State Government Council
of the
Nebraska Information Technology Commission

Thursday, September 6, 2007
1:30 p.m. - 2:30 p.m.
Nebraska State Office Building - Lower Level C
301 Centennial Mall South
Lincoln, Nebraska

AGENDA

Meeting Documents: Click the links in the agenda
or click here for all documents.

1. Roll Call, Meeting Notice & Open Meetings Act Information

2. Public Comment

3. Approval of Minutes - August 9, 2007 [Note: Approval of the August minutes will appear on the October meeting agenda.]

4. Standards and Guidelines

- Recommendations to the Technical Panel and NITC*
  - Information Security Policy (Comment Draft Version | Revised Version)
  - Data Security Standard (Comment Draft Version | Revised Version)
  - Password Standard (Comment Draft Version)
  [Comments Received through 8/30/2007 and Comments from Informational Meetings]

- Update
  - Email Standard for State Government Agencies

5. Other Business

6. Agency Reports

7. Next Meeting Date - October 11, 2007

8. Adjourn

* Denotes action items.

(The Council will attempt to adhere to the sequence of the published agenda, but reserves the right to adjust the order of items if necessary and may elect to take action on any of the items listed.)

NITC and State Government Council Websites: http://www.nitc.state.ne.us/
Meeting notice posted to the NITC Website: 16 AUG 2007
Meeting notice posted to the Nebraska Public Meeting Calendar: 16 AUG 2007
Agenda posted to the NITC Website: 31 AUG 2007

NEBRASKA TECHNOLOGY COMMISSION

STANDARDS AND GUIDELINES

Information Security Policy

Category	Security Architecture
Title	**Information Security Policy**
Number	

Applicability

☑ State Government Agencies

- ☐ **All**……Not Applicable
- ☑ **Excluding** Higher Education institutions ……Standard

☐ State Funded Entities - **All entities receiving state funding for matters covered by this document**…… ..... Not Applicable

☑ Other: **All Public Entities**..... Guideline

Definitions:
Standard - Adherence is required. Certain exceptions and conditions may appear in this document, all other deviations from the standard require prior approval of the NITC Technical Panel.
Guideline - Adherence is mandatory.

Status	☐ Adopted ☐ Draft ☑ Other: Reviewed
Dates	Date: January 23, 2001 Date Adopted by NITC: October 31, 2000 Last Review Date: Ma

TABLE OF CONTENTS

Deleted:  . 1¶
NEBRASKA TECHNOLOGY COMMISSION . 1¶
STANDARDS AND GUIDELINES . 1¶
TABLE OF CONTENTS . 2¶
PURPOSE . 4¶
SCOPE . 4¶
APPLICABILITY . 5¶

Deleted: PART

Deleted: SECTION 1. OPERATIONAL ROLES AND FUNCTIONAL RESPONSIBILITIES . 6¶

Deleted: PART

Deleted: SECTION 2. STATE OF NEBRASKA INFORMATION . 7¶
Management of the Confidentiality, Integrity, and Availability of State Information . 7¶
Sharing Information Outside the Agency . 7¶

Deleted: PART

Deleted: SECTION 3. PERSONNEL ACCOUNTABILITY AND SECURITY AWARENESS . 8¶
Individual Accountability . 8¶
Agency Accountability . 8¶
Including Security in Job Responsibilities . 9¶
User Training . 9¶
Separation of Duties . 9¶

Deleted: PART

Deleted: SECTION 4. COMPLIANCE . 9¶
Managing Compliance . 9¶
Monitoring . 10¶
Incident Response . 10¶

Deleted: PART

Deleted: SECTION 5. PHYSICAL AND ENVIRONMENTAL SECURITY . 10¶
Physical Security Perimeter . 10¶
Equipment Security . 11¶ ... [1]

Deleted: PART

Deleted: SECTION 6. ASSET CLASSIFICATION . 12¶

Deleted: PART

Deleted: SECTION 7. ACCESS CONTROL . 13¶ ... [2]

Deleted: PART

Deleted: SECTION 8. OPERATIONAL MANAGEMENT . 15¶ ... [3]

Deleted: PART

Deleted: SECTION 9. SYSTEM DEVELOPMENT AND MAINTENANC ... [4]

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, availability and privacy of State of Nebraska information collected, stored, and used to serve the citizens of the State of Nebraska. This Information Security Policy contains the minimum safeguards, responsibilities and acceptable behaviors required to establish and maintain a secure environment.

The Information Security Policy is based upon the ISO 27002 standard framework and is designed to comply with applicable laws and regulations; including the Records Management Act (Neb. Rev. Stat. § 84-1201 - 1227), however, if there is a conflict, applicable laws and regulations take precedence.

This Information Security Policy sets the direction, gives guidance, and defines requirements for information security processes and actions across agencies. This policy documents many of the security practices already in place in some agencies.

Deleted: broad

The primary objectives are to:

- effectively manage the risk of exposure or compromise to State resources;
- communicate the responsibilities for the protection of information;
- establish a secure, resilient processing environment;
- provide security controls for internally developed software to protect unauthorized access, tampering, or programming errors;
- provide a formal incident management processes; and
- promote and increase the awareness of information security.

SCOPE

This policy is applicable to State of Nebraska full time and temporary employees, third party contractors and consultants, volunteers and other agency workers (hereafter referred to as "Staff"). The Nebraska Information Technology Commission (hereafter referred to as the "NITC") is fully committed to information security and agrees that all staff or any other person working on behalf of the State of Nebraska have important responsibilities to continuously maintain the security and privacy of agency data.

This policy applies to all State Agencies, Boards and Commissions (hereafter referred to as "Agency"). Any agency may enact stronger security safeguard requirements, as necessary, to meet their individual business needs, State or Federal regulations. Where conflicts exist between this policy and an agency's policy, the more restrictive policy shall take precedence.

This Information Security Policy encompasses all systems, automated and manual, for which the State has administrative responsibility, including systems managed or hosted by third parties on behalf of an agency. This policy, subject to the provisions of the Records Management Act, applies to information in all forms, including but not limited to paper, microfilm, and electronic formats, created or used in support of business activities of the agency. This policy must be communicated to all staff that have access to or manage agency information.

Guidelines and standards, published by the NITC, which are associated with this policy, provide specific details for compliance with this mandatory Information Security Policy. Published guidelines and standards reflect current practices and will be periodically reviewed and updated as necessary to meet changes in business needs, State or Federal regulations, or changes in technology implemented or supported by the State of Nebraska.

APPLICABILITY

The NITC has statutory responsibility to adopt minimum standards and guidelines for acceptable and cost-effective use of information technology, and to provide strategic direction for State agencies and educational institutions for information technology. This Information Security Policy will be implemented to ensure uniformity of information protection and security management across the different technologies deployed within an agency.

The Secretary of State (State Records Administrator) has statutory responsibility to establish standards, procedures, and techniques to assist agencies in identifying essential records, and guide them in the establishment of schedules for the creation, preservation, and disposal of such records.

POLICY

The components of this Information Security Policy encompass: 1) Operational Roles and Functional Responsibilities, 2) Management of the confidentiality, integrity and availability of State of Nebraska Information, 3) Personnel Accountability and Security Awareness, 4) Compliance, 5) Physical and Environmental Security, 6) Asset Classification, 7) Access Control, 8) Operational Management, and 9) System Development and Maintenance.

Section 1. Operational Roles and Functional Responsibilities

Deleted: Part

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

State Agencies: Management will ensure that an information security organization structure is in place to:

Formatted: Indent: Left: 0"

- appoint, designate or hire an Information Security Officer to serve as the primary agency point of contact to the State Information Security Officer;
- implement information security policies, procedures and standards as necessary to meet security requirements imposed on the agency by federal, state or local regulations and as promulgated by the NITC;
- assign information security responsibilities;
- implement a security awareness program;
- monitor exposure and implement appropriate safeguards of information assets;
- monitor and implement changes to meet legal or regulatory requirements;
- respond to security incidents; and
- develop a process to measure compliance with this policy.

Formatted: Indent: Left: 0", Tabs: 0.25", List tab + Not at 0.63"

As required by this policy, an Agency Information Security Officer must be designated to oversee all security-related events and information. Depending on the agency's size and complexity, this role may be a fulltime position. The Agency Information Security Officer may report to the Agency Management.

Formatted: Indent: Left: 0"

Office of Chief Information Officer: The Chief Information Officer is the executor of this Information Security Policy, which establishes and monitors the effectiveness of information security, standards and controls within the State of Nebraska. The State Information Security Officer, operating through the Office of the Chief Information Officer, performs as a security consultant to agencies and Agency Information Security Officers. The Office of the CIO may also perform periodic reviews of agency security for compliance with this and other security policies and standards.

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

Formatted: Indent: Left: 0"

The **NITC Technical Panel**, with advice from the Security Work Group, has responsibility for recommending security policies and guidelines and making available best practices to operational entities.

For additional roles and responsibilities that an agency may adopt, see Addendum A.

Section 2. State of Nebraska Information

State information is a valuable asset and must be protected from unauthorized disclosure, modification, or destruction. Prudent information security policies, standards, and practices must be implemented to ensure the confidentiality, integrity, and availability of State information is not compromised.

Management of the Confidentiality, Integrity, and Availability of State Information

The confidentiality, integrity, and availability of State of Nebraska information is critical to support an agency's business activities. Security controls provide the necessary physical, logical and procedural safeguards to protect State resources.

All information, regardless of the form or format, which is created, acquired or used in support of State of Nebraska's business activities, must be used for official business only. Agency information is an asset and must be protected from its creation through its useful life, and to its authorized disposal in accordance with the Records Management Act and your agency's retention schedule. State information must be maintained in a secure, accurate, and reliable manner and be readily available for authorized use. Information must be classified and protected based on its importance to business activities, risks, and security best practices. (See NITC Data Security Standard.)

Sharing Non-public Information Outside the Agency

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

- evaluates and documents the sensitivity of the information to be released or shared;
- identifies the responsibilities of each party for protecting the information;
- defines the minimum controls required to transmit and use the information;
- records the measures that each party has in place to protect the information;
- defines a method for compliance measurement;
- provides a signoff procedure for each party to accept responsibilities;
- establishes a schedule and procedure for reviewing the controls (Refer to Section 6. Asset Classification).

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

Deleted: Part

Formatted: Indent: Left: 0"

Deleted: state

Deleted: ¶

Formatted: Heading 3, Indent: Left: 0", First line: 0"

Formatted: Indent: Left: 0"

Formatted: Indent: Left: 0"

Deleted: Sensitive or confidential

Deleted: information owner

Deleted: D

Deleted: O

Deleted: Sensitive

- critical infrastructure assets which are so vital that their infiltration, incapacitation, destruction or misuse could have a debilitating impact on health, welfare or economic security of the citizens and businesses of the State of Nebraska
- data that identifies specific structural, operational, or technical information, such as: mechanical or architectural drawings, floor plans, operational plans or procedures, or other detailed information relating to electric, natural gas, steam, water supplies, nuclear or telecommunications systems or infrastructure, including associated facilities;
- personal identifying information as defined under Neb. Rev. Stat. § 87-802.

Section 3. Personnel Accountability and Security Awareness

Deleted: Part

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

Individual Accountability

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

Formatted: Indent: Left: 0"

Deleted: information owner

Deleted: D

Deleted: O

Associated with each UserID is an authentication token, such as a password or pin, which must be used to authenticate the person accessing the data, system or network. These authentication tokens or similar technology must be treated as confidential information, and must not be shared or disclosed. *(Refer to Section 7. Access Control and, NITC Individual Use Policy).*

Deleted: *Part*

Agency Accountability

Deleted: ¶

Formatted: Heading 3, Indent: Left: 0"

Formatted: No underline

Formatted: Indent: Left: 0"

All agency information must be protected from unauthorized access to help ensure the information's confidentiality and maintain its integrity. As with other assets, not all information has the same use or value, and therefore information requires different levels of protection. Each agency will follow established data classification processes in accordance with the NITC Security Officer's Handbook, best practices, State directives, and legal and regulatory requirements, as determined by the appropriate levels of protection and classification of that information. All information will be classified and managed based on its confidentiality, integrity, and availability characteristics as defined in the *NITC Security Officer Handbook*.

Deleted: sensitivity

Formatted: Indent: Left: 0"

Formatted: Indent: Left: 0"

To ensure interruptions to normal agency business operations are minimized and critical agency business applications and processes are protected from the effects of major failures, each agency, in cooperation with the Chief Information Officer, must develop disaster recovery and business continuity plans that meet the recovery requirements defined by the agency. Preservation of critical data and software must be performed regularly and stored properly. Appropriate processes

Deleted: backup

Deleted: Back-ups

will be defined in the agency's recovery plan to ensure the reasonable and timely recovery of all information, applications, systems and security regardless of platform or physical form or format, should that information become corrupted, destroyed, or unavailable for a defined period. *(Refer to NITC Information Technology Disaster Recovery Plan Standard)*

Including Security in Job Responsibilities

Specific security roles and responsibilities for those individuals responsible for information security must be documented. *(See Addendum A and Addendum B for specific roles and responsibilities).*

User Training

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. *(See NITC Individual Use Standard)*. Technical staff must be trained to a level of competence in information security that matches their duties and responsibilities. (See NITC Education, Training & Awareness Policy)

Separation of Duties

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

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

Section 4. Compliance

Managing Compliance

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

Deleted: ¶

Deleted: ¶

Deleted: Part

Formatted: Font: Times New Roman, No underline

Formatted: Indent: Left: 0", Space Before: 12 pt

Formatted: Indent: Left: 0"

An agency review to ensure compliance with this policy must be conducted at least annually and each Agency management will certify and report the agency's level of compliance with this policy in accordance with the NITC Data Security Standard.

The State Information Security Officer may periodically review Agency compliance with this policy. Such reviews may include, but are not limited to, reviews of the technical and business analyses required to be developed pursuant to this policy, and other project documentation, technologies or systems which are the subject of the published policy or standard.

Monitoring

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

Only individuals with proper authorization from the Office of the Chief Information Officer will be permitted to use "sniffers" or similar technology on the network to monitor operational data and security events on the State network. Network connection ports should be monitored for unknown devices and un-authorized connections.

Incident Response

Agencies must identify incident response procedures to promote effective response of security incidents, including procedures for information system failure, denial of service, disclosure of confidential information and compromised systems, according to the NITC Incident Response and Reporting Procedure for State Government.

To ensure quick, orderly, and effective responses to security incidents, all users of agency systems must be made aware of the procedure for reporting security incidents, threats or malfunctions that may have an impact on the security of State information. ***Users must not attempt to prove a suspected weakness unless specifically authorized by the agency to do so*.**

Note: Access authorization for user accounts involved in a compromise may be suspended during the time when a suspected violation is under investigation.

Section 5. Physical and Environmental Security

Physical Security Perimeter

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

Formatted: Indent: Left: 0"
Formatted: Indent: Left: 0.13"
Formatted: Indent: Left: 0"
Formatted: No underline
Formatted: Indent: Left: 0"
Formatted: Indent: Left: 0"
Formatted: Indent: Left: 0.13"
Formatted: Indent: Left: 0"
Deleted: qualified agency staff or third party
Formatted: No underline
Formatted: Indent: Left: 0"
Formatted: Indent: Left: 0"
Formatted: Indent: Left: 0.38"
Formatted: Indent: Left: 0"
Deleted: Part
Formatted: No underline
Formatted: Indent: Left: 0"
Formatted: Indent: Left: 0"

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 sensitive information may be printed, 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 security 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 other physical barrier.

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

Equipment Security

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

To provide accountability regarding physical computing assets, an up-to-date inventory of all State hardware and software must be maintained.

Secure Disposal or Re-use of Storage Media and Equipment

Disclosure of sensitive information through careless disposal or re-use of equipment presents a risk to the State of Nebraska. Formal procedures must be established to minimize this risk. Storage devices such as hard disk drives, paper or other storage media (e.g. tape, diskette, CDs, DVDs, USB drives, cell phones, memory sticks, digital copiers/printers with data storage capabilities) regardless of physical form or format containing sensitive information (Refer to Section 6 Asset Classification) must be physically destroyed or securely overwritten when the data contained on the device is no longer required under the provisions of the Records Management Act.

Clear Screen

To prevent unauthorized access to information, agencies will implement automated techniques or controls to require authentication or re-authentication after a predetermined period of inactivity for desktops, laptops, PDA's and any other computer systems where authentication is required. These controls may include such techniques as password protected screen savers, automated logoff processes, or re-authentication after a set time out period.

Section 6. Asset Classification

Formatted: Indent: Left: 0"

Formatted: No underline

Formatted: Indent: Left: 0"

Formatted: Indent: Left: 0"

Deleted: , in accordance with DAS fixed asset guidelines

Formatted: No underline

Formatted: No underline

Formatted: Indent: Left: 0"

Formatted: Indent: Left: 0"

Formatted: No underline

Formatted: Indent: Left: 0"

Formatted: No underline

Formatted: Indent: Left: 0"

Deleted: Part

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

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

Deleted: information owner

Deleted: D

Deleted: O

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

- Public
- Internal Use Only
- Confidential
- Highly Restricted

~~When classifying data, agencies need to consider:~~

Formatted: Strikethrough

- ~~*Sensitivity of the data.*~~
  - ~~Consider disclosure, damage, loss of information, and potential impact on operations.~~

- ~~*Regulated/ legal and contractual obligations and penalties.*~~
  - ~~Consider the minimum level of classification required to which the law or contract applies, e.g. Personally Identifiable Information (PII) or Personal Health Information (PHI) is regulated by the Gramm Leach Bliley Act (GLB), Health Insurance Portability Accountability Act (HIPAA), or Family Educational Rights and Privacy Act (FERPA).~~

Formatted: Font: Not Bold, Strikethrough

Deleted: ~~GLB~~

Formatted: Strikethrough

Formatted: Font: Not Bold, Strikethrough

Formatted: Strikethrough

Formatted: Font: Not Bold, Strikethrough

Formatted: Strikethrough

- ~~*Standards and guidelines.*~~
  - ~~Consider "best practices" identified by information security professionals or other NITC standards and guidelines.~~

- ~~*Information lifecycle.*~~
  - ~~Consider the effects of the classification over time.~~

- ~~*Confidentiality*~~
  - ~~Consider the impact of unauthorized disclosure.~~

- ~~*Integrity*~~
  - ~~Consider the impact of inaccurate and incomplete information~~

- ~~*Availability*~~

- ~~Consider the impact of unavailable information and systems that use it.~~

- ~~*Non-repudiation*~~
  - ~~Consider the impact of not being able to prove the authenticity of an electronic transaction~~

(See NITC Security Officer Handbook)

Section 7. Access Control

To preserve the confidentiality, integrity and availability, state information assets must be protected by logical and physical access control mechanisms.

Logon Banner

Logon banners must be implemented on all workstations, servers and laptops to inform users that the system is for official agency use, or other approved use consistent with agency policy, and that user activities may be monitored, and the user should have no expectation of privacy. Logon banners are usually presented during the authentication process.

User Account Management

A user account management process will be established and documented to identify all functions of user account management, to include the creation, distribution, modification and deletion of user accounts. Data owner(s) are responsible for determining who should have access to information and the appropriate access privileges (read, write, delete, etc.). The "Principle of Least Privilege" should be used to ensure that only authorized individuals have access to applications and information and that these users only have access to the resources required for the normal performance of their job responsibilities. (See NITC Identity and Access Management Standard and NITC Acceptable Use Policy State Data Communication Network)

Agencies or data owner(s) should perform annual user reviews of access and appropriate privileges.

Privileged Accounts Management

The issuance and use of privileged accounts will be restricted and controlled. Processes must be developed to ensure that users of privileged accounts are monitored, and any suspected misuse is promptly investigated.

All individuals requiring special privileges (programmers, database administrators, network and security administrators, etc.) will have a unique privileged account (UserID) so activities can be traced to the responsible user. UserIDs must not give any indication of the user's privilege level, e.g., supervisor, manager, administrator, etc. (See NITC Remote Administration of Internal Devices Standard).

User Password Management

Deleted: Part

Formatted: No underline
Formatted: Indent: Left: 0"
Formatted: Indent: Left: 0"

Formatted: No underline
Formatted: Indent: Left: 0"
Formatted: Indent: Left: 0"

Deleted: Information owner
Deleted: O
Deleted:)

Deleted: information owner
Deleted: D
Deleted: O

Formatted: No underline
Formatted: Indent: Left: 0"
Formatted: Indent: Left: 0"

Formatted: Indent: Left: 0.13"
Formatted: Indent: Left: 0"

Formatted: No underline
Formatted: Indent: Left: 0"

Passwords are a common means of authenticating a user's identity to access information systems or services. Passwords must be implemented to ensure all authorized individuals accessing agency resources follow the NITC Password Standard.

Password management controls should be implemented, where technically or operationally feasible, to provide a reliable, effective method of ensuring the use of strong passwords.

Network Access Control

Access to an agency's trusted internal network must require all authorized users to authenticate themselves through the use of an individually assigned User ID and an authentication mechanism (e.g., password, token, smart card, etc.). Network controls must be developed and implemented that ensure authorized users can access only those network resources and services necessary to perform assigned job responsibilities.

User Authentication for External Connections (Remote Access Control)

In the special case where software, servers, storage devices or other computer equipment has the capability to automatically connect to a vendor (e.g. to report problems or suspected problems), the Agency Information Security Officer or designee must conduct a risk assessment prior to establishing access to ensure that connectivity does not compromise the state or other third party connections.

(See also Section 8. Operational Management, External Connections and NITC Remote Access Standard)

Segregation of Networks

When the state network is connected to another network, or becomes a segment on a larger network, controls must be in place to prevent users from other connected networks access to the agency's private network. Routers or other technologies must be implemented to control access to secured resources on the trusted state network.

Detailed maps of agency physical and logical network connections should be available to the State Information Security Officer.

Operating System

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

In certain circumstances, where there is a clear business requirement or system limitation, the use of a shared UserID/password for a group of users or a specific job can be used. Approval by Agency Information Security Officer or designee must be documented in these cases. The approval process must include the State Information Security Officer. Additional compensatory controls must be implemented to ensure confidentiality and accountability is maintained *(See Section 3. Personnel Accountability and Security Awareness, Individual Accountability).*

Formatted: Indent: Left: 0"
Formatted: No underline
Formatted: Indent: Left: 0"
Formatted: Indent: Left: 0"
Formatted: No underline
Formatted: Indent: Left: 0"
Formatted: Indent: Left: 0"
Formatted: No underline
Formatted: Indent: Left: 0"
Formatted: Indent: Left: 0"
Formatted: Indent: Left: 0"
Formatted: Indent: Left: 0"
Formatted: Indent: Left: 0.13"
Formatted: Indent: Left: 0"
Deleted: Part

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

Application Access Control

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.

Monitoring System Access and Use

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

Section 8. Operational Management

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

Network Management

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

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

Additions or changes to network configurations, including through the use of third party service providers, must be reviewed and approved through the Office of the Chief Information Officer's change management process.

Formatted: Indent: Left: 0"
Formatted: No underline
Formatted: Indent: Left: 0"
Formatted: Indent: Left: 0"
Formatted: No underline
Formatted: Indent: Left: 0"
Formatted: Indent: Left: 0"
Deleted: Part
Formatted: Indent: Left: 0"
Formatted: Indent: Left: 0"
Formatted: Indent: Left: 0"
Formatted: Indent: Left: 0.13"
Formatted: Indent: Left: 0"

Cooperation Between Organizations

The Agency Information Security Officer should maintain contact lists of both internal and external contacts and service providers. These lists should be organized to quickly facilitate security-related events and investigations and should detail the agency management staff authorized to make decisions regarding security-related events.

Membership in security-related organizations may provide valuable insight into the ongoing practices of security administration; however, the release of information regarding State security events and issues is strictly prohibited without Office of the Chief Information Officer prior approval.

Penetration Testing, Intrusion Testing, and 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 agency penetration testing, intrusion testing, and vulnerability scanning.

- All servers will be scanned for vulnerabilities and weaknesses by the Office of the Chief Information Officer before being installed on the State network. For both internal and external systems, scans will be performed at least annually or after any major software or configuration changes have been made, to ensure that no major vulnerabilities have been introduced. The frequency of additional scans will be determined by the agency and the data owner(s)), depending on the criticality and sensitivity of the information on the system.

- 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.

- 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.

Deleted: information owner
Deleted: D
Deleted: O
Deleted: information owner
Deleted: D
Deleted: O

The results of the penetration and intrusion testing, and vulnerability scans 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 and vulnerability scanning must be coordinated by both entities.

Any penetration or intrusion testing or vulnerability scanning, other than that performed by State Information Security Officer must be conducted by individuals who are authorized by the State Information Security Officer and who have requested and received written consent from the Office of the Chief Information Officer at least 24 hours prior to any testing or scanning. Agencies authorized to perform penetration and intrusion testing or

vulnerability scanning must have a process defined, tested and followed at all times to minimize the possibility of disruption. Any other attempts to perform tests or scans will be deemed an unauthorized access attempt.

External Connections

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

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

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.

(See also Section 7. Access Control, User Authentication for External Connections)

Portable Devices

All portable computing devices (notebooks, USB flash drives, PDA's, laptops and mobile phones) and information must be secured to prevent compromise of confidentiality or integrity. No device may store or transmit sensitive information without suitable protective measures that are approved by the agency data owner(s).

Deleted: information owner
Deleted: D
Deleted: O
Deleted:)

Special care must be taken to ensure that information stored on the device is not compromised. Appropriate safeguards must be in place for the physical protection, access control, cryptographic technique, back up, virus protection, and properly connected to the State network.

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

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

Server Hardening

In order to protect State resources, agencies must remove all unnecessary software and disable services in accordance with NITC Minimum Server Configuration Standard.

System Planning

Because system and data availability is a security concern, advance planning and preparation must be performed to ensure the availability of resources. Storage and memory capacity and other hardware requirements must be monitored and future requirements projected to ensure adequate processing and storage capabilities are available when needed. This information will be used to identify and avoid potential bottlenecks that might present a threat to system security or user services.

Protection against Malicious Code

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.

Software Maintenance

All installed software must be maintained at a vendor-supported level to ensure accuracy and integrity. 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 applied in a timely manner as defined by the Agency.

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 that is transmitted over the radio waves (wireless devices) can be intercepted. This represents a potential security issue. Agencies shall take appropriate steps, including the implementation of encryption, user authentication, and virus protection measures, to mitigate risks to the security of State data and information systems associated with the use of wireless network access technologies in accordance with the NITC Wireless Local Area Network Standard.

No wireless network or wireless access point will be installed without the written approval of the Office of the Chief Information Officer.

Communications

Security of Electronic Mail

Electronic mail provides an expedient method of creating and distributing messages both within the organization and outside of the organization. Users of the state E-mail system are a visible representative of the state and must use the system in a legal, professional and responsible manner. Users must comply with this policy, the Records Management Act, and be knowledgeable of their responsibilities as defined in NITC Secure E-Mail for State Agencies.

Telephones and Fax Equipment

Communication outside the state telephone system for business reasons is sometimes necessary, but it can create security exposures. Employees should take care that they are not overheard when discussing sensitive or confidential matters; avoid use of any wireless or cellular phones when discussing sensitive or confidential information; and avoid leaving sensitive or confidential messages on voicemail systems. (See Section 6. Asset Classification and NITC Use of Computer-based Fax Services by State Government Agencies)

Modem Usage

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

Section 9. System Development and Maintenance

Deleted: Part

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

Formatted: Indent: Left: 0"

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

Agencies should follow the latest "best practices" in secure coding techniques as identified in NIST guidelines, OWASP principles, etc.

System Acceptance

Formatted: No underline

The security requirements of new systems must be established, documented and tested prior to their acceptance and use. Agency Information Security Officer or designee will ensure that acceptance criteria are utilized for new information systems and upgrades. Acceptance testing

Formatted: Indent: Left: 0"

will be performed to ensure security requirements are met prior to the system being migrated to the production environment.

Separation of Development, 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. Separation must also be implemented between development and test functions. Each agency must consider the use of a quality assurance environment where user acceptance testing can be conducted. The following controls must be considered:

- access to compilers, editors and other system utilities must be removed from production systems when not required; and
- logon procedures and environmental identification must be sufficiently unique for production testing and development.

Risk Assessment

Security requirements and controls must reflect the value of the information involved, and the potential damage that might result from a failure or absence of security measures. This is especially critical for Internet (Web) and other online applications. The framework for analyzing the security requirements and identifying controls to meet them is associated with a risk assessment, which must be performed by the data owner) and Agency management. A process must be established and implemented for each application to:

- address the business risks and develop a data classification profile to help to understand the risks;
- identify security measures based on the criticality and data sensitivity and protection requirements;
- identify and implement specific controls based on security requirements and technical architecture;
- implement a method to test the effectiveness of the security controls; and
- identify processes and standards to support changes, ongoing management and to measure compliance.

Input Data Validation

An application's input data must be validated to ensure it is correct and appropriate including the detection of data input errors. The checks that are performed on the client side must also be performed at the server to ensure data integrity. Checks will be performed on the input of business transactions, static data (names, addresses, employee numbers, etc.) and parameter tables. A process should be set up to verify and correct fields, characters, and completeness of data and range/volume limits.

Formatted: No underline
Formatted: Indent: Left: 0"
Formatted: Indent: Left: 0"
Formatted: No underline
Formatted: Indent: Left: 0"
Formatted: Indent: Left: 0.13"
Formatted: Indent: Left: 0"
Deleted: information owner
Deleted: D
Deleted: O
Formatted: No underline
Formatted: Indent: Left: 0"
Formatted: Indent: Left: 0.13"
Formatted: Indent: Left: 0"

Control of Internal Processing

Data that has been entered correctly can be corrupted by processing errors or through deliberate acts. Checks and balances must be incorporated into systems to prevent or stop an incorrect program from running. Application design must ensure that controls are implemented to minimize the risk of processing failures leading to a loss of data or system integrity.

Message Integrity

Message integrity must be considered for applications where there is a security requirement to protect the message or data content from unauthorized changes (e.g. electronic funds transfer, EDI transactions, etc.) Encryption techniques should be used as a means of implementing message integrity. *It should be noted that message integrity does not protect against unauthorized disclosure.*

Cryptographic Controls

Use of encryption for protection of high-risk information should be considered when other controls do not provide adequate protection. The decision to use encryption should be based on the level of risk of unauthorized access and the sensitivity of the data to be protected. Consideration must also be given to the regulations and national restrictions that may apply to the use of cryptographic techniques in different parts of the world.

Key Management

Protection of cryptographic keys is essential if cryptographic techniques are going to be used. Access to these keys must be tightly controlled to only those individuals who have a business need to access the keys. Loss of a cryptographic key would cause all information encrypted with that key to be considered at risk.

Protection of System Test Data

Test data is developed to test a comprehensive set of conditions and outcomes, including exception processing and error conditions to demonstrate accurate processing and handling of information and the stability of the software, system or application. Production data may not be used for testing unless all personally identifiable information is removed.

Once test data is developed, it must be protected and controlled for the life of the software, system or application. This protection mechanism is essential to ensuring a valid and controlled simulation with predictable outcomes.

Protection of Source 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.

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,

Formatted: No underline
Formatted: Indent: Left: 0"
Formatted: No underline
Formatted: No underline
Formatted: Indent: Left: 0"
Formatted: No underline
Formatted: Indent: Left: 0"
Formatted: No underline
Formatted: Indent: Left: 0"
Formatted: Indent: Left: 0"
Formatted: No underline
Formatted: Indent: Left: 0.13"
Formatted: Indent: Left: 0"
Formatted: No underline
Formatted: No underline
Formatted: Indent: Left: 0.13"
Formatted: Indent: Left: 0"

systems, software, or procedures. Agency management must formally authorize all changes before implementation and ensure that accurate documentation is maintained. These change control procedures will apply to agency business applications as well as systems software used to maintain operating systems, network software, hardware changes, etc.

DOCUMENT CHANGE MANAGEMENT

Requests for changes to this policy must be presented to the State Information Security Officer. If the State Information Security Officer agrees to the change, he or she will formally draft the change and have it reviewed and approved through the NITC normal policy approval process. Each Agency Information Security Officer will be responsible for communicating the approved changes to their organization.

This policy and supporting policies and standards will be reviewed at a minimum on an annual basis.

CONTACT INFORMATION

Questions concerning this policy may be directed to State Information Security Officer, or (402) 471-7031.

DEFINITIONS

Agency: State agencies, boards and commissions are collectively referred to as 'agency' throughout this document.

Authentication: The process to establish and prove the validity of a claimed identity.

Authenticity: This is the exchange of security information to verify the claimed identity of a communications partner.

Authorization: The granting of rights, which includes the granting of access based on an authenticated identity.

Availability: This is the 'property' of being operational, accessible, functional and usable upon demand by an authorized entity, e.g. a system or user

Biometrics: Refers to the use of electro-mechanical devices that measure some physical, electrical or audio characteristic of an individual and make use of that specific measurement to verify identity.

Business Risk: This is the combination of sensitivity, threat and vulnerability.

Change Management Process: A business process that ensures that no changes occur on a computing resource without having gone through a methodology to ensure that changes will perform as expected, with no unexpected repercussions.

Chief Information Officer: The Chief Information Officer is responsible for vision, strategy, direction, and oversight for Information Technology for State of Nebraska. The Chief Information Officer reports to the Governor, is a member of the Governor's cabinet, and is a member of the Nebraska Information Technology Commission, which oversees and legislates IT standards and policy as empowered by law.

Classification: The designation given to information or a document from a defined category on the basis of its sensitivity.

Computer: All physical, electronic and other components, types and uses of computers, including but not limited to hardware, software, central processing units, electronic communications and systems, databases, memory, Internet service, information systems, laptops, Personal Digital Assistants and accompanying equipment used to support the use of computers, such as printers, fax machines and copiers, and any updates, revisions, upgrades or replacements thereto.

Confidentiality: The property that information is not made available or disclosed to unauthorized individuals, entities, or processes.

Controls: Countermeasures or safeguards that are the devices or mechanisms that are needed to meet the requirements of policy.

Critical: A condition, vulnerability or threat that could cause danger to data, a system, network, or a component thereof.

Data: Any information created, stored (in temporary or permanent form), filed, produced or reproduced, regardless of the form or media, including all records as defined by the Records Management Act.. Data may include, but is not limited to personally identifying information, reports, files, folders, memoranda, statements, examinations, transcripts, images, communications, electronic or hard copy.

Data Security: The protection of information assets from accidental or intentional but unauthorized disclosure, modification, or destruction, or the inability to process that information.

Data Owner: An individual or a group of individuals with responsibility for making classification and control decisions regarding use of information.

Denial of Service: An attack that takes up so much of the company's business resource that it results in degradation of performance or loss of access to the company's business services or resources.

Disaster: A condition in which information is unavailable, as a result of a natural or man-made occurrence, that is of sufficient duration to cause significant disruption in the accomplishment of the State of Nebraska's business objectives.

DMZ: Demilitarized zone; a semi-secured buffer or region between two networks such as between the public Internet and the trusted private State network.

Encryption: The cryptographic transformation of data to render it unintelligible through an algorithmic process using a cryptographic key.

Executive Management: The person or persons charged with the highest level of responsibility for an Agency (e.g. Agency Director, CEO, Executive Board, etc.).

External Network: The expanded use and logical connection of various local and wide area networks beyond their traditional Internet configuration that uses the standard Internet protocol, TCP/IP, to communicate and conduct E-commerce functions.

Family Educational Rights and Privacy Act (FERPA): Federal law regarding the privacy of educational information. For additional information visit: http://www.ed.gov/policy/gen/guid/fpco/ferpa/index.html

Firewall: A security mechanism that creates a barrier between an internal network and an external network.

Gramm-Leach-Bliley Act (GLB): Federal regulation requiring privacy standards and controls on personal information for financial institutions. For additional information visit: http://www.ftc.gov/privacy/privacyinitiatives/glbact.html

Guideline: An NITC document aims to streamline a particular process that Agency compliance is voluntary.

Health Insurance Portability Accountability Act (HIPAA): A Congressional act that addresses the security and privacy of health data. For additional information visit: http://www.hhs.gov/ocr/hipaa/

Host: A system or computer that contains business and/or operational software and/or data.

Incident: Any adverse event that threatens the confidentiality, integrity or accessibility of information resources.

Incident Response: The manual and automated procedures used to respond to reported network intrusions (real or suspected); network failures and errors; and other undesirable events.

Information: Information is defined as the representation of facts, concepts, or instructions in a formalized manner suitable for communication, interpretation, or processing by human or automated means.

Information Assets: (1) All categories of automated information, including but not limited to: records, files, and databases, and (2) information technology facilities, equipment (including microcomputer systems), and software owned or leased by the State.

Information Security: The concepts, techniques and measures used to protect information from accidental or intentional unauthorized access, modification, destruction, disclosure or temporary or permanent loss (See Availability).

Deleted: **Information Owner**

Deleted: **Data Owner:** An individual or a group of individuals that has responsibility for making classification and control decisions regarding use of information.¶

Information Technology Resources: Hardware, software, and communications equipment, including, but not limited to, personal computers, mainframes, wide and local area networks, servers, mobile or portable computers, peripheral equipment, telephones, wireless communications, public safety radio services, facsimile machines, technology facilities including but not limited to, data centers, dedicated training facilities, and switching facilities, and other relevant hardware and software items as well as personnel tasked with the planning, implementation, and support of technology.

Integrity: The property that data has not been altered or destroyed from its intended form or content in an unintentional or an unauthorized manner.

Internet: A system of linked computer networks, international in scope, which facilitates data transmission and exchange, which all use the standard Internet protocol, TCP/IP, to communicate and share data with each other.

Internal Network: An internal (i.e., non-public) network that uses the same technology and protocols as the Internet.

Malicious Code: Malicious Code refers to code that is written intentionally to carry out annoying, harmful actions or use up the resources of a target computer. They sometimes masquerade as useful software or are embedded into useful programs, so that users are induced into activating them. Types of malicious code include Trojan horses and computer viruses.

Nebraska Information Technology Commission (NITC): The governing body, set forth by the State of Nebraska Legislature. See http://www.nitc.state.ne.us/

Penetration Testing: The portion of security testing in which evaluators attempt to exploit physical, network, system or application weaknesses to prove whether these weaknesses can be exploited by gaining extended, unauthorized or elevated privileged access to protected resources.

Personal Information: Personal information means any information concerning a person, which, because of name, number, personal mark or other identifier, can be used to identify such natural person.

Physical Security: The protection of information processing equipment from damage, destruction or theft; information processing facilities from damage, destruction or unauthorized entry; and personnel from potentially harmful situations.

Policy: An NITC document that establishes a set of consistent rules and the means of achieving them that support the business objectives for the State of Nebraska

Principle of Least Privilege: A framework that requires users be given no more access privileges (read, write, delete, update, etc.) to systems than necessary to perform their normal job functions, and those privileges be granted no longer than the time required to perform authorized tasks.

Privacy: The right of individuals and organizations to control the collection, storage, and dissemination of information about themselves.

Private Information: Private Information means personal information in combination with any one or more of the following data elements, when either the personal information or the data element is not encrypted or encrypted with an encryption key that has also been acquired:

- social security number; or
- driver's license number or non-driver identification card number; or
- account number, credit or debit card number, in combination with any required security code, access code, or password which would permit access to an individual's financial account

"Private information" does not include publicly available information that is lawfully made available to the general public from federal, state, or local government records.

Privileged Account: The User ID or account of an individual whose job responsibilities require special system authorization, such as a network administrator, security administrator, etc. Special authorizations are allocated to this account such as RACF Administrator, auditor, Special, UNIX root or Microsoft Administrator, etc.

Procedures: Specific operational steps that individuals must take to achieve goals stated in this policy.

Records Officer: The agency representative from the management or professional level, as appointed by each agency head, who is responsible for the overall coordination of records management activities within the agency.

Records Management Act: The governing statute, set forth by the State of Nebraska Legislature. Neb. Rev. Stat. § 84-1201 through § 84-1228

Risk: The probability of suffering harm or loss. It refers to an action, event or a natural occurrence that could cause an undesirable outcome, resulting in a negative impact or consequence.

Risk Assessment: The process of identifying threats to information or information systems, determining the likelihood of occurrence of the threat, and identifying system vulnerabilities that could be exploited by the threat.

Risk Management: The process of taking actions to assess risks and avoid or reduce risk to acceptable levels.

Security Management: The responsibility and actions required to manage the security environment including the security policies and mechanisms.

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

Separation of Duties: A concept that no individual should have control over two or more phases of an operation or areas of conflicting responsibility.

Sensitive Information: Disclosure or modification of this data would be in violation of law, or could harm an individual, business, or the reputation of the agency.

Sensitivity: The measurable, harmful impact resulting from disclosure, modification, or destruction of information.

Sniffer: Monitoring network traffic.

Staff: Any State of Nebraska full time and temporary employees, third party contractors and consultants who operate as employees, volunteers and other agency workers.

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

State: The State of Nebraska.

State Information Security Officer: The Information Security Officer appointed by the Chief Information Officer to lead the NITC Security Architecture Workgroup. Responsibilities include creating and maintaining polices for the State of Nebraska, conducting vulnerability / penetration tests at an enterprise level, and to assist Agency Information Security Officer's.

State Network: The State of Nebraska's internal, private network, e.g. the State's 10.x.x.x address space.

State Records Administrator: The Secretary of State is the State Records Administrator. The Secretary of State establishes and administers the records management program for all state agencies.

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

System Development Life Cycle: A software development process that includes defining the system requirements, the design specifications, the software development, installation and training, maintenance, and disposal.

Third Party: Any non-agency contractor, vendor, consultant, or external entity, etc.

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

Token: A device that operates much like a smart card but is in a physical shape that makes its use easier to manage.

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

Unauthorized Access Or Privileges: Insider or outsider who gains access to network or computer resources without permission.

User: Any agency (ies), federal government entity (ies), political subdivision(s), their employees or third party contractor(s) or business associates, or any other individual(s) who are authorized by such entities to access a System for a legitimate government purpose.

Virus: A program that replicates itself on computer systems by incorporating itself into other programs that are shared among computer systems. Once in the new host, a virus may damage data in the host's memory, display unwanted messages, crash the host or, in some cases, simply lie dormant until a specified event occurs (e.g., the birth date of a historical figure).

Vulnerability: A weakness of a system or facility holding information that can be exploited to gain access or violate system integrity. Vulnerability can be assessed in terms of the means by which the attack would be successful.

Vulnerability Scanning: The portion of security testing in which evaluators attempt to identify physical, network, system or application weaknesses to discover whether these weaknesses may be exploited by persons or machines seeking to gain either unauthorized or elevated privileged access to otherwise protected resources.

World Wide Web (WWW): A hypertext-based system designed to allow access to information in such a way that the information may physically reside on locally or geographically different servers. This access was greatly improved through the introduction of a graphical interface to the World Wide Web called a web browser. Netscape and Internet Explorer are two of the most popular web browsers.

Worm: A program similar to a virus that can consume large quantities of network bandwidth and spread from one network to another.

INDEX

Deleted: Section Break (Continuous)

 ... [5]

ADDENDUM A

Operational and Functional Responsibilities

Data Owner: An individual or a group of individuals designated by the agency will serve as or represent Data owners for the data and tools they use. Data owners are responsible for determining who should have access to protected resources within their jurisdiction, and what those access privileges should be (read, update, etc.). Data owners also communicate to the Agency Information Security Officer the legal requirements for access and disclosure of their data. Data owners must be identified for all agency information assets and assigned responsibility for the maintenance of appropriate security measures such as assigning and maintaining asset classification and controls, managing user access to their resources, etc. Responsibility for implementing security measures may be delegated, though accountability remains with the identified owner of the asset.

Deleted: Information Owner

Deleted: :

Deleted: information

Deleted: Information

Deleted: Information

Deleted: Information

Data Custodian: An individual or a group of individuals designated by the Data owner who will be responsible for maintaining and protecting the data. This role is typically filled by the IT department, and the duties include performing regular backups of the data, periodic validating the integrity of the data, restoring data from backup media, retaining records of activity, and fulfilling the requirements specified in this Security Policy and NITC standards and guidelines that pertain to information security and data protection.

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

Security Administrators: When such an individual or individuals exist, the individual or individuals will work closely with the Agency Information Security Officer and support staff. Security Administrators are the staff normally responsible for administering security tools, reviewing security practices, identifying and analyzing security threats and solutions, and responding to security violations. This individual or individuals has administrative responsibility over all UserIDs and passwords and the associated processes for reviewing, logging, implementing access rights, emergency privileges, exception handling, and reporting requirements. Where a formal Security Administration function does not exist, the organization or staff responsible for the security administration functions described above will adhere to this policy.

Information Technology (IT) Management: IT management has responsibility for the data processing infrastructure and computing network which support the data owners. It is the

Deleted: information owner

Deleted: D

Deleted: O

responsibility of IT management to support the Information Security Policy and provide resources needed to enhance and maintain a level of information security control consistent with the agency's Information Security Policy.

IT management has the following responsibilities in relation to the security of information:

- ensuring processes, policies and requirements are identified and implemented relative to security requirements defined by the agency's business;
- ensuring the proper controls of information are implemented for which the agency's business have assigned ownership responsibility, based on the agency's classification designations;
- ensuring the participation of the Agency Information Security Officer and technical staff in identifying and selecting appropriate and cost-effective security controls and procedures, and in protecting information assets;
- ensuring that appropriate security requirements for user access to automated information are defined for files, databases, and physical devices assigned to their areas of responsibility;
- ensuring that critical data and recovery plans are backed up and kept at a secured off-site storage facility and that recovery of backed-up media will work if and when needed.

NITC Technical Panel: The NITC Technical Panel, with advice from the Security Work Group, has responsibility for recommending security policies and guidelines and making available best practices to operational entities.

State Records Administrator: The State Records Administrator establishes and administers, within and for state and local agencies, (1) a records management program which will apply efficient and economical methods to the creation, utilization, maintenance, retention, preservation, and disposal of state and local records, (2) a program for the selection and preservation of essential state and local records, (3) establish and maintain a depository for the storage and service of state records, and advise, assist, and govern by rules and regulations the establishment of similar programs in local political subdivisions in the state, and (4) establish and maintain a central microfilm agency for state records and advise, assist, and govern by rules and regulations the establishment of similar programs in state agencies and local political subdivisions in the State of Nebraska. Neb. Rev. State § 84-1203

ADDENDUM B

Role and Responsibilities of the Agency Information Security Officer

The Agency Information Security Officer is responsible for performing, at a minimum, the following tasks:

- coordinate the development and implementation of information security policies, standards, procedures, and other control processes that meet the business needs of the agency;
- provide consultation on the various agency computing platforms;
- work closely with security administration or those serving in that function to ensure security measures are implemented that meet policy requirements;
- evaluate new security threats and counter measures that could affect the agency and make appropriate recommendations to the State Information Security Officer and other appropriate management to mitigate the risks;
- review and approve all external network connections to the agency's network;
- provide consultation to the agency management with regard to all information security;
- investigate and report to appropriate agency management and the State Information Security Officer according to the NITC Incident Reporting Policy;
- ensure that appropriate follow-up to security violations is conducted;
- ensure appropriate information security awareness and education to all agency
- staff, and where appropriate third party individuals;
- be aware of laws and regulations that could affect the security controls and classification requirements of the agency's information;

The mission of the Information Security Function is to:

- develop, deploy and maintain an information security architecture that will provide security policies, mechanisms, processes, standards and procedures that meet current and future business needs of the agency;
- provide information security recommendations to the agency regarding security threats that could affect the agency's computing and business operations, and make recommendations to mitigate the risks associated with these threats;
- assist management in the implementation of security measures that meet the business needs of the agency;
- develop and implement security training and awareness programs that educate agency employees, contractors and vendors with regard to the agency's information security requirements;
- investigate and report to management breaches of security controls, and implement additional compensating controls when necessary to help ensure security safeguards are maintained;
- participate in the development, implementation and maintenance of disaster recovery processes and techniques to ensure the continuity of the agency's business and the security controls, in the event of an extended period of computing resource unavailability;

- although information security roles & responsibilities may be outsourced to third parties, it is the overall responsibility of each agency to maintain control of the security of the information that it owns.

Nebraska Information Technology Commission

STANDARDS AND GUIDELINES

Data Security Standard

Category	**Security Architecture**
Title	**Data Security Standard**
Number	

Applicability

☑ State Government Agencies
- ☐ **All** ..... Not Applicable
- ☑ **Excluding higher education institutions** .....Standard

☐ State Funded Entities - **All entities receiving state funding for matters covered by this document** ..... Not Applicable

☑ Other: **All Public Entities**..... Guideline

Definitions:
Standard - Adherence is required. Certain exceptions and conditions may appear in this document, all other deviations from the standard require prior approval of _____.
Guideline - Adherence is voluntary.

Status	☐ **Adopted** ☐ **Draft** ☐ **Other:**_____
Dates	**Date:** **Date Adopted by NITC:** **Other:**

Prepared by: Technical Panel of the Nebraska Information Technology Commission
Authority: Neb. Rev. Stat. § 86-516(6)
http://www.nitc.state.ne.us/standards/

1.0 Standard

It is the responsibility of all State of Nebraska agencies to protect all information stored in electronic form against unauthorized access.

2.0 Purpose and Objectives

In the normal course of business operations information is gathered, stored and transmitted in electronic form. This information is normally required to provide public services or to carry out other state business responsibilities. Information collected may be of a nature deemed confidential to the business process being carried out and as such not open to sharing with any other entity. Certain types of data may also be deemed personal information. It is the objective of this policy to provide safeguards to protect that information.

Common methods of protecting information include, but are not limited to:

- Staff education
- Restricted data access and usage
- Administrative policies and procedures
- Data encryption
- Network encryption
- Account authorization
- Strong passwords
- Biometric authentication
- Physical security
- Network Firewalls
- Server hardening

3.0 Applicability

3.1 State Government Agencies

All State agencies, boards, and commissions are required to comply with the standard listed in Section 1.0.

3.2 Exemption

Exemptions may be granted by the NITC Technical Panel upon request by an agency.

3.2.1 Exemption Process

Any agency may request an exemption from this standard by submitting a “Request for Exemption” to the NITC Technical Panel. Requests should state the reason for the exemption. Reasons for an exemption include, but are not limited to: statutory exclusion; federal government requirements; or financial hardship. Requests may be submitted to the Office of the NITC via e-mail or letter (Office of the NITC, 501 S 14th Street, Lincoln, NE 68509). The NITC Technical Panel will consider the request and grant or deny the exemption. A denial of an exemption by the NITC Technical Panel may be appealed to the NITC.

4.0 Responsibility

4.1 NITC

The NITC shall be responsible for adopting minimum technical standards, guidelines, and architectures upon recommendation by the technical panel. (Neb. Rev. Stat. § 86-516(6))

4.2 State Agencies

Each state agency will be responsible for ensuring that all information stored in an electronic manner is protected with appropriate safeguards in a manner consistent with this standard and any other applicable security policies.

Each state agency will designate a data owner for each application or system who will be responsible for assigning the data classification according to the sensitivity and criticality of the information in accordance with the NITC Security Officer Handbook, and making all decisions regarding controls, access privileges, and information management.

Each state agency is responsible for ~~conducting an annual inventory of all data and to~~ filing a Data Security Compliance Report with the Office of the CIO by October 31 of each year.

Formatted: Strikethrough

Deleted: file

5.0 Related Documents

5.1 NITC Security Officer Handbook (http://www.nitc.state.ne.us/standards/security/so_guide.doc)
5.2 NITC Network Security Policy (http://www.nitc.state.ne.us/standards/index.html)
5.3 Data Security Compliance Report – See appendix A
5.4 NITC Data Classification Standard (http:// something.something.something)

6.0 References

6.1 State of Nebraska Records Management Act (Neb. Rev. Stat. § 84-1201-1227)
6.2 National Institute Standards and Technology (NIST) Special Publication, 800-53, revision 1, "Recommended Security Controls for Federal Information Systems". (http://csrc.nist.gov/publications/drafts/800-53-rev1-clean-sz.pdf).
6.3 NSA (INFOSEC) Assessment Methodology (IAM) (http://www.iatrp.com/certclass.cfm)

Appendix A

Data Security Standard Compliance Report for _____,
(hereafter referred to as 'Agency').

I affirm that the Agency has performed an inventory of all Agency data, classified the data in accordance with the NITC Security Officer Handbook, and have implemented appropriate safeguards to protect the data from unauthorized access or disclosure.

_____ _____
Agency Director Date

Submit by October 31st to:

Office of the CIO
Attn: Steve Hartman
501 South 14th Street
Lincoln, NE 68509

Technical Panel
of the
Nebraska Information Technology Commission

Standards and Guidelines

Draft Document
30-Day Comment Period

Title: Password Standard

Notes to Readers:

1. The following document is a draft document under review by the Technical Panel of the Nebraska Information Technology Commission (NITC). This document is available in both PDF and Word versions at http://nitc.ne.gov/standards/.
2. If you have comments on this document, you can send them by email to rick.becker@nitc.ne.gov, or call 402-471-7984 for more information on submitting comments.
3. The comment period for this document ends on September 9, 2007.
4. The Technical Panel will consider this document and any comments received at their next meeting following the comment period, currently scheduled for September 11, 2007. Information about this meeting will be posted on the NITC web site at http://nitc.ne.gov/.

Nebraska Information Technology Commission

STANDARDS AND GUIDELINES

Password Standard

Category	**Security Architecture**
Title	**Password Standard**
Number	

Applicability

☑ State Government Agencies
- ☐ **All**.....Not Applicable
- ☑ **Excluding higher education institutions**.....Standard

☐ State Funded Entities - **All entities receiving state funding for matters covered by this document**.....Not Applicable

☑ Other: **All Public Entities**.....Guideline

Definitions:
Standard - Adherence is required. Certain exceptions and conditions may appear in this document, all other deviations from the standard require prior approval (see Section 3.2).
Guideline - Adherence is voluntary.

Status	☐ **Adopted** ☐ **Draft** ☐ **Other:**_____
Dates	**Date:** **Date Adopted by NITC:** **Other:**

Prepared by: Technical Panel of the Nebraska Information Technology Commission
Authority: Neb. Rev. Stat. § 86-516(6)
http://www.nitc.state.ne.us/standards/

1.0 Standard

Passwords are a primary means to control access to systems; therefore all users must select, use, and manage passwords to protect against unauthorized discovery or usage.

1.1 Password Construction

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

- Must contain at least eight (8) characters
- Must contain at least three (3) of the following four (4):
  - At least one (1) uppercase character
  - At least one (1) lowercase character
  - At least one (1) numeric character
  - At least one (1) symbol
- Must change at least every 90 days
- Must not repeat any character sequentially more than two (2) times
- Can not repeat any of the passwords used during the previous 365 days.

1.2 Non-Expiring Passwords

Agencies may use non-expiring passwords for automated system accounts (e.g. backups and batch jobs) after submitting the form found in Appendix A. All non-expiring passwords should exceed the character requirements listed in Section 1.1.

2.0 Purpose and Objectives

Passwords are used to authenticate a unique User ID to a variety of State of Nebraska resources. Some of the more common uses include: user accounts, web accounts, email accounts.

3.0 Applicability

3.1 State Government Agencies

All State agencies, boards, and commissions are required to comply with the standard listed in Section 1.0.

3.2 Exemption

Exemptions may be granted by the NITC Technical Panel upon request by an agency.

3.2.1 Exemption Process

Any agency may request an exemption from this standard by submitting a “Request for Exemption” to the NITC Technical Panel. Requests should state the reason for the exemption. Reasons for an exemption include, but are not limited to: statutory exclusion; federal government requirements; system limitation, or financial hardship. Requests may be submitted to the Office of the NITC via e-mail or letter (Office of the NITC, 501 S 14th Street, Lincoln, NE 68509). The NITC Technical Panel will consider the request and grant or deny the exemption. A denial of an exemption by the NITC Technical Panel may be appealed to the NITC.

4.0 Responsibility

4.1 NITC

The NITC shall be responsible for adopting minimum technical standards, guidelines, and architectures upon recommendation by the technical panel. (Neb. Rev. Stat. § 86-516(6))

4.2 State Agencies

Each state agency will be responsible for ensuring that any application or system requiring the use of a password adheres to this standard.

5.0 Related Documents

5.1 NITC Information Security Policy (http://www.nitc.state.ne.us/standards/index.html)
5.2 Non-expiring Password Agreement (Appendix A)

Appendix A

Non-Expiring Password Agreement

This agreement describes the agreed upon policy exception and/or level of security provided by the Office of the CIO for the application known as:

To the limits dictated by the State of Nebraska and Federal laws, agency data and system owners are responsible for determining how critical and sensitive information is for their applications to insure integrity, availability, and confidentiality.

Security Classification Levels

The NITC Data Security Standard recognizes four basic levels of security classifications that are associated with varying degrees of known risks. (See NITC Security Officer Handbook for more details). They can be summarized as follows:

HIGHLY RESTRICTED is for the most sensitive information intended strictly for use within your organization and controlled by special rules to specific personnel. It is highly critical and demands the highest possible security.

CONFIDENTIAL is for less sensitive information intended for use within your organization, yet still requires a high level of security. It may be regulated for privacy considerations. (e.g. HIPAA)

INTERNAL USE ONLY is for non-sensitive information intended for use within your organization. The security is controlled, but not highly protected.

UNCLASSIFIED/ PUBLIC is for information that requires minimal security and can be handled in the public domain.

Agency Justification

The undersigned agency representative has been authorized to request a **non-expiring password** for the application and data named above with a **security classification level** of _____ and includes the following criteria as supporting justification:

* * * * *

Office of the CIO Justification

The Office of the CIO recommends **no policy exceptions** with the following justification:

Agency Representative	Date	Office of the CIO Representative	Date

Comments - Security Related Documents

Comment #1
I was trained to be an ISO9000 lead auditor about ten years ago, and I have found that training to be very useful in many areas of my life even though I only worked with it for a few months. I continue to have an interest in quality standards, and like to contribute if I can.

I remember reading through some records retention standards while I was at DAS-Personnel. They might be useful to look at in creating the NITC Data Classification Standard, since they have already classified many types of information in them.

Thanks,

Brad Finch
IT Business Systems Analyst
NDOR - Materials and Research

Comment #2
In the password standard document, point 1.1 states...
Must not repeat any character sequentially more than 2 times.

RACF can't enforce it without an exit, which I prefer to avoid coding.
Besides that, I believe the statement is ambiguous, e.g., AAbbCC22 might be viewed as invalid, as could AAAbcde1. My recommendation would be to remove that requirement.

Fred Lupher
Enterprise Computing Services
Office of the CIO
State of NE

Comment #3
We are in complete support of the strong password/frequent password reset policy for granting access to State network resources. Where I began to get uncomfortable with the proposal is when I realized that it's intended to also apply to applications that reside outside the State firewall (in an appropriately designed dmz).

I am confident our internal customers will have significant concerns with this, and I don't believe addressing them through the NITC exceptions policy is the correct method of handling them. Generally, the NITC exceptions tend to be for legacy systems, and granted until such time as a revision or replacement to the system occurs. In a couple of instances in our environment, I'd expect our customer requirements in the event of a rewrite to include less stringent password policies. In both cases, the end users is accessing only resources that reside in a dmz - and thus has no direct access to the State network. Here's some examples;

Our UIConnect application is used by employers to pay Unemployment Insurance taxes, file associated reports, and set up new accounts. We purposely use a pin, which is refreshed and sent to the employer each quarter, for access. During the initial design of the system we had extensive debate regarding authentication, including a review of risk. The conclusion, there is little risk - few people will try to pay taxes they don't owe, and the repair to incorrect information in the system is inexpensive and doesn't have long term impact. The advantages of having a simple authentication are large in terms of employer support, and in terms of reduced cost of government. I know our business unit has a goal of having essentially all taxes filed through this

self-service application in the future. A strong password on a 90 day refresh would significantly hamper their ability to achieve that goal...

Our Nebraska JobLink Application is used by job seekers to search and apply for jobs, and to post resume's for employer review, as well as used by Employers to search for applicants and post jobs available. Again, this application provides an important service, reduces the cost of delivering government services, and we believe would see a reduction in usage with a strong password - frequent reset policy.

Both applications sit in a dmz - the purpose of which is to protect network resources. I'm wondering if applying the strong password requirements to services of this type is a case of requiring both belt and suspenders....

Thanks for your consideration - please let me know if you have questions.

Robert Shanahan, Executive Director
Office of Information Technology
Nebraska Workforce Development - Department of Labor
402-471-2518

Comment #4
1. Password policy
(http://nitc.ne.gov/standards/comment/Password_Standard_20070814_comment.pdf)
While having strong passwords can be an inconvenience to our staff, it is important to remember the kind of data that these passwords help safeguard... Nebraskan's social security numbers, personal information, and in some instances systems that access their bank accounts or credit card numbers. Good passwords are an important step in doing our due diligence in protecting that data.
One thing that may help users is to use passphrases, as opposed to passwords. Some users are under the impression that a strong password must resemble the cryptic form of /#*aKj8$, which forces them to write it on a nearby paper. A passphrase such as MyN@me15T1b0r (my name is tibor) are just as secure and much easier to remember.

2. Information Security Policy
(http://nitc.ne.gov/standards/comment/ITS_Security_Policy_2007_20070814_comment.pdf)
I like the open-ness of the document. It is a very nicely written and all-encompassing, dealing with many areas that security-minded sysadmins are aware of, but unfortunately many of our peers may not be. This document brings important information to all IT personnel and points out the things we should all be paying attention to.

None of us would like to see our name on the top half of the newspaper one morning and having to explain to media how we lost personal data on 50000 Nebraskans and businesses, and these 2 documents , as well as the data classification one go a long way towards protecting all of us.

Tibor Moldovan

Infrastructure Support Analyst
NDE Vocational Rehabilitation Services
402.471.1201

Comments from Informational Meetings

Comment #5
Information Security Policy

1. Remove the word 'Broad' in the 3rd paragraph on pg. 4 Change the phrase "must be used for state business only" to read "must be used for official business only". (pg. 7
2. Sharing Information Outside of the Agency.
    a. Add " within the control of the agency. Now reads" For information (that lays within the control of the Agency) to be released…"
    b. Strike "Sensitive or Confidential" and replace with "Non-public" – confusion on the multiple uses of the word confidential
3. Agency Accountability (pg. 8-9)
    a. Replace 'Sensitivity' of that information to read "classification' of that data
    b. Strike Backup plans (bottom of page 7) and replace with Disaster Recovery (DR) and Business Continuity Plans (BCP)
    c. Strike backup of critical data, to read "Preservation of critical data
4. User Training – Delete developed from the first line.
5. Monitoring Pg. 10 – Rework
    a. Old: Only qualified agency staff or third party individuals with proper authorization from the Office of the Chief Information Officer will be permitted to use 'sniffers' or similar technology on the network to monitor operational data and security events on the State network.
    b. NEW: Only individuals with proper authorization from the Office of the Chief Information Officer will be permitted to use 'sniffers' or similar technology on the network to monitor operational data and security events on the State network.
6. Equipment Security: Strike "… in accordance with DAS fixed asset guidelines"

DEQ

Comment #6
Information Security Policy

User Authentication for External Connections (Remote Access Control) – Pg. 14
What about Windows Update services? Java updates? Adobe? Are these covered under this section?

NIS CNC

Comment #7
Information Security Policy

Section 3: Agency accountability – Pg. 14; "Add a reference that recovery plans should be tested on a regular basis, and those tests documented."
Section 6 – Delete "when classifying data…
Section 9 – Change Control Management – Needs a standard to Guideline spell this out in detail.

Password Standard

Applications that are available only once you have authenticated to the state's network (e.g. - a domain or LAN) should be allowed to use non-expiring passwords as allowed in 1.2

Randy Cecrle – WCC

Comment #8
Information Security Policy

Section 6 –
Spell out GLB, HIPAA, FERPA

Janette Lee – Banking

Comment #9
Data Security Standard

Check court rulings on the use of “Data Owner” and “Data Custodian”

Mike Overton – Crime Commission