, PII);

(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; and

(11) Applications must be configured such that CONFIDENTIAL or RESTRICTED data will be encrypted when transmitted outside the agency internal network.

--

History: Adopted on July 12, 2017.
URL: https://nitc.nebraska.gov/standards/8-604.pdf

8-605. Web applications 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 vendor 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). The following are the security standards for web applications and services:

(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, availability of 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 agency internal network, that information must be encrypted in all cases – whether stored or in transit. Encryption technology must be approved by Office of the CIO;

(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 information security officer. Higher risk or impact applications should be tested annually. This test shall be coordinated and supervised by the state information security officer, agency information security officer, 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; and

(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 (https://www.owasp.org/index.php/Category:OWASP_Guide_Project) and SANS (http://www.sans.org/top25-software-errors/) websites.]

--

History: Adopted on July 12, 2017.
URL: https://nitc.nebraska.gov/standards/8-605.pdf

8-606. Staff use of cloud storage websites.

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 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 state information security officer.

--

History: Adopted on July 12, 2017.
URL: https://nitc.nebraska.gov/standards/8-606.pdf

8-607. Cloud computing.

(1) Cloud computing, defined.

This standard incorporates the following definition from the National Institute of Standards and Technology (NIST SP 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 [not part of the NIST definition]:

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 Office of the CIO.

(2) Standard.

(a) The following table contains the acceptable uses of cloud computing by state 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 must 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 Office of the CIO is required.

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

(c) Exemption for existing services. Cloud computing services in use on December 31, 2017, are exempt from the requirements of this section. 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.

(d) FedRAMP compliance. If the cloud service provider (CSP) does not have an official FedRAMP certification by an accredited third-party assessor organization (3PAO) and the CSP may store or process any CONFIDENTIAL or RESTRICTED data, the following conditions must be met or addressed in an agreement with the CSP:

(i) 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's internal systems;

(ii) Access to the cloud service must require multi-factor authentication based on data classification levels;

(iii) De-provisioning of credentials must occur within two (2) hours of de-provisioning of the internal system credentials;

(iv) Information must be encrypted using IT approved technology for information in transit as well as information stored or at rest;

(v) Encryption key management will be controlled and managed by the state unless explicit approval for key management is provided to CSP/3PH by the agency;

(vi) All equipment removed from service, information storage areas, or electronic media that contained state information must have the 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;

(vii) CSP/3PH must provide vulnerability scanning and testing on a schedule approved by the state information security officer. Results will be provided to agency;

(viii) Patch management of hardware and software at the CSP/3PH are required to meet the same standards that are required at state;

(ix) CSP/3PH must meet all state requirements for chain of custody and information breach notification. CSP/3PH will maintain an incident management program that notifies the state within one (1) hour of a breach;

(x) 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 gency-authorized parties;

(xi) 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 United States. This includes both primary and alternate sites;

(xii) 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.;

(xiii) CSP/3PH's must have SLAs in place that clearly define security and performance standards;

(xiv) CSP/3PH will provide adequate security and privacy training to its associates, and provide the state information security officer with evidence of this training;

(xv) CSP/3PH will provide the state with the functionality to conduct a search of the data to meet public records requests; and

(xvi) 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.

--

History: Adopted on July 12, 2017.
URL: https://nitc.nebraska.gov/standards/8-607.pdf

ARTICLE 7

AUDITING AND COMPLIANCE

Section.

8-701. Auditing and compliance; responsibilities; review.

It is the responsibility of the state information security officer 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 state information security officer and agency information security officer have the responsibility to ensure the overall security program meets state and federal legal requirements.

The state information security officer 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.

An agency review to ensure compliance with this policy and applicable NIST SP 800-53 security guidelines must be conducted at least annually.

The state information security officer may periodically review agency compliance with this policy and the related NIST control framework. Such reviews may include: (1) reviews of the technical and business analyses required to be developed pursuant to this policy; and (2) 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 must be documented in an agency security corrective action plan that shall be made available to the state information security officer as necessary. This 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 Office of the CIO management to ensure acceptable progress is being made on mitigating or remediating security gaps.

--

History: Adopted on July 12, 2017.
URL: https://nitc.nebraska.gov/standards/8-701.pdf

8-702. Awareness and training.

(1) The state 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.

(2) New Hire and Refresher Training. All new hires must complete security training, including information about this policy, as part of their orientation. On an annual basis, all staff must complete a security and privacy training session. The state will maintain records of all attendance for new hire and refresher training.

(3) Periodic Briefings. Management should periodically incorporate information security topics into their meetings with staff. Additionally, the state information security officer may 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.

--

History: Adopted on July 12, 2017.
URL: https://nitc.nebraska.gov/standards/8-702.pdf

8-703. Security reviews; risk management.

(1) This policy is based on the NIST SP 800-53 security controls framework. Pursuant to that framework, the state must 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 state information security officer 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 SP 800-53 security controls, such that over a three-year timeframe all control areas will have been assessed. This review must be conducted for each major system used within the state, and must include all infrastructure and peripheral processes that are used to support state business processes.

(2) Unscheduled Risk Assessments. Unscheduled risk assessments may be performed at the discretion of the state information security officer or agency information security officer, 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.

--

History: Adopted on July 12, 2017.
URL: https://nitc.nebraska.gov/standards/8-703.pdf

8-704. Logging.

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

(1) What activity was performed?

(2) Who or what performed the activity, including on what system the activity was performed?

(3) What the activity was performed on (object)?

(4) When was the activity performed?

(5) What tool(s) was the activity performed with?

(6) What was the status (such as success vs. failure), outcome, or result of the activity?

--

History: Adopted on July 12, 2017.
URL: https://nitc.nebraska.gov/standards/8-704.pdf

8-705. Logging; format, storage, and retention.

The state is required to ensure the availability of audit log information that is subject to federal audit by allocating sufficient audit record storage capacity to meet policy requirements. Office of the CIO 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 must be regularly monitored and reported, and action will be taken to keep an approved level of free space available for use. Automated notification of agency or Office of the CIO personnel must 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 Office of the CIO 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). All system logs must 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 subject to federal audit requirements must be retained for seven years.

--

History: Adopted on July 12, 2017.
URL: https://nitc.nebraska.gov/standards/8-705.pdf

8-706. Logging; auditable events.

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 events should be logged and reviewed on a weekly basis:

(1) Log on and off the system;

(2) Change of password;

(3) All system administrator commands, while logged on as system administrator;

(4) Switching accounts or running privileged actions from another account (e.g., Linux/Unix SU or Windows RUNAS);

(5) Creation or modification of super-user groups;

(6) Subset of security administrator commands, while logged on in the security administrator role;

(7) Subset of system administrator commands, while logged on in the user role;

(8) Clearing of the audit log file;

(9) Startup and shutdown of audit functions;

(10) Use of identification and authentication mechanisms (e.g., user ID and password);

(11) Change of file or user permissions or privileges (e.g., use of suid/guid, chown, su);

(12) Remote access outside of the corporate network communication channels (e.g., modems, dedicated VPN) and all dial-in access to the system;

(13) Changes made to an application or database by a batch file;

(14) Application-critical record changes;

(15) Changes to database or application records, where the application has been bypassed to produce the change (via a file or other database utility);

(16) All system and data interactions concerning FTI;

(17) Additional platform-specific events, as defined by agency needs or requirements;

(18) Detection of suspicious or malicious activity such as from an intrusion detection or prevention system (IDS/IPS), anti-virus system, or anti-spyware system; and

(19) Physical entrance or access to secured and restricted areas or facilities where system and network infrastructure reside.

--

History: Adopted on July 12, 2017.
URL: https://nitc.nebraska.gov/standards/8-706.pdf

8-707. Logging; audit log contents.

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

(1) Type of action (e.g., authorize, create, read, update, delete, and accept network connection);

(2) Subsystem performing the action (e.g., process or transaction name, process or transaction identifier);

(3) Identifiers (as many as available) for the subject requesting the action (e.g., user name, computer name, IP address, and MAC address). Note that such identifiers should be standardized to facilitate log correlation;

(4) Date and time the action was performed, including relevant time-zone information if not in Coordinated Universal Time;

(5) Whether the action was allowed or denied by access-control mechanisms;

(6) Description or reason-codes of why the action was denied by the access-control mechanism, if applicable; and

(7) Depending on the nature of the event that is logged, there may be other information necessary to collect.

--

History: Adopted on July 12, 2017.
URL: https://nitc.nebraska.gov/standards/8-707.pdf

8-708. Logging; audit review, monitoring, findings and remediation.

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

(a) Logs of suspicious activity must be reviewed as soon as possible;

(b) Logs of system capacity and log integrity must be reviewed on a weekly basis;

(c) Logs of privilege access account creation or modification must be reviewed on a weekly basis; and

(d) All other logs must be reviewed at least monthly.

(2) When possible, the agency or Office of the CIO will employ automated mechanisms to alert the Office of the CIO, state information security officer, or agency information security officer when inappropriate or unusual activities with security implications are discovered. Any automation used for log analysis must 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.

(3) All relevant findings discovered because of an audit log review must be listed in the appropriate problem tracking system or the corrective action planning 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 agency management within one week of completion. This report should be considered CONFIDENTIAL information.

--

History: Adopted on July 12, 2017.
URL: https://nitc.nebraska.gov/standards/8-708.pdf

8-709. Logging; application logging review and monitoring.

All state applications must provide 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 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 must be reviewed at least monthly. Corrective actions to address application deficiencies must be managed through the application development process or the applicable corrective action planning process.

--

History: Adopted on July 12, 2017.
URL: https://nitc.nebraska.gov/standards/8-709.pdf

ARTICLE 8

VULNERABILITY AND INCIDENT MANAGEMENT

Section.

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's ability to adequately detect, respond and recover from security incidents.

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 Office of the CIO 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.

--

History: Adopted on July 12, 2017.
URL: https://nitc.nebraska.gov/standards/8-801.pdf

8-802. Incident response plan.

All agencies that process, store, or access CONFIDENTIAL or RESTRICTED information are required to maintain an incident response plan. This plan must 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.

(a) 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). 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 email containing CONFIDENTIAL or RESTRICTED information (e.g. Federal Tax Information, Personally Identifiable Information) sent outside the secured state network is a security incident and should be reported as such.

(b) All security incidents must be reported to the state information security officer, agency management, and the Office of the CIO Service Desk immediately. Security incidents will be tracked by the state information security officer. Any state staff who observe, experience, or are notified of a security incident, should immediately report the situation to the agency information security officer, state information security officer or the Office of the CIO Service Desk, but at the very least to their supervisor. All state management are responsible to ensure that their staff understand that awareness of the incident are to be reported immediately.

(c) State Information Security Officer and Agency Information Security Officer.

The security officers are responsible for assembling, engaging, and overseeing the 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.

Agency information security officers are also responsible for ensuring that all technical areas within the agency have an understanding and ability to meet this standard. They are required to

perform education and training of this standard to all applicable agency personnel, and then test the incident response process annually.

(d) Incident Response Team.

The state information security officer will identify key personnel who will serve as members of the state incident response team. 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 may change from time to time, depending on the nature of the incident and the skills necessary to recover from it. Agencies may also identify additional incident response teams for their specific environment. The state information security officer or agency information security officer 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:

(i) The state's priority is "prevention over forensics." In other words, do not allow a damaging incident to continue so that additional evidence may be collected;

(ii) Conduct the initial triage. Perform a damage and impact assessment and document the findings;

(iii) Report to agency management on a regular schedule with status and action plans;

(iv) Maintain confidentiality of the circumstances around the incident;

(v) Follow procedures to maintain a chain of trust and to preserve evidence;

(vi) Initiate the root cause analysis; bring in other resources as necessary; and

(vii) Initiate return to normal operations; bring in other resources as necessary.

(e) 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 should be carefully managed and controlled by the Office of the CIO and agency senior management. All personnel involved in an incident management support activity will communicate only with the parties necessary for incident analysis or recovery activity, and to the state information security officer, Office of the CIO, or the agency information technology team. No other communication, unless explicitly authorized, is allowed.

A security incident report is classified as RESTRICTED information.

(f) Incident Management Training and Testing.

Annually, the state information security officer and agency information security officers 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 will simulate a variety of security related incidents.

(2) 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 will be conducted by the state information security officer/agency information security officer, Office of the CIO Service 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 state information security officer/agency information security officer 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 state information security officer/agency information security officer and IT management may quarantine any potentially threatening system and terminate any threatening activity. The state information security officer 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 state information security officer, Office of the CIO, agency information security officer, 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 state information security officer or the incident response team. They will determine if the incident impacts organizations outside of the agency'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 agency management, state information security officer, and agency information security officer is required. Agency management 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), will 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.

(3) Incident Containment.

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 state information security officer has the authority to coordinate with the Office of the CIO 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 Office of the CIO 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.

(4) Incident Communication.

Reportable conditions, such as the breach of PHI, PII or FTI, require notification within specific timeframes as defined in state and federal law. It is the responsibility of the state information security officer and agency information security officers to understand these requirements and ensure the state and agency remain 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 state information security officer, agency information security officer, Office of the CIO, and agency management to ensure that all communication regarding any security incident is managed and controlled.

(5) 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 will work with law enforcement to secure the potential evidence without reviewing additional content. Network hardware, software or data may be considered potential evidence.

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 agency information 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 (e.g., opening files, deleting, rebooting);

(e) Dump memory contents to a file;

(f) Label all evidence; and

(g) Log all steps.

(6) 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.

A formal root cause analysis must be performed within two weeks of the occurrence of the incident. This analysis should 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.

(7) 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 will be limited to authorized personnel until the security incident has been

contained and root cause mitigated. Analysis and mitigation procedures must be completed as soon as possible, recognizing state systems are vulnerable to other occurrences of the same type.

The Office of the CIO, state information security officer, and agency information security officer shall define and prioritize the requirements to be met before returning an affected or compromised system to normal operations.

Recovery procedures:

(a) Reinstalling compromised systems from trusted backup-ups, if required;

(b) Reinstalling system user files, startup routines, or settings from trusted versions or sources, if required;

(c) Validating restored systems through system or application regression tests, user verification, penetration tests, and vulnerability testing and test result comparisons; and

(d) Increasing security monitoring and heighten awareness for a recurrence of the incident.

--

History: Adopted on July 12, 2017. Amended on March 12, 2020.
URL: https://nitc.nebraska.gov/standards/8-802.pdf

8-803. 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 CIO 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 to minimize the possibility of disruption. Any other attempts to perform tests or scans will be deemed an unauthorized access attempt.

--

History: Adopted on July 12, 2017.
URL: https://nitc.nebraska.gov/standards/8-803.pdf

8-804. 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 CIO 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 Office of the CIO 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.

--

History: Adopted on July 12, 2017.
URL: https://nitc.nebraska.gov/standards/8-804.pdf

8-805. 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.

--

History: Adopted on July 12, 2017.
URL: https://nitc.nebraska.gov/standards/8-805.pdf

8-806. Security deficiencies.

All security deficiencies reported or identified in any security review, scan, assessment, or analysis must be documented in the state or agency plan of action and milestones report. These gaps must be managed to mitigation, remediation, or approved risk acceptance.

--

History: Adopted on July 12, 2017.
URL: https://nitc.nebraska.gov/standards/8-806.pdf

ARTICLE 9

DATA SECURITY

Section.

8-901. State data.

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, irrespective of the medium on which the data resides and regardless of format.

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 any applicable 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, how it is stored, and who has access.

--

History: Adopted on July 12, 2017.
URL: https://nitc.nebraska.gov/standards/8-901.pdf

8-902. Data classification categories.

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

(1) 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, and privileged administrator credentials. This level requires internal security protections and could have a high impact in the event of an unauthorized data disclosure;

(2) 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, and personally identifiable information (PII);

(3) 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. This data may also be data that is sold; and

(4) PUBLIC. This classification is for information that requires no security and can be handled in the public domain.

--

History: Adopted on July 12, 2017.
URL: https://nitc.nebraska.gov/standards/8-902.pdf

8-903. Data inventory.

Each agency shall identify and classify all information according to this policy. Each agency shall maintain an inventory of where CONFIDENTIAL and RESTRICTED information reside, so those environments can be assessed for security adequacy.

--

History: Adopted on July 12, 2017.
URL: https://nitc.nebraska.gov/standards/8-903.pdf

8-904. Data security control assessment.

Each agency shall perform a security control assessment that assesses the adequacy of security controls for compliance with this policy and any applicable security frameworks (e.g., NIST, PCI, CMS, and IRS). The assessment may be performed internally by the agency information security officer or with the assistance of the state information security officer. Each agency is required to have an assessment at least once every year, covering at least one-third 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.

--

History: Adopted on July 12, 2017.
URL: https://nitc.nebraska.gov/standards/8-904.pdf

8-905. Data 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 Office of the CIO are required to have a security program that meets this policy. The agency information security officer shall develop a system security plan that must be approved by the state information security officer. 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 state information security officer, an approved and signed interconnection system agreement that describes the security controls and plans will be in place to protect state information.

--

History: Adopted on July 12, 2017.
URL: https://nitc.nebraska.gov/standards/8-905.pdf

8-906. Data destruction.

Agency data must be disposed of in accordance with the Records Management Act and any related records retention schedule. Disclosure of sensitive information through careless disposal or re-use of equipment presents a risk to the state. 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, and memory sticks) regardless of physical form or format containing CONFIDENTIAL or RESTICTED information must be physically destroyed or securely overwritten when the data contained on the device is to be disposed. 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) when any significant change occurs.

--

History: Adopted on July 12, 2017.
URL: https://nitc.nebraska.gov/standards/8-906.pdf