

Security Architecture

Title	Individual Use Policy
Category	Security Architecture
Date Adopted	January 23, 2001
Date of Last Revision	October 31, 2000

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-owned 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.

Security Architecture

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:*

Security Architecture

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

Security Architecture

- 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

Security Architecture

- 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 Architecture

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.

Security Architecture

- 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.

Security Architecture**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