| | |
|---|---|
| **Title** | **Information Security Management Policy** |
| **Category** | **Security Architecture** |
| **Date Adopted** | |
| **Date of Last Revision** | **October 31, 2000** |
| **Status** | **Draft Policy** |

## *A. Authority*

Section 86-1506 (6). "(The Nebraska Information Technology Commission shall) adopt minimum technical standards, guidelines, and architectures upon recommendation by the technical panel created in Section 86-1511."

## *B. Purpose and Objectives*

The purpose of this document is to define and clarify policies, principles, standards, guidelines, and responsibilities related to the security of the state's information technology resources.

An information security management policy is necessary to serve statutory goals pertaining to government operations, public records, and facilities. These include:

1. Insure continuity of government operations (Article III, Section 29 of the Nebraska Constitution; Nebraska Revised Statutes Sections 28-901 and 84-1201)
2. Protect safety and integrity of public records (Nebraska Revised Sections 28-911, 29-2391, and 84-1201)
3. Prevent unauthorized access to public records (Nebraska Revised Statutes Sections 29-319, 81-1117.02, and 84-712.02)
4. Insure proper use of communications facilities (Nebraska Revised Statutes Section 81-1117.02)
5. Assign responsibility for efficient and economical management of public records (Nebraska Revised Statutes Section 84-1207)
6. Protect privacy of citizens (Nebraska Revised Statutes Section 84, Article 7)

The primary objectives of Information Security Policies are:

1. To effectively manage the risk of security exposure or compromise within the systems
2. To communicate the responsibilities for the protection of information
3. To establish a secure processing base and a stable processing environment
4. To promote understanding and compliance with all applicable laws and regulations

To protect management and preserve management's options in the event of an information asset misuse, loss or unauthorized disclosure.

Section D provides key definitions.

Section E explains applicability.

Section F describes roles and responsibilities.

## *C. Information Security Management Policy*

POLICY STATEMENT

Owners of systems must determine how critical and sensitive information is and must adopt and implement comprehensive security programs that offer a level of protection commensurate with the value of the assets. Information security programs must provide reasonable protection against unauthorized access, disclosure, modification, or destruction, as well as to assure the availability, integrity, utility, authenticity and confidentiality of information. This applies to all systems that gather, generate and store data.

EXPLANATION

Information takes many forms. It may be stored on computers, transmitted across networks, printed or written on paper, and spoken in conversations. Information and information technology systems are assets of vital importance to the institutions and government agencies of Nebraska. These information assets are central to the daily operation of the institutions and agencies and may impact each legislator, administrator, faculty, student, or patron that provides or relies on their services. Information security has four main components:

1. Confidentiality. Protecting sensitive information from unauthorized disclosure or intelligible interception;
2. Integrity. Safeguarding the accuracy and completeness of information and processing methods;
3. Availability. Ensuring that information and services are available when required;
4. Non-repudiation. Proving transfer and receipt of an unforgeable electronic transaction.

The Information Security Management Policy provides guidance for establishing effective security measures. The goal of this policy is to ensure the confidentiality of information systems, the continued availability of information systems to support critical activities, and the implementation of appropriate technologies and controls to protect information from intentional or accidental disclosure, manipulation, modification, erasure or copying.

Information security policies must serve several core principles. These include:

1. Information is an asset. It has value to the organization and needs to be suitably protected.
2. Information resources must be available when needed. Continuity of information resources supporting critical services must be ensured in the event of a disruption to business or a disaster, which makes critical systems unavailable.
3. Risks to information resources must be managed. The expense of security safeguards must be cost effective and commensurate with the value of the assets being protected.
4. Computer security must support the mission of the organization. It should be an integral element of sound management. It requires a comprehensive and integrated approach, which is periodically reassessed.

5. All individuals are accountable for their actions relating to information resources. Information resources shall be used only for intended purposes as defined by the owner and consistent with applicable laws. Owners of sensitive information and critical systems have security responsibilities outside their organization. Responsibilities for information security management must be explicit.

These policies and principles are designed to manage the risk of exposure or compromise within the system. This requires communicating the responsibilities for the protection of information, establishing a secure processing base and a stable processing environment, promoting understanding and compliance with all applicable laws and regulations, and protecting management and preserving management's options in the event of and information asset misuse, loss or unauthorized disclosure.

STANDARDS

Information security programs must include the following elements:

1. Security policies, standards, and procedures for the agency or institution;
2. Risk assessment, including inventory, value of assets, asset classification, cost of reconstruction, and mitigation strategies;
3. Organizational responsibilities for implementing the security program, including security administration and a steering committee within the organization with authority over all aspects of security;
4. Security framework for identification and authentication, authorization and access control, accountability, integrity and availability, security of communication, and security administration;
5. Personnel security;
6. Physical and environmental security;
7. Disaster recovery;
8. Incident reporting;
9. Compliance, including consequences of violations;
10. Training and education;
11. Security audits
12. Data classification system for determining the appropriate level of security.

The Information Security Program should include the steps in the flow chart at the end of this document.

### *D. Key Definitions*

1. Agency shall mean any governmental entity, including state government, local government, or third party entities under contract to the agency.
2. Critical Systems are those systems or system components (hardware, data, or software) that if lost or compromised would jeopardize the ability of the system to continue processing.
3. Disaster refers to any event that threatens the destruction of information or availability of computer systems. A disaster may affect the physical security of computer systems, including equipment failures, fire, flood, other natural calamities, or theft of equipment. A disaster may involve destruction or

information or availability of computer systems due to system failure, human error, or intentional acts including computer crimes.

4. E-mail is the exchange and or sharing of messages, attachments, and calendar and scheduling information.
5. Information Security is the protection of data against accidental or malicious destruction, modification or disclosure.
6. Security Policy is a statement of the goals, responsibilities, and accepted behaviors required for maintaining a secure environment. Security policies set the direction, give broad guidance and demonstrate senior management support for security-related facilities and actions across the organization.
7. Security Standard is a set of tasks, responsibilities, or guidelines that provide metrics to policies. Security procedures are standards that are very specific in nature, applying to group or individual systems. Procedures are directive in nature, whereas policies provide principles.
8. Sensitive Information is that information which must be protected to insure only authorized access or if lost or compromised might negatively affect the owner of the information or require substantial resources to recreate.
9. State Data Communications Network (SDCN) shall mean any data communications facility contracted for or provided by the State of Nebraska, including State-provided Internet access and network connections to state computers.
10. Users of electronic assets include any employee, business partner, contractor, consultant, or customer who is authorized to use the information technology assets of a state agency or institution.
11. Value of information includes the cost of collection, cost of reconstruction, and legal or operational consequences if information is lost or compromised.

## *E. Applicability*

GENERAL STATEMENT

These policies are intended to be sufficiently generic to apply to a wide range of governmental and educational agencies in the State of Nebraska. Each agency or operational entity must develop detailed procedures to implement broad policies and standards. Compliance with these security policies and standards will be a requirement during consideration of funding for any projects requiring review by the NITC. Compliance may be used in audit reviews or budget reviews.

EXCEPTION STATEMENT

"Computer security must support the mission of the organization." "The expense of security safeguards must be cost effective and commensurate with the value of the assets being protected." "Owners of sensitive information and critical systems have security responsibilities outside their organization." (From the Information Security Management Policy, in Part C.)

These three principles provide the basis for determining the applicability of security policies and standards to specific situations within an organization. The responsible security authority of an organization should establish a two-step test, before exempting a unit within the organization from a particular security requirement. The first test is met, if a security requirement is contrary to the organization's mission or is

not cost-effective given the value of the assets being protected. The second test is met, if exempting a security requirement does not create unreasonable risk of adverse consequences to people or entities outside of the organization. Both tests should be met.

COMPLIANCE AND ENFORCEMENT STATEMENT

The Governing board or chief administrative officer of each organization must develop internal compliance and enforcement policies as part of its information security program. Such policies should be effective and commensurate with the risks involved. The NITC intends to incorporate adherence to security policies as part of its evaluation and prioritization of funding requests. The NITC recommends that the Governor and Legislature give due consideration to requests for security improvements during the budget process.

### *F. Responsibility*

An effective security program involves cooperation of many different entities. Major participants and their responsibilities include:

1. Nebraska Information Technology Commission. The NITC provides strategic direction for state agencies and educational institutions in the area of information technology. The NITC also has statutory responsibility to adopt minimum technical standards and guidelines for acceptable and cost-effective use of information technology. Implicit in these requirements is the responsibility to promote adequate security of information systems through adoption of policies, standards, and guidelines. The NITC must develop strategies for implementing and evaluating the effectiveness of information security programs.
2. Technical Panel Security Work Group. 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.
3. Chief Information Officer, State of Nebraska. The CIO has the responsibility to assist in building the business case for cost-effective implementation of security programs in non-education state agencies. The CIO must also work with non-education state agencies to coordinate and evaluate security programs. The CIO shall insure that non-education state agencies have documented procedures to demonstrate compliance with these security policies.
4. Agency and Institutional Heads. The highest authority within an agency or institution is responsible for the protection of information resources, including developing and implementing information security programs consistent with this policy. The authority may delegate this responsibility but delegation does not remove the accountability.
5. Agency Information Officer. In most cases, the highest authority within an agency or institution delegates the general responsibility for security of the agency's information technology resources to the agency's highest ranking information technology professional. This responsibility includes development and promulgation of agency-specific information security policies.

6. Agency Security Officer. In some cases, the Agency Information Officer assigns an Agency Security Officer who is responsible for:
    - Implementing enterprise and agency-specific or application-specific security policies and procedures.
    - Developing procedures and administering the information access control decisions made by information custodians within the agency.
    - Identifying training requirements.
    - Implementing procedures for authentication of users and messages.
    - Publish guidelines for creating and managing passwords.
    - Developing and implementing strategies to make users aware of security policies, procedures and benefits.
    - Documenting the security support structure across platforms.
    - Enforcing agency security policies.
    - Establishing and chairing agency security committees.
    - Monitoring unusual activities and report security breaches and incidents, including identifying resources to assist with tracking, analysis, and responding to incidents.
    - Periodically evaluating effectiveness of security policies and procedures.
    - Fact gathering and analysis on information security issues.
    - Developing recommendations for the agency or institution on security matters.
    - Reviewing changes to the configuration of security administration facilities and settings.
    - Participate in preparing a disaster recovery plan. They must understand the risks posed by disruption of computer systems. They must help prepare contingencies and be ready to implement the disaster recovery plan.

    The Agency Security Officer may work with a security committee of the agency or institution. The Security Committee is an advisory group made up of key technical and management personnel within the agency to coordinate security efforts and resolve security problems.
7. Program Managers and Information Custodians In most cases, the authority within the agency or institution delegates custody of specific types of information maintained by the agency to administrators in the agency who may further delegate to employees in their organizations. These persons have direct responsibility for:
    - deciding issues pertaining to access to information
    - insuring information security
    - participating in preparing a disaster recovery plan.
8. Users of Electronic Assets. All authorized users shall be accountable for their actions relating to information assets, including hardware, software and electronic information. Information resources shall be used only for intended purposes as defined by the agency and consistent with applicable laws.
9. Information Technology Staff. Staff who are directly responsible for security, system management, and applications development have special privileges in relation to information resources such as the ability to examine the files of

other users. People with access management rights must follow strict procedures regarding their access to information resources and sharing that access with others.

10. Employees and persons under contract. Employees must become knowledgeable about their organization's security policies and procedures. Employees must exercise due diligence in following those procedures and incorporating sound security practices in the discharge of their normal duties.

### *G. Related Policies, Standards and Guidelines*

Section 3 of the Statewide Technology Plan established a state enterprise architecture framework to guide decisions on the exchange of information and utilization of shared information technology resources. One element of the framework is security architecture, which includes information security policies. In addition, security policies will affect other components of the framework, including network, applications, data, hardware, electronic commerce, and systems management. Standards, guidelines, and best practices for each element of the technical architecture must reflect security considerations.

The Information Security Management Policy provides the general requirements for a set of policies, standards, and procedures to protect the information assets of an organization. Other information security policies address the specific topics of:

1. Access Control Policy
2. Disaster Recovery Policy
3. Education, Training and Awareness Policy
4. Individual Use Policy
   - Acceptable Use
   - Copyrighted Materials
   - E-mail Use
5. Network Security Policy
   - General Network Controls
   - Perimeter Security for Internet and Intranet Connections
   - Remote Access
6. Security Breaches / Incident Reporting Policy

The following statutes also relate to security policies:

Section 86-1510 (2). "(The Chief Information Officer shall) recommend policies and guidelines for acceptable and cost-effective use of information technology in non-education state government."

Section 86-1511 (2). "The technical panel may recommend technical standards and guidelines to be considered for adoption by the commission."

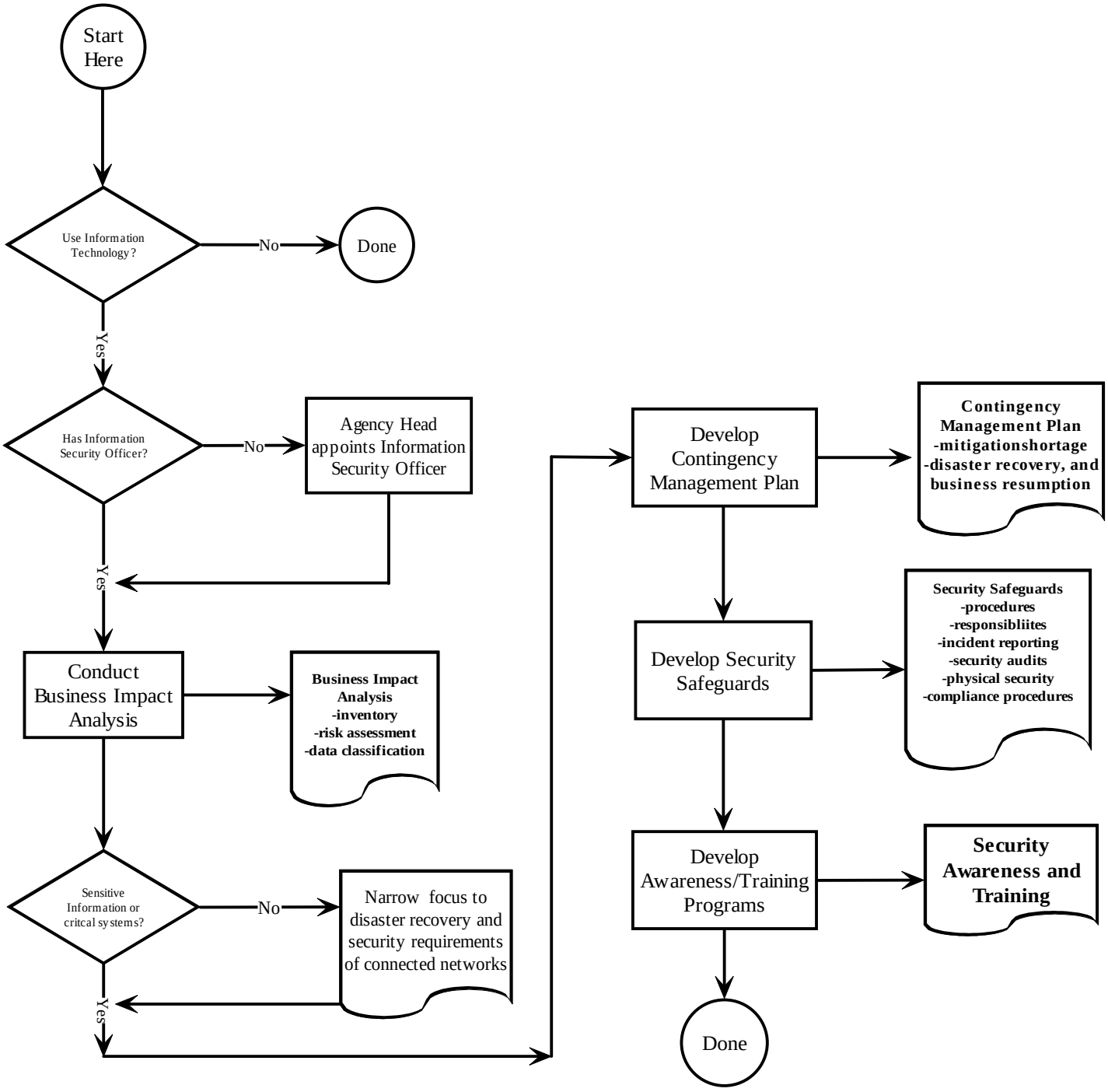
Section 86-1514 (2)(d). "(The Appropriations Committee and the Transportation and Telecommunications Committee of the Legislature shall determine the extent to which) policies, standards, guidelines, and architectures have been developed and observed."

Section 84-1201 (Records Management Act). "(The Legislature declares) that records containing information essential to the operations of government and to the protection of the rights and interests of persons, must be safeguarded against the destructive effects of all forms of disaster and must be available as needed;

wherefore it is necessary to adopt special provisions for the selection and preservation of essential state and local records, thereby insuring the protection and availability of such information."

Section 84-1213. (Records Management Act). Anyone mutilating, destroying, transferring, removing or damaging public records, except as provided by law, is guilty of a Class III misdemeanor.

# Information Security Program



| | |
|---|---|
| **Title** | **Access Control Policy** |
| **Category** | **Security Architecture** |
| **Date Adopted** | |
| **Date of Last Revision** | **October 31, 2000** |
| **Status** | **Draft Policy** |

## *A. Authority*

Section 86-1506 (6). "(The Nebraska Information Technology Commission shall) adopt minimum technical standards, guidelines, and architectures upon recommendation by the technical panel created in Section 86-1511."

## *B. Purpose and Objectives*

The purpose of this document is to define and clarify policies, principles, standards, guidelines, and responsibilities related to the security of the state's information technology resources.

A policy on access control is intended to support information security by preventing unauthorized access to computer systems and data.

The primary objectives of the Access Control Policy are:

1. To communicate the need for access control.
2. To establish specific requirements for protecting against unauthorized access.
3. To create an infrastructure that will foster data sharing without sacrificing security of information resources.

Section D provides key definitions.
Section E explains applicability.
Section F describes roles and responsibilities.

## *C. Access Control Policy*

POLICY STATEMENT

Access Control protects information by managing access to all entry and exit points, both logical and physical. Adequate perimeter security and logical security measures must protect against unauthorized access to sensitive information on a governmental facility, network, or application. These measures ensure that only authorized users, as determined by each governmental entity, have access to specific computer resources, networks, data, and applications.

EXPLANATION

New technologies and more automation are increasing opportunities for data sharing. Agencies must seek a balance between the need to protect information resources and allowing greater access to data and applications. Multiple factors will affect how an agency chooses to control access to its computers, networks and data. This includes some calculation of risk and consequences of unauthorized access. In

addition, agencies with interconnected systems must collaborate to achieve mutually effective protection against unauthorized access.

STANDARDS

1. Access by technical specialists. Information technology specialists include those individuals such as application developers and LAN administrators who have specific types of responsibilities and access to agency and enterprise information. Agency policy should define these roles and responsibilities consistent with enterprise policy directives and unique business needs of the agency. Application developers should have limited ongoing access to production databases. Agencies that allow application developers access to production databases because of business needs should do so limiting such access to only those tasks that are essential to ensure that the application runs smoothly once applications are in a production environment. Agency policy should establish a change control system for managing modifications to applications. The change control system should define the process for review and approval of code changes.
2. Administration. Security administration activity regarding access should be recorded and reviewed and security violations or incidents should be detected and reported.
3. Application requirements. Applications shall incorporate controls for managing access to selected information and functions. Applications must include auditing capabilities to track access to sensitive information.
4. Authentication. Systems should implement authentication functions that are consistent with the level of confidentially or sensitively of the information they contain and process. Identification should be unique for each user of the system. The system should provide a method to accurately identify the user through a directory system, passwords, smart tokens, smart cards, or other means.
5. Authorization. The authorities to read, write, modify, update, or delete information from automated files or databases should be established by the owner(s) of the information. Individuals may be granted a specific combination of authorities. Individuals should not be given any authority beyond their needs. Access rules or profiles should be established in a manner that restricts users from performing incompatible functions or functions beyond their responsibility and enforces a separation of duties.
6. Systems with Sensitive Information.. Computer operations which support sensitive information shall operate in accordance with procedures approved by the information custodians of participating agencies and assure that:
    - information cannot be modified or destroyed except in accordance with procedures;
    - Operating programs prohibit unauthorized inquiry, changes or destruction of records;
    - Operating programs are used to detect and store all unauthorized attempts to penetrate the system;
    - Special requirements are met, such as those for criminal justice records.

7. Department of Administrative Services. Neither the data processing administrator, the Director of Administrative Services, nor any employee of such administrator or director shall release or permit the release of any data maintained in computer files to any person or persons without the express written approval of both the agency primarily responsible for collection and maintenance of such data and the employee to whom such data pertains, except to the Legislative Fiscal Analyst pursuant to section 50-420 and Auditor of Public Accounts solely for use in the performance of audits prescribed by law.
8. Network access. Access to a secure network shall be subject to the security policies and procedures of the network operator.
9. Passwords. Passwords should be confidential and at least 5 alphanumeric characters long. Passwords should not be a single dictionary word, repeating character strings, or identifying information that is linked to the user. Depending on the critical nature of the system, passwords should expire on a time-prescribed basis, at least every six months.
10. Personnel. Specialized Technical Staff with broad access to data are in sensitive positions and may be required to undergo a security check as a condition of employment.
11. Physical access. Security is required not only for software and information, but also for physical security of equipment. All agencies must develop and implement policies which include at least the following:
    - Restrict physical access to computer facilities where continued operation is essential or where sensitive or confidential data are stored online.
    - Restrict access to computer facilities to agency employees or agents who need such access to perform assigned work duties.
    - Restrict access to software documentation and data storage to state employees or agents who need such access to perform assigned work duties.
12. Sanctions. The operator of a secure network may revoke access to the network to insure the security, integrity, and availability of the network to other users.
13. Termination of employment or duties. Information custodians must notify the person performing the duties of the agency security officer when an employee or agent leaves or there is a significant change in duties that affect changes in access to information resources.
14. Workstation security.
    - Sensitive or confidential information should not be on the workstation hard drive for security and business reasons. Most workstations pose a risk of unauthorized access because the drives are accessible.
    - Reasonable efforts should be made to safeguard individual workstations to protect against unauthorized access to the workstation, network or data. Workstations can be secured by securing the rooms where they are located and by physically attaching them to tables or work areas so that special tools are required to remove them from the premises.

- Passwords for workstation logon should not be built into the logon script for auto-signon.
- Users of portable technology must follow agency guidelines to protect against the theft, destruction or loss of equipment and information.
- Users should sign-off when the system will be left inactive or unattended.

### *D. Key Definitions*

1. Agency shall mean any governmental entity, including state government, local government, or third party entities under contract to the agency.
2. Critical Systems are those systems or system components (hardware, data, or software) that if lost or compromised would jeopardize the ability of the system to continue processing.
3. Disaster refers to any event that threatens the destruction of information or availability of computer systems. A disaster may affect the physical security of computer systems, including equipment failures, fire, flood, other natural calamities, or theft of equipment. A disaster may involve destruction or information or availability of computer systems due to system failure, human error, or intentional acts including computer crimes.
4. E-mail is the exchange and or sharing of messages, attachments, and calendar and scheduling information.
5. Information Security is the protection of data against accidental or malicious destruction, modification or disclosure.
6. Security Policy is a statement of the goals, responsibilities, and accepted behaviors required for maintaining a secure environment. Security policies set the direction, give broad guidance and demonstrate senior management support for security-related facilities and actions across the organization.
7. Security Standard is a set of tasks, responsibilities, or guidelines that provide metrics to policies. Security procedures are standards that are very specific in nature, applying to group or individual systems. Procedures are directive in nature, whereas policies provide principles.
8. Sensitive Information is that information which must be protected to insure only authorized access or if lost or compromised might negatively affect the owner of the information or require substantial resources to recreate.
9. State Data Communications Network (SDCN) shall mean any data communications facility contracted for or provided by the State of Nebraska, including State-provided Internet access and network connections to state computers.
10. Users of electronic assets include any employee, business partner, contractor, consultant, or customer who is authorized to use the information technology assets of a state agency or institution.
11. Value of information includes the cost of collection, cost of reconstruction, and legal or operational consequences if information is lost or compromised.

## *E. Applicability*

GENERAL STATEMENT

These policies are intended to be sufficiently generic to apply to a wide range of governmental and educational agencies in the State of Nebraska. Each agency or operational entity must develop detailed procedures to implement broad policies and standards. Compliance with these security policies and standards will be a requirement during consideration of funding for any projects requiring review by the NITC.

EXCEPTION STATEMENT

"Computer security must support the mission of the organization." "The expense of security safeguards must be cost effective and commensurate with the value of the assets being protected." "Owners of sensitive information and critical systems have security responsibilities outside their organization." (From the Information Security Management Policy.)

These three principles provide the basis for determining the applicability of security policies and standards to specific situations within an organization. The responsible security authority of an organization should establish a two-step test, before exempting a unit within the organization from a particular security requirement. The first test is met, if a security requirement is contrary to the organization's mission or is not cost-effective given the value of the assets being protected. The second test is met, if exempting a security requirement does not create unreasonable risk of adverse consequences to people or entities outside of the organization. Both tests should be met.

COMPLIANCE AND ENFORCEMENT STATEMENT

The governing board or chief administrative officer of each organization must develop internal compliance and enforcement policies as part of its information security program. Such policies should be effective and commensurate with the risks involved. The NITC intends to incorporate adherence to security policies as part of its evaluation and prioritization of funding requests. The NITC recommends that the Governor and Legislature give due consideration to requests for security improvements during the budget process.

## *F. Responsibility*

An effective security program involves cooperation of many different entities. Major participants and their responsibilities include:

1. Nebraska Information Technology Commission. The NITC provides strategic direction for state agencies and educational institutions in the area of information technology. The NITC also has statutory responsibility to adopt minimum technical standards and guidelines for acceptable and cost-effective use of information technology. Implicit in these requirements is the responsibility to promote adequate security of information systems through adoption of policies, standards, and guidelines. The NITC must develop strategies for implementing and evaluating the effectiveness of information security programs.

2. Technical Panel Security Work Group. 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.
3. Chief Information Officer, State of Nebraska. The CIO has the responsibility to assist in building the business case for cost-effective implementation of security programs in non-education state agencies. The CIO must also work with non-education state agencies to coordinate and evaluate security programs. The CIO shall insure that non-education state agencies have documented procedures to demonstrate compliance with these security policies.
4. Agency and Institutional Heads. The highest authority within an agency or institution is responsible for the protection of information resources, including developing and implementing information security programs consistent with this policy. The authority may delegate this responsibility but delegation does not remove the accountability.
5. Agency Information Officer. In most cases, the highest authority within an agency or institution delegates the general responsibility for security of the agency's information technology resources to the agency's highest ranking information technology professional. This responsibility includes development and promulgation of agency-specific information security policies.
6. Agency Security Officer. In some cases, the Agency Information Officer assigns an Agency Security Officer who is responsible for:
    - Implementing enterprise and agency-specific or application-specific security policies and procedures.
    - Developing procedures and administering the information access control decisions made by information custodians within the agency.
    - Identifying training requirements.
    - Implementing procedures for authentication of users and messages.
    - Publish guidelines for creating and managing passwords.
    - Developing and implementing strategies to make users aware of security policies, procedures and benefits.
    - Documenting the security support structure across platforms.
    - Enforcing agency security policies.
    - Establishing and chairing agency security committees.
    - Monitoring unusual activities and report security breaches and incidents.
    - Periodically evaluating effectiveness of security policies and procedures.
    - Fact gathering and analysis on information security issues.
    - Developing recommendations for the agency or institution on security matters.
    - Reviewing changes to the configuration of security administration facilities and settings.
    - Participate in preparing a disaster recovery plan. They must understand the risks posed by disruption of computer systems. They

must help prepare contingencies and be ready to implement the disaster recovery plan.

The Agency Security Officer may work with a security committee of the agency or institution. The Security Committee is an advisory group made up of key technical and management personnel within the agency to coordinate security efforts and resolve security problems.

7. Program Managers and Information Custodians In most cases, the authority within the agency or institution delegates custody of specific types of information maintained by the agency to administrators in the agency who may further delegate to employees in their organizations. These persons have direct responsibility for:
   - deciding issues pertaining to access to information
   - insuring information security
   - participating in preparing a disaster recovery plan.
8. Users of Electronic Assets. All authorized users shall be accountable for their actions relating to information assets, including hardware, software and electronic information. Information resources shall be used only for intended purposes as defined by the agency and consistent with applicable laws.
9. Information Technology Staff. Staff who are directly responsible for security, system management, and applications development have special privileges in relation to information resources such as the ability to examine the files of other users. People with access management rights must follow strict procedures regarding their access to information resources and sharing that access with others.
10. Employees and persons under contract. Employees must become knowledgeable about their organization's security policies and procedures. Employees must exercise due diligence in following those procedures and incorporating sound security practices in the discharge of their normal duties.

### *G. Related Policies, Standards and Guidelines*

The Information Security Management Policy provides the general requirements for a set of policies, standards, and procedures to protect the information assets of an organization. Other information security policies address the specific topics of:

1. Access Control Policy
2. Disaster Recovery Policy
3. Education, Training and Awareness Policy
4. Individual Use Policy
   - Acceptable Use
   - Copyrighted Materials
   - E-mail Use
5. Network Security Policy
   - General Network Controls
   - Perimeter Security for Internet and Intranet Connections
   - Remote Access
6. Security Breaches / Incident Reporting Policy

| | |
|---|---|
| **Title** | **Disaster Recovery Policy** |
| **Category** | **Security Architecture** |
| **Date Adopted** | |
| **Date of Last Revision** | **October 31, 2000** |
| **Status** | **Draft Policy** |

## *A. Authority*

Section 86-1506 (6). "(The Nebraska Information Technology Commission shall) adopt minimum technical standards, guidelines, and architectures upon recommendation by the technical panel created in Section 86-1511."

Section 84-1201 (Records Management Act). "(The Legislature declares) that records containing information essential to the operations of government and to the protection of the rights and interests of persons, must be safeguarded against the destructive effects of all forms of disaster and must be available as needed; wherefore it is necessary to adopt special provisions for the selection and preservation of essential state and local records, thereby insuring the protection and availability of such information."

## *B. Purpose and Objectives*

The purpose of this document is to define and clarify policies, principles, standards, guidelines, and responsibilities related to the security of the state's information technology resources.

A policy on disaster recovery is intended to serve statutory goals pertaining to government operations, public records, and facilities. These include:

1. Insure continuity of government operations (Article III, Section 29 of the Nebraska Constitution; Nebraska Revised Statutes Sections 28-901 and 84-1201)
2. Protect safety and integrity of public records (Nebraska Revised Sections 28-911, 29-2391, and 84-1201)

The primary objectives of the Disaster Recovery Policy are:

1. To reduce the risk of disruption of operations or loss of information;
2. To communicate responsibilities for the protection of information and continuity of government operations;
3. To establish a plan for restoration of information and operations following a disaster.

Section D provides key definitions.
Section E explains applicability.
Section F describes roles and responsibilities.

## *C. Disaster Recovery Policy*

POLICY STATEMENT

Each agency must have a disaster recovery plan that at least identifies and militates against risks to critical systems and sensitive information in the event of a disaster. The plan shall provide for contingencies to restore information and systems if a disaster occurs. The disaster recovery plan for information technology may be a subset of an agency's comprehensive disaster recovery plan. The concept of a disaster recovery includes business resumption.

EXPLANATION

Disaster recovery plans must serve several core principles. These include:

1. Information is an asset. It has value to the organization and needs to be suitably protected.
2. Information resources must be available when needed. Continuity of information resources supporting critical services must be ensured in the event of a disruption to business or a disaster, which makes critical systems unavailable.
3. Risks to information resources must be managed. The expense of security safeguards must be cost effective and commensurate with the value of the assets being protected.

STANDARDS

Disaster recovery plans must include the following elements:

1. Business impact analysis, including risk assessment, asset classification, and potential disruption to stakeholders.
2. Classification system to identify critical systems and essential records;
3. Mitigation strategies and safeguards to avoid disasters. Safeguards should include protective measures such as redundancy, fire suppression, uninterruptable power supply (UPS), surge protection, and environmental measures to protect sensitive equipment from dust, temperature or humidity.
4. Backups and offsite storage.
5. Business resumption.
6. Contingency plans for different types of disruption to information systems.
7. Organizational responsibilities for implementing the disaster recovery plan.
8. Procedures for reporting incidents and implementing the disaster recovery plan and escalating the agency or institution's response to a disaster.
9. Multiple site storage of back-up documents identified in the plan.
10. Training, testing, and improvement.
11. Annual review and revision.

### *D. Key Definitions*

1. Agency shall mean any governmental entity, including state government, local government, or third party entities under contract to the agency.
2. Critical Systems are those systems or system components (hardware, data, or software) that if lost or compromised would jeopardize the ability of the system to continue processing.
3. Disaster refers to any event that threatens the destruction of information or availability of computer systems. A disaster may affect the physical security of computer systems, including equipment failures, fire, flood, other natural calamities, or theft of equipment. A disaster may involve destruction or

information or availability of computer systems due to system failure, human error, or intentional acts including computer crimes.

4. E-mail is the exchange and or sharing of messages, attachments, and calendar and scheduling information.
5. Information Security is the protection of data against accidental or malicious destruction, modification or disclosure.
6. Security Policy is a statement of the goals, responsibilities, and accepted behaviors required for maintaining a secure environment. Security policies set the direction, give broad guidance and demonstrate senior management support for security-related facilities and actions across the organization.
7. Security Standard is a set of tasks, responsibilities, or guidelines that provide metrics to policies. Security procedures are standards that are very specific in nature, applying to group or individual systems. Procedures are directive in nature, whereas policies provide principles.
8. Sensitive Information is that information which must be protected to insure only authorized access or if lost or compromised might negatively affect the owner of the information or require substantial resources to recreate.
9. State Data Communications Network (SDCN) shall mean any data communications facility contracted for or provided by the State of Nebraska, including State-provided Internet access and network connections to state computers.
10. Users of electronic assets include any employee, business partner, contractor, consultant, or customer who is authorized to use the information technology assets of a state agency or institution.
11. Value of information includes the cost of collection, cost of reconstruction, and legal or operational consequences if information is lost or compromised.

## *E. Applicability*

GENERAL STATEMENT

These policies are intended to be sufficiently generic to apply to a wide range of governmental and educational agencies in the State of Nebraska. Each agency or operational entity must develop detailed procedures to implement broad policies and standards. Compliance with these security policies and standards will be a requirement during consideration of funding for any projects requiring review by the NITC. Compliance may be used in audit reviews or budget reviews.

EXCEPTION STATEMENT

"Computer security must support the mission of the organization." "The expense of security safeguards must be cost effective and commensurate with the value of the assets being protected." "Owners of sensitive information and critical systems have security responsibilities outside their organization." (From the Information Security Management Policy)

These three principles provide the basis for determining the applicability of security policies and standards to specific situations within an organization. The responsible security authority of an organization should establish a two-step test, before exempting a unit within the organization from a particular security requirement. The first test is met, if a security requirement is contrary to the organization's mission or is

not cost-effective given the value of the assets being protected. The second test is met, if exempting a security requirement does not create unreasonable risk of adverse consequences to people or entities outside of the organization. Both tests should be met.

COMPLIANCE AND ENFORCEMENT STATEMENT

The governing board or chief administrative officer of each organization must develop internal compliance and enforcement policies as part of its information security program. Such policies should be effective and commensurate with the risks involved. The NITC intends to incorporate adherence to security policies as part of its evaluation and prioritization of funding requests. The NITC recommends that the Governor and Legislature give due consideration to requests for security improvements during the budget process.

### *F. Responsibility*

An effective security program involves cooperation of many different entities. Major participants and their responsibilities include:

1. Nebraska Information Technology Commission. The NITC provides strategic direction for state agencies and educational institutions in the area of information technology. The NITC also has statutory responsibility to adopt minimum technical standards and guidelines for acceptable and cost-effective use of information technology. Implicit in these requirements is the responsibility to promote adequate security of information systems through adoption of policies, standards, and guidelines. The NITC must develop strategies for implementing and evaluating the effectiveness of information security programs.
2. Technical Panel Security Work Group. 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.
3. Chief Information Officer, State of Nebraska. The CIO has the responsibility to assist in building the business case for cost-effective implementation of security programs in non-education state agencies. The CIO must also work with non-education state agencies to coordinate and evaluate security programs. The CIO shall insure that non-education state agencies have documented procedures to demonstrate compliance with these security policies.
4. Agency and Institutional Heads. The highest authority within an agency or institution is responsible for the protection of information resources, including developing and implementing information security programs consistent with this policy. The authority may delegate this responsibility but delegation does not remove the accountability.
5. Agency Information Officer. In most cases, the highest authority within an agency or institution delegates the general responsibility for security of the agency's information technology resources to the agency's highest ranking information technology professional. This responsibility includes development and promulgation of agency-specific information security policies.

6. Agency Security Officer. In some cases, the Agency Information Officer assigns an Agency Security Officer who is responsible for:
    - Implementing enterprise and agency-specific or application-specific security policies and procedures.
    - Developing procedures and administering the information access control decisions made by information custodians within the agency.
    - Identifying training requirements.
    - Implementing procedures for authentication of users and messages.
    - Publish guidelines for creating and managing passwords.
    - Developing and implementing strategies to make users aware of security policies, procedures and benefits.
    - Documenting the security support structure across platforms.
    - Enforcing agency security policies.
    - Establishing and chairing agency security committees.
    - Monitoring unusual activities and report security breaches and incidents.
    - Periodically evaluating effectiveness of security policies and procedures.
    - Fact gathering and analysis on information security issues.
    - Developing recommendations for the agency or institution on security matters.
    - Reviewing changes to the configuration of security administration facilities and settings.
    - Participate in preparing a disaster recovery plan. They must understand the risks posed by disruption of computer systems. They must help prepare contingencies and be ready to implement the disaster recovery plan.

    The Agency Security Officer may work with a security committee of the agency or institution. The Security Committee is an advisory group made up of key technical and management personnel within the agency to coordinate security efforts and resolve security problems.
7. Program Managers and Information Custodians In most cases, the authority within the agency or institution delegates custody of specific types of information maintained by the agency to administrators in the agency who may further delegate to employees in their organizations. These persons have direct responsibility for:
    - deciding issues pertaining to access to information
    - insuring information security
    - participating in preparing a disaster recovery plan.
8. Users of Electronic Assets. All authorized users shall be accountable for their actions relating to information assets, including hardware, software and electronic information. Information resources shall be used only for intended purposes as defined by the agency and consistent with applicable laws.
9. Information Technology Staff. Staff who are directly responsible for security, system management, and applications development have special privileges in relation to information resources such as the ability to examine the files of other users. People with access management rights must follow strict

procedures regarding their access to information resources and sharing that access with others.

10. Employees and persons under contract. Employees must become knowledgeable about their organization's security policies and procedures. Employees must exercise due diligence in following those procedures and incorporating sound security practices in the discharge of their normal duties.

### *G. Related Policies, Standards and Guidelines*

The Information Security Management Policy provides the general requirements for a set of policies, standards, and procedures to protect the information assets of an organization. Other information security policies address the specific topics of:

1. Access Control Policy
2. Disaster Recovery Policy
3. Education, Training and Awareness Policy
4. Individual Use Policy
   - Acceptable Use
   - Copyrighted Materials
   - E-mail Use
5. Network Security Policy
   - General Network Controls
   - Perimeter Security for Internet and Intranet Connections
   - Remote Access
6. Security Breaches / Incident Reporting Policy

| | |
|---|---|
| **Title** | **Education, Training and Awareness Policy** |
| **Category** | **Security Architecture** |
| **Date Adopted** | |
| **Date of Last Revision** | **October 31, 2000** |
| **Status** | **Draft Policy** |

## *A. Authority*

Section 86-1506 (6). "(The Nebraska Information Technology Commission shall) adopt minimum technical standards, guidelines, and architectures upon recommendation by the technical panel created in Section 86-1511."

## *B. Purpose and Objectives*

The purpose of this document is to define and clarify policies, principles, standards, guidelines, and responsibilities related to the security of the state's information technology resources.

A policy on Education, Training and Awareness is intended to support information security by communicating security needs, best practices, and procedures to all stakeholders. Adequate training of information technology staff is essential to effective implementation of security.

The primary objectives of the Education, Training and Awareness Policy are:

1. To communicate responsibilities for the Education, Training and Awareness of information security policies and procedures;
2. To provide adequate skills for technical staff responsible for implementing security procedures;
3. To establish specific requirements for achieving the goals of Education, Training, and Awareness.
4. To communicate the consequences of violations of security procedures.

Section D provides key definitions.
Section E explains applicability.
Section F describes roles and responsibilities.

## *C. Education, Training and Awareness Policy*

POLICY STATEMENT

The information security policies and procedures of the agency or institution will be communicated to all employees. Information security policy and procedures will be available for reference and review by employees, contractors, agents acting on behalf of the state and all others in a position to impact the security and integrity of the information assets of the state. A program to maintain effective awareness of information security policy, standards and acceptable practices will exist. Persons responsible for information technology resources must have adequate training on implementing proper security controls for the equipment, software, and networks under their control.

EXPLANATION

Established security policy and standards must be followed to achieve the intended level of information security, control and integrity.

Information security policy and standards are ineffective if individuals at any level of the organization are unaware of the importance of security policy, do not understand established standards or fail to perform required practices for any reason. Good security is "a state of mind" that can best be achieved by a program or process that reinforces the concern and appropriate actions on a regular and ongoing basis.

Without confirmation that all new and existing employees are aware of security policy there is no assurance that the desired actions are understood or followed. Failure to follow policy or practice standards for any reason reduces the value of such statements to "documents of prosecution" and negates the positive reinforcement and protective intent for which the information policy and standards exist.

Information Security is not a one-time event, nor is it a "volume of rules sitting on the shelf." Good security practices are not always obvious, intuitive or easily incorporated into established routines. To have maximum effectiveness information security standards must be known, understood, believed to have value, and appropriately and consistently practiced.

Effective information security is most nearly achieved when it is a part of everyone's thinking with regard to daily operations and assignments. A program that reinforces the organization's position with regard to handling the many aspects of information security provides the tone and commitment to support greater sensitivity to the potential of an unwanted compromise or loss of assets.

Ongoing and positive reinforcement for the necessity for information security policy and standards provides awareness and a "mind set" that encourages the intended practice of the established procedures. Without such reinforcement, policies or standards may be perceived as not relevant, necessary or valuable and may be "followed" but not be practiced in a manner that supports full effectiveness.

STANDARDS

1. All employees with access to computer systems must be informed of security policies and procedures and their responsibilities in writing. All new employees with access to critical systems or sensitive information will sign a statement acknowledging they have received and read the policy and understand their responsibilities. This should include knowledge of the consequences of violations of security procedures.
2. All users must be informed that any actions taken under their assigned identification (e.g., userid) are their responsibility.
3. A signed statement indicating awareness, compliance and intent of continued compliance with information security policy and standards will be required upon annual review of each employee with access to critical systems or sensitive information.

4. Important aspects of information security policy and standards will be communicated on a regular basis through postings, distributions, logon screens, meetings or other means that provide regular and useful reminders concerning information security policy and standards.
5. Contractors, agents acting on behalf of the state, auditors, and other non-employees in a position to impact the security or integrity of information assets of the state will be made aware of the Information Security Policy. These individuals must sign a statement acknowledging they have received and read the policy and understand their responsibilities.
6. Persons responsible for information technology resources must be aware of the information security policies and must be knowledgeable about effective security practices for the technical environment under their control.
7. The agency security officer will develop and disseminate guidelines and examples for users to assist them in maintaining good security practices. This material may include brochures, electronic reminders, desk references, web sites, etc., and should include but not be limited to information on passwords and password protection, logon id, virus protection strategies, etc.

### *D. Key Definitions*

1. Agency shall mean any governmental entity, including state government, local government, or third party entities under contract to the agency.
2. Critical Systems are those systems or system components (hardware, data, or software) that if lost or compromised would jeopardize the ability of the system to continue processing.
3. Disaster refers to any event that threatens the destruction of information or availability of computer systems. A disaster may affect the physical security of computer systems, including equipment failures, fire, flood, other natural calamities, or theft of equipment. A disaster may involve destruction or information or availability of computer systems due to system failure, human error, or intentional acts including computer crimes.
4. E-mail is the exchange and or sharing of messages, attachments, and calendar and scheduling information.
5. Information Security is the protection of data against accidental or malicious destruction, modification or disclosure.
6. Security Policy is a statement of the goals, responsibilities, and accepted behaviors required for maintaining a secure environment. Security policies set the direction, give broad guidance and demonstrate senior management support for security-related facilities and actions across the organization.
7. Security Standard is a set of tasks, responsibilities, or guidelines that provide metrics to policies. Security procedures are standards that are very specific in nature, applying to group or individual systems. Procedures are directive in nature, whereas policies provide principles.
8. Sensitive Information is that information which must be protected to insure only authorized access or if lost or compromised might negatively affect the owner of the information or require substantial resources to recreate.
9. State Data Communications Network (SDCN) shall mean any data communications facility contracted for or provided by the State of Nebraska,

including State-provided Internet access and network connections to state computers.

10. Users of electronic assets include any employee, business partner, contractor, consultant, or customer who is authorized to use the information technology assets of a state agency or institution.
11. Value of information includes the cost of collection, cost of reconstruction, and legal or operational consequences if information is lost or compromised.

## *E. Applicability*

GENERAL STATEMENT

These policies are intended to be sufficiently generic to apply to a wide range of governmental and educational agencies in the State of Nebraska. Each agency or operational entity must develop detailed procedures to implement broad policies and standards. Compliance with these security policies and standards will be a requirement during consideration of funding for any projects requiring review by the NITC. Compliance may be used in audit reviews or budget reviews.

EXCEPTION STATEMENT

"Computer security must support the mission of the organization." "The expense of security safeguards must be cost effective and commensurate with the value of the assets being protected." "Owners of sensitive information and critical systems have security responsibilities outside their organization." (From the Information Security Management Policy)

These three principles provide the basis for determining the applicability of security policies and standards to specific situations within an organization. The responsible security authority of an organization should establish a two-step test, before exempting a unit within the organization from a particular security requirement. The first test is met, if a security requirement is contrary to the organization's mission or is not cost-effective given the value of the assets being protected. The second test is met, if exempting a security requirement does not create unreasonable risk of adverse consequences to people or entities outside of the organization. Both tests should be met.

COMPLIANCE AND ENFORCEMENT STATEMENT

The governing board or chief administrative officer of each organization must develop internal compliance and enforcement policies as part of its information security program. Such policies should be effective and commensurate with the risks involved. The NITC intends to incorporate adherence to security policies as part of its evaluation and prioritization of funding requests. The NITC recommends that the Governor and Legislature give due consideration to requests for security improvements during the budget process.

## *F. Responsibility*

An effective security program involves cooperation of many different entities. Major participants and their responsibilities include:

1. Nebraska Information Technology Commission. The NITC provides strategic direction for state agencies and educational institutions in the area of

information technology. The NITC also has statutory responsibility to adopt minimum technical standards and guidelines for acceptable and cost-effective use of information technology. Implicit in these requirements is the responsibility to promote adequate security of information systems through adoption of policies, standards, and guidelines. The NITC must develop strategies for implementing and evaluating the effectiveness of information security programs.

2. Technical Panel Security Work Group. 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.
3. Chief Information Officer, State of Nebraska. The CIO has the responsibility to assist in building the business case for cost-effective implementation of security programs in non-education state agencies. The CIO must also work with non-education state agencies to coordinate and evaluate security programs. The CIO shall insure that non-education state agencies have documented procedures to demonstrate compliance with these security policies.
4. Agency and Institutional Heads. The highest authority within an agency or institution is responsible for the protection of information resources, including developing and implementing information security programs consistent with this policy. The authority may delegate this responsibility but delegation does not remove the accountability.
5. Agency Information Officer. In most cases, the highest authority within an agency or institution delegates the general responsibility for security of the agency's information technology resources to the agency's highest ranking information technology professional. This responsibility includes development and promulgation of agency-specific information security policies.
6. Agency Security Officer. In some cases, the Agency Information Officer assigns an Agency Security Officer who is responsible for:
    - Implementing enterprise and agency-specific or application-specific security policies and procedures.
    - Developing procedures and administering the information access control decisions made by information custodians within the agency.
    - Identifying training requirements.
    - Implementing procedures for authentication of users and messages.
    - Publish guidelines for creating and managing passwords.
    - Developing and implementing strategies to make users aware of security policies, procedures and benefits.
    - Documenting the security support structure across platforms.
    - Enforcing agency security policies.
    - Establishing and chairing agency security committees.
    - Monitoring unusual activities and report security breaches and incidents.
    - Periodically evaluating effectiveness of security policies and procedures.

- Fact gathering and analysis on information security issues.
- Developing recommendations for the agency or institution on security matters.
- Reviewing changes to the configuration of security administration facilities and settings.
- Participate in preparing a disaster recovery plan. They must understand the risks posed by disruption of computer systems. They must help prepare contingencies and be ready to implement the disaster recovery plan.

The Agency Security Officer may work with a security committee of the agency or institution. The Security Committee is an advisory group made up of key technical and management personnel within the agency to coordinate security efforts and resolve security problems.

7. Program Managers and Information Custodians In most cases, the authority within the agency or institution delegates custody of specific types of information maintained by the agency to administrators in the agency who may further delegate to employees in their organizations. These persons have direct responsibility for:
   - deciding issues pertaining to access to information
   - insuring information security
   - participating in preparing a disaster recovery plan.
8. Users of Electronic Assets. All authorized users shall be accountable for their actions relating to information assets, including hardware, software and electronic information. Information resources shall be used only for intended purposes as defined by the agency and consistent with applicable laws.
9. Information Technology Staff. Staff who are directly responsible for security, system management, and applications development have special privileges in relation to information resources such as the ability to examine the files of other users. People with access management rights must follow strict procedures regarding their access to information resources and sharing that access with others.
10. Employees and persons under contract. Employees must become knowledgeable about their organization's security policies and procedures. Employees must exercise due diligence in following those procedures and incorporating sound security practices in the discharge of their normal duties.

### *G. Related Policies, Standards and Guidelines*

The Information Security Management Policy provides the general requirements for a set of policies, standards, and procedures to protect the information assets of an organization. Other information security policies address the specific topics of:

1. Access Control Policy
2. Disaster Recovery Policy
3. Education, Training and Awareness Policy
4. Individual Use Policy
   - Acceptable Use
   - Copyrighted Materials
   - E-mail Use

5. Network Security Policy
   - General Network Controls
   - Perimeter Security for Internet and Intranet Connections
   - Remote Access
6. Security Breaches / Incident Reporting Policy

| | |
|---|---|
| **Title** | **Security Breaches and Incident Reporting Policy** |
| **Category** | **Security Architecture** |
| **Date Adopted** | |
| **Date of Last Revision** | **October 31, 2000** |
| **Status** | **Draft Policy** |

## *A. Authority*

Section 86-1506 (6). "(The Nebraska Information Technology Commission shall) adopt minimum technical standards, guidelines, and architectures upon recommendation by the technical panel created in Section 86-1511."

## *B. Purpose and Objectives*

The purpose of this document is to define and clarify policies, principles, standards, guidelines, and responsibilities related to the security of the state's information technology resources.

A policy on security breaches and incident reporting is intended to support information security by documenting security violations and taking actions to discourage or apprehend those who are responsible. The ultimate goal of this policy is the protection of state assets, containment of damage, and restoration of service. Secondary goals are dependent on the category of violation.

The primary objectives of the Network Security Policy are:

1. To document security violations and incidents;
2. To share information on security problems with other system managers;
3. To cooperate with state and federal law enforcement.
4. To communicate responsibilities implementing this policy;

Section D provides key definitions.
Section E explains applicability.
Section F describes roles and responsibilities.

## *C. Security Breaches and Incident Reporting Policy*

POLICY STATEMENT

Agencies and institutions shall prepare procedures for monitoring, investigating and reporting security breaches and incidents. Security breaches shall be investigated promptly and documented. If criminal action is suspected, the agency or institution must contact the appropriate law enforcement and investigative authorities as quickly as possible. Agencies and institutions shall cooperate with local and national programs for reporting security incidents. The policies and standards pertaining to access controls, acceptable use, education and network security shall apply.

EXPLANATION

Security is a growing problem. Collective action is required to counteract security violations and activities that lead to security breaches. Agency management, law

enforcement, and others must know the extent of security problems. Quick reporting of some incidents, such as new viruses, is essential to stopping them from spreading and impacting other systems. Reporting computer crimes is the only way for law enforcement to deter and apprehend violators.

Not all agencies or institutions have the resources to conduct their own intrusion detection and analysis. In these situations, it may be necessary to identify other sources for assistance in tracking and responding to incidents. It is important to have a clear understanding of when to escalate an issue.

STANDARDS

1. All users of agency information technology resources must receive education and training on security issues, obligations, procedures, and consequences of violations.
2. Agencies and institutions shall provide for the following security measures:
   a. Reviewing and analyzing incident tracking databases;
   b. Reporting and documenting security incidents to the appropriate level of management;
   c. Implementing procedures for logging information on intrusion attempts and storing that information in a manner for later analysis or use by law enforcement.
   d. When appropriate, notifying the workforce of known incidents and precautionary measures that are being taken;
   e. Reporting incidents to local and national organizations.
3. Agencies and institutions shall report potential criminal violations to the Nebraska State Patrol and the Federal Bureau of Investigation.
4. In addition to the general reporting requirements stated above, the following requirements pertain to specific categories of security breaches:
   a. For catastrophic disasters such as fire, bomb threats, hostage situations, floods or destructive storms, the goals of employee safety and damage containment apply. Notification procedures will include the appropriate public service departments (Fire Department or Police Department).
   b. For intrusion of secured areas, the goals of employee safety, intruder identification, and if warranted, the intruder's removal from the premises apply. Notification procedures will include building security or local police.
   c. For cases involving electronic intrusion, the goals of data integrity, data recovery, method of breach and intruder identification apply. Notification procedures could include the State Patrol (if deemed serious enough), the potentially affected business area manager, software application support manager, and data center manager. Any activity monitor data, collected as a normal part of doing business, should be kept until the incident has been cleared.
   d. For cases involving deception and fraud, the goal of identifying the perpetrator applies.

### *D. Key Definitions*

1. Agency shall mean any governmental entity, including state government, local government, or third party entities under contract to the agency.

2. Critical Systems are those systems or system components (hardware, data, or software) that if lost or compromised would jeopardize the ability of the system to continue processing.
3. Disaster refers to any event that threatens the destruction of information or availability of computer systems. A disaster may affect the physical security of computer systems, including equipment failures, fire, flood, other natural calamities, or theft of equipment. A disaster may involve destruction or information or availability of computer systems due to system failure, human error, or intentional acts including computer crimes.
4. E-mail is the exchange and or sharing of messages, attachments, and calendar and scheduling information.
5. Information Security is the protection of data against accidental or malicious destruction, modification or disclosure.
6. Security Policy is a statement of the goals, responsibilities, and accepted behaviors required for maintaining a secure environment. Security policies set the direction, give broad guidance and demonstrate senior management support for security-related facilities and actions across the organization.
7. Security Standard is a set of tasks, responsibilities, or guidelines that provide metrics to policies. Security procedures are standards that are very specific in nature, applying to group or individual systems. Procedures are directive in nature, whereas policies provide principles.
8. Sensitive Information is that information which must be protected to insure only authorized access or if lost or compromised might negatively affect the owner of the information or require substantial resources to recreate.
9. State Data Communications Network (SDCN) shall mean any data communications facility contracted for or provided by the State of Nebraska, including State-provided Internet access and network connections to state computers.
10. Users of electronic assets include any employee, business partner, contractor, consultant, or customer who is authorized to use the information technology assets of a state agency or institution.
11. Value of information includes the cost of collection, cost of reconstruction, and legal or operational consequences if information is lost or compromised.

## *E. Applicability*

GENERAL STATEMENT

These policies are intended to be sufficiently generic to apply to a wide range of governmental and educational agencies in the State of Nebraska. Each agency or operational entity must develop detailed procedures to implement broad policies and standards. Compliance with these security policies and standards will be a requirement during consideration of funding for any projects requiring review by the NITC. Compliance may be used in audit reviews or budget reviews.

EXCEPTION STATEMENT

"Computer security must support the mission of the organization." "The expense of security safeguards must be cost effective and commensurate with the value of the assets being protected." "Owners of sensitive information and critical systems have

security responsibilities outside their organization." (From the Information Security Management Policy, below.)

These three principles provide the basis for determining the applicability of security policies and standards to specific situations within an organization. The responsible security authority of an organization should establish a two-step test, before exempting a unit within the organization from a particular security requirement. The first test is met, if a security requirement is contrary to the organization's mission or is not cost-effective given the value of the assets being protected. The second test is met, if exempting a security requirement does not create unreasonable risk of adverse consequences to people or entities outside of the organization. Both tests should be met.

COMPLIANCE AND ENFORCEMENT STATEMENT

The governing board or chief administrative officer of each organization must develop internal compliance and enforcement policies as part of its information security program. Such policies should be effective and commensurate with the risks involved. The NITC intends to incorporate adherence to security policies as part of its evaluation and prioritization of funding requests. The NITC recommends that the Governor and Legislature give due consideration to requests for security improvements during the budget process.

### *F. Responsibility*

An effective security program involves cooperation of many different entities. Major participants and their responsibilities include:

1. Nebraska Information Technology Commission. The NITC provides strategic direction for state agencies and educational institutions in the area of information technology. The NITC also has statutory responsibility to adopt minimum technical standards and guidelines for acceptable and cost-effective use of information technology. Implicit in these requirements is the responsibility to promote adequate security of information systems through adoption of policies, standards, and guidelines. The NITC must develop strategies for implementing and evaluating the effectiveness of information security programs.
2. Technical Panel Security Work Group. 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.
3. Chief Information Officer, State of Nebraska. The CIO has the responsibility to assist in building the business case for cost-effective implementation of security programs in non-education state agencies. The CIO must also work with non-education state agencies to coordinate and evaluate security programs. The CIO shall insure that non-education state agencies have documented procedures to demonstrate compliance with these security policies.
4. Agency and Institutional Heads. The highest authority within an agency or institution is responsible for the protection of information resources, including developing and implementing information security programs consistent with

this policy. The authority may delegate this responsibility but delegation does not remove the accountability.

5. Agency Information Officer. In most cases, the highest authority within an agency or institution delegates the general responsibility for security of the agency's information technology resources to the agency's highest ranking information technology professional. This responsibility includes development and promulgation of agency-specific information security policies.
6. Agency Security Officer. In some cases, the Agency Information Officer assigns an Agency Security Officer who is responsible for:
    - Implementing enterprise and agency-specific or application-specific security policies and procedures.
    - Developing procedures and administering the information access control decisions made by information custodians within the agency.
    - Identifying training requirements.
    - Implementing procedures for authentication of users and messages.
    - Publish guidelines for creating and managing passwords.
    - Developing and implementing strategies to make users aware of security policies, procedures and benefits.
    - Documenting the security support structure across platforms.
    - Enforcing agency security policies.
    - Establishing and chairing agency security committees.
    - Monitoring unusual activities and report security breaches and incidents, including identifying resources to assist with tracking, analysis, and responding to incidents.
    - Periodically evaluating effectiveness of security policies and procedures.
    - Fact gathering and analysis on information security issues.
    - Developing recommendations for the agency or institution on security matters.
    - Reviewing changes to the configuration of security administration facilities and settings.
    - Participate in preparing a disaster recovery plan. They must understand the risks posed by disruption of computer systems. They must help prepare contingencies and be ready to implement the disaster recovery plan.

    The Agency Security Officer may work with a security committee of the agency or institution. The Security Committee is an advisory group made up of key technical and management personnel within the agency to coordinate security efforts and resolve security problems.
7. Program Managers and Information Custodians In most cases, the authority within the agency or institution delegates custody of specific types of information maintained by the agency to administrators in the agency who may further delegate to employees in their organizations. These persons have direct responsibility for:
    - deciding issues pertaining to access to information
    - insuring information security

- participating in preparing a disaster recovery plan.

8. Users of Electronic Assets. All authorized users shall be accountable for their actions relating to information assets, including hardware, software and electronic information. Information resources shall be used only for intended purposes as defined by the agency and consistent with applicable laws.
9. Information Technology Staff. Staff who are directly responsible for security, system management, and applications development have special privileges in relation to information resources such as the ability to examine the files of other users. People with access management rights must follow strict procedures regarding their access to information resources and sharing that access with others.
10. Employees and persons under contract. Employees must become knowledgeable about their organization's security policies and procedures. Employees must exercise due diligence in following those procedures and incorporating sound security practices in the discharge of their normal duties.

### *G. Related Policies, Standards and Guidelines*

The Information Security Management Policy provides the general requirements for a set of policies, standards, and procedures to protect the information assets of an organization. Other information security policies address the specific topics of:

1. Access Control Policy
2. Disaster Recovery Policy
3. Education, Training and Awareness Policy
4. Individual Use Policy
   - Acceptable Use
   - Copyrighted Materials
   - E-mail Use
5. Network Security Policy
   - General Network Controls
   - Perimeter Security for Internet and Intranet Connections
   - Remote Access
6. Security Breaches / Incident Reporting Policy

| | |
|---|---|
| **Title** | **Individual Use Policy** |
| **Category** | **Security Architecture** |
| **Date Adopted** | |
| **Date of Last Revision** | **October 31, 2000** |
| **Status** | **Draft Policy** |

## *A. Authority*

Section 86-1506 (6). "(The Nebraska Information Technology Commission shall) adopt minimum technical standards, guidelines, and architectures upon recommendation by the technical panel created in Section 86-1511."

## *B. Purpose and Objectives*

The purpose of this document is to define and clarify policies, principles, standards, guidelines, and responsibilities related to the security of the state's information technology resources.

A policy on individual use is intended to support information security by reducing exposure to security problems and insuring proper use of publicly owned communications facilities. This policy addresses use of computers and communication resources for e-mail, Internet, and copyright protected information.

The primary objectives of the Individual Use Policy are:

1. To communicate responsibilities for the education and awareness of information security policies and procedures;
2. To establish specific requirements for acceptable use of state-owed resources;
3. To reduce exposure to security risks associated with e-mail;
4. To reduce exposure to legal liability because of wrongful acts committed by employees using information technology resources of the agency;
5. To establish specific requirements pertaining to the use of copyright protected materials.

Section D provides key definitions.
Section E explains applicability.
Section F describes roles and responsibilities.

## *C. Individual Use Policy*

POLICY STATEMENT

*General Statement*

Agencies and institutions must adopt policies governing the use of computer and communication facilities by individuals. Like all communications conducted on behalf of the State of Nebraska, users must exercise good judgement in Internet, e-mail and other use of state computing and communication facilities. Use of the Internet, e-mail, and other actions must always be able to withstand public scrutiny without legal liability or embarrassment to the agency or institution.

EXPLANATION

The use of e-mail has become a mission critical function for most state agencies. As such, it must be operational 24 hours a day - 7 days/week - 52 weeks/year. In order to achieve this it must be operated in a secure and managed environment.

Courts have found organizations and their officers liable for copyright infringement where unauthorized copies were used to the organizations benefit -- even when the copying of software or other copyrighted material was done without management's knowledge.

Improper use of e-mail and the Internet detract from performance of duties and subjects agencies and institutions to potential legal action. Careless use of e-mail and the Internet can subject other users to security problems such as viruses.

STANDARDS

1. *General Requirement*
   a. All computers of critical systems or systems with sensitive information shall display a log-in warning, such as the following message:
      "THIS IS A GOVERNMENT COMPUTER SYSTEM. UNAUTHORIZED ACCESS IS PROHIBITED. ANYONE USING THIS SYSTEM IS SUBJECT TO MONITORING. UNAUTHORIZED ACCESS OR ATTEMPTS TO USE, ALTER, DESTROY OR DAMAGE DATA, PROGRAMS OR EQUIPMENT COULD RESULT IN CRIMINAL PROSECUTION. USERS MUST COMPLY WITH POLICIES PERTAINING TO E-MAIL, INTERNET, AND OTHER USES."
   b. Agencies should develop policies regarding monitoring e-mail, Internet use, and other computer resources. The policies should identify the circumstances under which monitoring will occur and who may authorize such monitoring.

2. *E-mail:*
   a. Agencies, in coordination with the manager of the central mail address directory, must provide an appropriate e-mail system that allows authorized state employees, upon proper authentication, to easily exchange business-related information in a secure and managed manner.
   b. The manager of the state's central address directory will provide the single point of entry for all state e-mail post offices other than the SMTP mail servers.
   c. Agencies shall employ virus protection software on workstations to prevent transmission of viruses in e-mail attachments and diskettes.
   d. In agencies that use central e-mail systems, managers of mail servers shall employ virus protection software to prevent transmission of viruses in e-mail attachments.
   e. E-mail shall be used for business purposes, only.
   f. E-mail that is not secure or encrypted should not be used to send private or confidential information.

3. *Protection of Software and Other Copyrighted Material:*
   Users must comply with copyright laws. Agencies and institutions must communicate this policy to users. Agencies shall designate a single point of contact for inquiries about copyright violations, pursuant to federal law.

   Agency policies should convey that:
   a. Documents or software protected by copyright may only be copied with the written permission of the copyright holder;
   b. Any unauthorized reproduction of the copyrighted material may subject the responsible employee to disciplinary action, civil liability, or both;
   c. The state and/or agency is not obligated to defend or indemnify employees in actions based on copyright violation; and
   d. The agency policy may include statements such as the following suggested by the Software Publishers Association:
   e. "According to the U.S. Copyright Law, illegal reproduction of software can be subject to civil damages of as much as $100,000, and criminal penalties, including fines and imprisonment. (Agency) employees who make, acquire or use unauthorized copies of computer software shall be disciplined as appropriate under the circumstances. Such discipline may include termination. (Agency) does not condone the illegal duplication of software."

4. *Acceptable Use:*
   Each agency or institution or affiliate organization using the State Data Communications Network SDCN is responsible for the activity of its users and for ensuring that its users are familiar with this policy. Unacceptable uses of the SDCN include:
   a. Violation of the privacy of other users and their data. For example, users shall not intentionally seek information on, obtain copies of, or modify files, other data or passwords belonging to other users, or represent themselves as another user unless explicitly authorized to do so by that user.
   b. Violation of the legal protection provided by copyright and licensing laws applied to programs and data. It is assumed that information and resources available via the SDCN are private to those individuals and organizations owning or holding rights to such information and resources, unless specifically stated otherwise by the owners or holders, or unless such information and resources clearly fall within the statutory definition of a public record. It is unacceptable for an individual to use the SDCN to gain access to information or resources not considered a public record without the granting of permission to do so by the owners or holders of rights to such information or resources.
   c. Downloading of software in violation of license agreements.
   d. Violation of the integrity of computing systems. For example, users shall not intentionally develop programs that harass other users or infiltrate a computer or computing system and/or damage or alter the software components of a computer or computing system.
   e. Use of the SDCN for fund-raising or public relations activities unrelated to an individual's employment by the State of Nebraska.

f. Use inconsistent with laws, regulations or accepted community standards. Transmission of material in violation of any local, state or federal law or regulation is prohibited. It is not acceptable to transmit or knowingly receive threatening, obscene or harassing material.
g. Malicious or disruptive use, including use of the SDCN or any attached network in a manner that precludes or significantly hampers its use by others. Disruptions include, but are not limited to, distribution of unsolicited advertising, propagation of computer worms or viruses, and use of the SDCN to make unauthorized entry to any other machine accessible via the network.
h. Unsolicited advertising, unless authorized by the governing body of the organization.
i. Use of the SDCN for recreational games.
j. Use in conjunction with for-profit or activities, unless such activities are stated as a specifically acceptable use.
k. Use for private or personal business.
l. Misrepresentation of one's self, an agency, or the State of Nebraska when using the SDCN.
m. Accessing or attempting to access another individual's data or information without proper authorization;
n. Obtaining, possessing, using or attempting to use someone else's password regardless of how the password was obtained;
o. Making more copies of licensed software than allowed;
p. Sending an overwhelming number of files across the network (e.g. spamming or e-mail bombing);
q. Releasing a virus or other program that damages, harms, or disrupts a system or network;
r. Preventing others from accessing services;
s. Unauthorized use of state resources;
t. Sending forged messages under someone else's userid;
u. Using state resources for unauthorized or illegal purposes;
v. Unauthorized access to data or files even if they are not securely protected.

### *D. Key Definitions*

1. Agency shall mean any governmental entity, including state government, local government, or third party entities under contract to the agency.
2. Critical Systems are those systems or system components (hardware, data, or software) that if lost or compromised would jeopardize the ability of the system to continue processing.
3. Disaster refers to any event that threatens the destruction of information or availability of computer systems. A disaster may affect the physical security of computer systems, including equipment failures, fire, flood, other natural calamities, or theft of equipment. A disaster may involve destruction or information or availability of computer systems due to system failure, human error, or intentional acts including computer crimes.
4. E-mail is the exchange and or sharing of messages, attachments, and calendar and scheduling information.
5. Information Security is the protection of data against accidental or malicious destruction, modification or disclosure.

6. Security Policy is a statement of the goals, responsibilities, and accepted behaviors required for maintaining a secure environment. Security policies set the direction, give broad guidance and demonstrate senior management support for security-related facilities and actions across the organization.
7. Security Standard is a set of tasks, responsibilities, or guidelines that provide metrics to policies. Security procedures are standards that are very specific in nature, applying to group or individual systems. Procedures are directive in nature, whereas policies provide principles.
8. Sensitive Information is that information which must be protected to insure only authorized access or if lost or compromised might negatively affect the owner of the information or require substantial resources to recreate.
9. State Data Communications Network (SDCN) shall mean any data communications facility contracted for or provided by the State of Nebraska, including State-provided Internet access and network connections to state computers.
10. Users of electronic assets include any employee, business partner, contractor, consultant, or customer who is authorized to use the information technology assets of a state agency or institution.
11. Value of information includes the cost of collection, cost of reconstruction, and legal or operational consequences if information is lost or compromised.

## *E. Applicability*

GENERAL STATEMENT

These policies are intended to be sufficiently generic to apply to a wide range of governmental and educational agencies in the State of Nebraska. Each agency or operational entity must develop detailed procedures to implement broad policies and standards. Compliance with these security policies and standards will be a requirement during consideration of funding for any projects requiring review by the NITC. Compliance may be used in audit reviews or budget reviews.

EXCEPTION STATEMENT

"Computer security must support the mission of the organization." "The expense of security safeguards must be cost effective and commensurate with the value of the assets being protected." "Owners of sensitive information and critical systems have security responsibilities outside their organization." (From the Information Security Management Policy, below.)

These three principles provide the basis for determining the applicability of security policies and standards to specific situations within an organization. The responsible security authority of an organization should establish a two-step test, before exempting a unit within the organization from a particular security requirement. The first test is met, if a security requirement is contrary to the organization's mission or is not cost-effective given the value of the assets being protected. The second test is met, if exempting a security requirement does not create unreasonable risk of adverse consequences to people or entities outside of the organization. Both tests should be met.

COMPLIANCE AND ENFORCEMENT STATEMENT

The governing board or chief administrative officer of each organization must develop internal compliance and enforcement policies as part of its information security program. Such policies should be effective and commensurate with the risks involved. The NITC has no operational responsibilities, but intends to incorporate adherence to security policies as part of its evaluation and prioritization of funding requests. The NITC recommends that the Governor and Legislature give due consideration to requests for security improvements during the budget process.

### *F. Responsibility*

An effective security program involves cooperation of many different entities. Major participants and their responsibilities include:

1. Nebraska Information Technology Commission. The NITC provides strategic direction for state agencies and educational institutions in the area of information technology. The NITC also has statutory responsibility to adopt minimum technical standards and guidelines for acceptable and cost-effective use of information technology. Implicit in these requirements is the responsibility to promote adequate security of information systems through adoption of policies, standards, and guidelines. The NITC must develop strategies for implementing and evaluating the effectiveness of information security programs.
2. Technical Panel Security Work Group. 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.
3. Chief Information Officer, State of Nebraska. The CIO has the responsibility to assist in building the business case for cost-effective implementation of security programs in non-education state agencies. The CIO must also work with non-education state agencies to coordinate and evaluate security programs. The CIO shall insure that non-education state agencies have documented procedures to demonstrate compliance with these security policies.
4. Agency and Institutional Heads. The highest authority within an agency or institution is responsible for the protection of information resources, including developing and implementing information security programs consistent with this policy. The authority may delegate this responsibility but delegation does not remove the accountability.
5. Agency Information Officer. In most cases, the highest authority within an agency or institution delegates the general responsibility for security of the agency's information technology resources to the agency's highest ranking information technology professional. This responsibility includes development and promulgation of agency-specific information security policies.
6. Agency Security Officer. In some cases, the Agency Information Officer assigns an Agency Security Officer who is responsible for:
    - Implementing enterprise and agency-specific or application-specific security policies and procedures.
    - Developing procedures and administering the information access control decisions made by information custodians within the agency.

- Identifying training requirements.
- Implementing procedures for authentication of users and messages.
- Publish guidelines for creating and managing passwords.
- Developing and implementing strategies to make users aware of security policies, procedures and benefits.
- Documenting the security support structure across platforms.
- Enforcing agency security policies.
- Establishing and chairing agency security committees.
- Monitoring unusual activities and report security breaches and incidents.
- Periodically evaluating effectiveness of security policies and procedures.
- Fact gathering and analysis on information security issues.
- Developing recommendations for the agency or institution on security matters.
- Reviewing changes to the configuration of security administration facilities and settings.
- Participate in preparing a disaster recovery plan. They must understand the risks posed by disruption of computer systems. They must help prepare contingencies and be ready to implement the disaster recovery plan.

The Agency Security Officer may work with a security committee of the agency or institution. The Security Committee is an advisory group made up of key technical and management personnel within the agency to coordinate security efforts and resolve security problems.

7. Program Managers and Information Custodians In most cases, the authority within the agency or institution delegates custody of specific types of information maintained by the agency to administrators in the agency who may further delegate to employees in their organizations. These persons have direct responsibility for:
    - deciding issues pertaining to access to information
    - insuring information security
    - participating in preparing a disaster recovery plan.
8. Users of Electronic Assets. All authorized users shall be accountable for their actions relating to information assets, including hardware, software and electronic information. Information resources shall be used only for intended purposes as defined by the agency and consistent with applicable laws.
9. Information Technology Staff. Staff who are directly responsible for security, system management, and applications development have special privileges in relation to information resources such as the ability to examine the files of other users. People with access management rights must follow strict procedures regarding their access to information resources and sharing that access with others.
10. Employees and persons under contract. Employees must become knowledgeable about their organization's security policies and procedures. Employees must exercise due diligence in following those procedures and incorporating sound security practices in the discharge of their normal duties.

### *G. Related Policies, Standards and Guidelines*

The Information Security Management Policy provides the general requirements for a set of policies, standards, and procedures to protect the information assets of an organization. Other information security policies address the specific topics of:

1. Access Control Policy
2. Disaster Recovery Policy
3. Education, Training and Awareness Policy
4. Individual Use Policy
   - Acceptable Use
   - Copyrighted Materials
   - E-mail Use
5. Network Security Policy
   - General Network Controls
   - Perimeter Security for Internet and Intranet Connections
   - Remote Access
6. Security Breaches / Incident Reporting Policy

| | |
|---|---|
| **Title** | **Network Security Policy** |
| **Category** | **Security Architecture** |
| **Date Adopted** | |
| **Date of Last Revision** | **October 31, 2000** |
| **Status** | **Draft Policy** |

### *A. Authority*

Section 86-1506 (6). "(The Nebraska Information Technology Commission shall) adopt minimum technical standards, guidelines, and architectures upon recommendation by the technical panel created in Section 86-1511."

### *B. Purpose and Objectives*

The purpose of this document is to define and clarify policies, principles, standards, guidelines, and responsibilities related to the security of the state's information technology resources.

A policy on network security is intended to support information security by reducing exposure to security problems when providing remote access to computer networks, allowing connections to the Internet, using the Internet or an Intranet to deliver information or services, and connecting networks.

The primary objectives of the Network Security Policy are:

1. To protect the integrity of networks operated by state agencies and institutions from unauthorized access and fraudulent use and /or abuse.
2. To communicate responsibilities implementing the network security policy;
3. To reduce exposure to security risks associated with remote access, Internet use, and connecting networks;
4. To monitor network use.

Section D provides key definitions.
Section E explains applicability.
Section F describes roles and responsibilities.

### *C. Network Security Policy*

POLICY STATEMENT

State agencies and institutions shall manage networks in a manner that insures their proper use, prevents unauthorized access or use, maintains availability and protects the security of information resources. State agencies and institutions shall establish controls that are commensurate to the security needs of the information and computer resources on the network. Controls shall also reflect the security needs of other agencies or institutions connected to the network.

Internet and Intranet sites must be protected from intrusion so that an unauthorized individual cannot alter data and information or compromise the integrity of state controlled networks. Intranet sites must be further protected by user-Ids and passwords or other unique identifier so that access by unauthorized individuals is not

allowed. The policy and standards set forth in the Individual Use and Access Policies will apply.

EXPLANATION

Networks allow sharing of information, applications, and other computer resources. Dependence on networks requires availability 24 hours per day, every day of the year. Integrity and confidentiality are paramount. Networks also represent major points of vulnerability to a large range of security problems. Public networks such as the Internet compound the security threat. Remote access, connections between networks, Internet access by workstations on the network, Internet access to information and services, and other configurations make network security a complex problem.

Internet or Intranet connections pose a risk of unauthorized access to state maintained data by compromising the integrity and privacy (where appropriate) of data. Potential consequences of unauthorized access include altering, erasing, or otherwise rendering the information invalid or unavailable by manipulating the data or the underlying programs.

TCP/IP is becoming the universal communications protocol for all computer systems, whether internal or external, by employees or customers. This exposes any connected computer to potential malicious attacks from anonymous persons anywhere in the world. Sufficient security controls are needed to provide access to those who have the need and keep out those who do not, while maintaining public trust and confidence.

Currently there are many unsecured entry points servers called "ports" (such as SMTP gateways) in systems across various state agencies. When no policies or standards in place, all state applications are at risk of being penetrated or attacked with results varying from denial of service to loss of data and confidentiality.

STANDARDS

1. General Network Controls. Network resources participating in the access of sensitive information or critical systems shall assume the security level of that information for the duration of the session. Controls shall be implemented commensurate with the highest risk. All network components must be identifiable and restricted to their intended use. Specific standards and guidelines include:
    a. Password protected screen savers, terminal lock and key, or terminal software locking options will be enabled on each terminal so that access can be controlled by locking the terminal while it is unattended.
    b. All line junction points (cable and line facilities) should be located in secure areas or under lock and key).
    c. Control units, concentrators, multiplexers switches, hubs, and front-end processors will be protected from unauthorized physical access.
    d. Procedures will be implemented which ensure that access to data or information is not dependent on any individual. There should be more than one person with authorized access.

e. Some types of network protocol analyzers and test equipment are capable of monitoring (and some, altering) data passed over the network. Use of such equipment will be tightly controlled, since it can emulate terminals, monitor and modify sensitive information, or contaminate both encrypted and unencrypted data.
f. The network manager must maintain up-to-date diagrams showing all major network components, to maintain an inventory of all network connections, and ensure that all unneeded connections are disabled.
g. Default passwords on network hardware, such as routers, should be changed immediately after the hardware is installed. Security updates and patches for software should be kept current.
h. The network manager must maintain a list of all approved dial access modems. The network manager should establish a procedure that periodically checks for any unapproved modems that have been added to the network.
i. The network manager must periodically monitor sharing and trusting relationships for connecting with other networks to ensure they are still valid.
j. An audit of network security should be conducted annually.

2. Perimeter Security (for Internet and Intranet Connections). Perimeter security protects a network by controlling access to all entry and exit points. Perimeter security must be managed as a mission critical infrastructure. Specific standards include:
    a. Agencies and institutions shall manage the security for all points of entry to and from the state's network. Customers with all WAN connections provided and managed by a central network manager are considered "internal networks" located within the secure network perimeter boundary. Additional WAN connections that are not provided by the central network manager may be considered "internal networks" if they are authorized and approved by the central network manager. Customers with connections that are not managed by the central network manager must comply with perimeter security procedures established by the central network manager in order to connect to the network.
    b. The central network manager shall develop and use an on-going process to assess vulnerability of the network and risk in order to maintain adequate perimeter security controls. The central network manger and customer representatives must work together to address ways to meet customer business needs within a secured environment.
    c. Entry controls -- Appropriate access controls such as identification, authentication, certification, and authorization must be implemented to control entry to the network.
    d. Monitoring -- A program of continuous tracking, detection, and monitoring with audit trail and reporting is required for all network entry and exit points. This program must contain procedures for adequate and timely response to intruders.
    e. Operations -- Perimeter security is required 24 hours per day, every day of the year in order to support continuous business operations.

f. Implementation -- The central network manager shall work with customers to develop operating procedures and business rules needed to implement perimeter protection.
g. Managing Risk -- Security for a connected network should reflect the security requirements of the highest risk elements on the network.

3. Remote Access. Remote access to State of Nebraska computer resources and information shall be controlled to insure the integrity, availability and confidentiality (according to the sensitivity and criticality) of the information stored within, processed by or transmitted by a system. Specific standards include:
   a. To determine the appropriate level of security investment, a risk assessment is performed to estimate the magnitude of harm resulting from the loss, misuse, or unauthorized access to or modification of information in any state system. Included are considerations of the major factors of risk management: the value of the system or application, threats, vulnerabilities, and the effectiveness of current or proposed safeguards.
   b. To apply these standards consistently, categories should be established to rank systems and applications according to the criticality and sensitivity of the information stored within.
   c. Other than public access to general information, access by dial-up or Internet will require user authentication and encryption services to protect the confidentiality of the session.
   d. Monitoring and intrusion detection shall be employed to provide a feedback mechanism to indicate the effectiveness of tools used to support this security policy.
   h. Security for a connected network should reflect the security requirements of the highest risk elements on the network.

### *D. Key Definitions*

1. Agency shall mean any governmental entity, including state government, local government, or third party entities under contract to the agency.
2. Critical Systems are those systems or system components (hardware, data, or software) that if lost or compromised would jeopardize the ability of the system to continue processing.
3. Disaster refers to any event that threatens the destruction of information or availability of computer systems. A disaster may affect the physical security of computer systems, including equipment failures, fire, flood, other natural calamities, or theft of equipment. A disaster may involve destruction or information or availability of computer systems due to system failure, human error, or intentional acts including computer crimes.
4. E-mail is the exchange and or sharing of messages, attachments, and calendar and scheduling information.
5. Information Security is the protection of data against accidental or malicious destruction, modification or disclosure.
6. Security Policy is a statement of the goals, responsibilities, and accepted behaviors required for maintaining a secure environment. Security policies set the direction, give broad guidance and demonstrate senior management support for security-related facilities and actions across the organization.

7. Security Standard is a set of tasks, responsibilities, or guidelines that provide metrics to policies. Security procedures are standards that are very specific in nature, applying to group or individual systems. Procedures are directive in nature, whereas policies provide principles.
8. Sensitive Information is that information which must be protected to insure only authorized access or if lost or compromised might negatively affect the owner of the information or require substantial resources to recreate.
9. State Data Communications Network (SDCN) shall mean any data communications facility contracted for or provided by the State of Nebraska, including State-provided Internet access and network connections to state computers.
10. Users of electronic assets include any employee, business partner, contractor, consultant, or customer who is authorized to use the information technology assets of a state agency or institution.
11. Value of information includes the cost of collection, cost of reconstruction, and legal or operational consequences if information is lost or compromised.

## *E. Applicability*

GENERAL STATEMENT

These policies are intended to be sufficiently generic to apply to a wide range of governmental and educational agencies in the State of Nebraska. Each agency or operational entity must develop detailed procedures to implement broad policies and standards. Compliance with these security policies and standards will be a requirement during consideration of funding for any projects requiring review by the NITC. Compliance may be used in audit reviews or budget reviews.

EXCEPTION STATEMENT

"Computer security must support the mission of the organization." "The expense of security safeguards must be cost effective and commensurate with the value of the assets being protected." "Owners of sensitive information and critical systems have security responsibilities outside their organization." (From the Information Security Management Policy, below.)

These three principles provide the basis for determining the applicability of security policies and standards to specific situations within an organization. The responsible security authority of an organization should establish a two-step test, before exempting a unit within the organization from a particular security requirement. The first test is met, if a security requirement is contrary to the organization's mission or is not cost-effective given the value of the assets being protected. The second test is met, if exempting a security requirement does not create unreasonable risk of adverse consequences to people or entities outside of the organization. Both tests should be met.

COMPLIANCE AND ENFORCEMENT STATEMENT

The governing board or chief administrative officer of each organization must develop internal compliance and enforcement policies as part of its information security program. Such policies should be effective and commensurate with the risks involved. The NITC has no operational responsibilities, but intends to

incorporate adherence to security policies as part of its evaluation and prioritization of funding requests. The NITC recommends that the Governor and Legislature give due consideration to requests for security improvements during the budget process.

### *F. Responsibility*

An effective security program involves cooperation of many different entities. Major participants and their responsibilities include:

1. Nebraska Information Technology Commission. The NITC provides strategic direction for state agencies and educational institutions in the area of information technology. The NITC also has statutory responsibility to adopt minimum technical standards and guidelines for acceptable and cost-effective use of information technology. Implicit in these requirements is the responsibility to promote adequate security of information systems through adoption of policies, standards, and guidelines. The NITC must develop strategies for implementing and evaluating the effectiveness of information security programs.
2. Technical Panel Security Work Group. 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.
3. Chief Information Officer, State of Nebraska. The CIO has the responsibility to assist in building the business case for cost-effective implementation of security programs in non-education state agencies. The CIO must also work with non-education state agencies to coordinate and evaluate security programs. The CIO shall insure that non-education state agencies have documented procedures to demonstrate compliance with these security policies.
4. Agency and Institutional Heads. The highest authority within an agency or institution is responsible for the protection of information resources, including developing and implementing information security programs consistent with this policy. The authority may delegate this responsibility but delegation does not remove the accountability.
5. Agency Information Officer. In most cases, the highest authority within an agency or institution delegates the general responsibility for security of the agency's information technology resources to the agency's highest ranking information technology professional. This responsibility includes development and promulgation of agency-specific information security policies.
6. Agency Security Officer. In some cases, the Agency Information Officer assigns an Agency Security Officer who is responsible for:
    - Implementing enterprise and agency-specific or application-specific security policies and procedures.
    - Developing procedures and administering the information access control decisions made by information custodians within the agency.
    - Identifying training requirements.
    - Implementing procedures for authentication of users and messages.
    - Publish guidelines for creating and managing passwords.

- Developing and implementing strategies to make users aware of security policies, procedures and benefits.
- Documenting the security support structure across platforms.
- Enforcing agency security policies.
- Establishing and chairing agency security committees.
- Monitoring unusual activities and report security breaches and incidents.
- Periodically evaluating effectiveness of security policies and procedures.
- Fact gathering and analysis on information security issues.
- Developing recommendations for the agency or institution on security matters.
- Reviewing changes to the configuration of security administration facilities and settings.
- Participate in preparing a disaster recovery plan. They must understand the risks posed by disruption of computer systems. They must help prepare contingencies and be ready to implement the disaster recovery plan.

The Agency Security Officer may work with a security committee of the agency or institution. The Security Committee is an advisory group made up of key technical and management personnel within the agency to coordinate security efforts and resolve security problems.

7. Program Managers and Information Custodians In most cases, the authority within the agency or institution delegates custody of specific types of information maintained by the agency to administrators in the agency who may further delegate to employees in their organizations. These persons have direct responsibility for:
    - deciding issues pertaining to access to information
    - insuring information security
    - participating in preparing a disaster recovery plan.
8. Users of Electronic Assets. All authorized users shall be accountable for their actions relating to information assets, including hardware, software and electronic information. Information resources shall be used only for intended purposes as defined by the agency and consistent with applicable laws.
9. Information Technology Staff. Staff who are directly responsible for security, system management, and applications development have special privileges in relation to information resources such as the ability to examine the files of other users. People with access management rights must follow strict procedures regarding their access to information resources and sharing that access with others.
10. Employees and persons under contract. Employees must become knowledgeable about their organization's security policies and procedures. Employees must exercise due diligence in following those procedures and incorporating sound security practices in the discharge of their normal duties.

### *G. Related Policies, Standards and Guidelines*

The Information Security Management Policy provides the general requirements for a set of policies, standards, and procedures to protect the information assets of an organization. Other information security policies address the specific topics of:

1. Access Control Policy
2. Disaster Recovery Policy
3. Education, Training and Awareness Policy
4. Individual Use Policy
   - Acceptable Use
   - Copyrighted Materials
   - E-mail Use
5. Network Security Policy
   - General Network Controls
   - Perimeter Security for Internet and Intranet Connections
   - Remote Access
6. Security Breaches / Incident Reporting Policy