NEBRASKA INFORMATION TECHNOLOGY COMMISSION

TECHNICAL STANDARDS AND GUIDELINES

XX-XXX Secure E-mail Transmission

Category	**Security Architecture**
Title	**Secure E-mail Transmission**
Number	**XX-XXX**

Applicability

☑ **State Government Agencies,**
excluding _____ ..... **Standard**
☐ **State Government Agencies,** all .....**Not Applicable**
☐ **State Funded Entities -** All entities receiving state funding for matters covered by this document.....**Not Applicable**
☐ **Other:** _____ .....**Not Applicable**

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

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

Prepared by: Technical Panel of the Nebraska Information Technology Commission
Authority: Neb. Rev. Stat. § 86-1506(6)
http://www.nitc.state.ne.us/standards/

1.0 Technical Standard

Electronic Mail systems in Nebraska must be designed to allow the transmission of confidential information through electronic mail in a secure manner. Every State Employee, including staff at the University of Nebraska campuses, should expect that email, sent to employees in other state agencies, is secure.

2.0 Purpose and Objectives

Purpose - Resolve existing email security risks.

Existing Environments

Email Systems - Most state agencies currently use email based on IBM Lotus Notes, MicroSoft Exchange, a generic Pop3 email systems, or external third party providers (Alltel, NOL, HotMail, and Yahoo.)

A. **Email Transmission Security** - Currently each electronic mail environment exists as a server or collection of servers that can transmit email securely only to other mail users defined in that system. Electronic mail sent to other email environments must travel through non-secure networks including the Internet.

   State and federal definitions consider email transmitted between environments non-secure. Currently, all confidential information must be exchanged using facsimile transmission, public key encryption processes, telephone or land-mail postal services. These methods all have limitations.

C. **Email Directory Leaks** - Some address book listings are used to forward email to nonsecure internet-based email addresses. This practice can only be managed through administrative agreements and may require compliance monitoring to assure that email is transmitted in a secure manner to the location where it is expected.

D. **Internet Email -** Unencrypted email transmitted over the Internet is considered nonsecure. State agencies using a non-secured email system must prohibit transmission of confidential information in this manner.

Objectives

1. Secure Email Transmission - The State shall provide technical methods and operational standards to support and enforce transmission of confidential information in a secure manner. All agencies that choose to use electronic mail for conducting business with other state agencies shall comply with these methods and standards. Adoption and compliance is the only way to assure a secure email environment for the State.

2. Secure Directory - The State shall develop and operate an email directory to support agencies included in the secured Email environment. The directory will record and display email addresses that are considered secure for transmission of confidential data. Methods will be developed to collect, update, and share directory data with participating agencies.

3. Email Restrictions - The State shall issue a policy outlining email restrictions. Email addresses not listed in the Secure Directory will be considered non-secure for purposes of transmitting confidential information via email. Email will not be sent to or received from agencies not in compliance with secure email methods.

3.0 Definitions

4.0 Applicability

All Agencies have the potential for sending confidential information to other agencies. The state needs to recognize the need for secure communications.

5.0 Responsibility

Contracts - IMS shall work with education, executive, judicial, and legislative bodies to identify and implement the technical and administrative methods for secure transmission of data through electronic mail. Agencies that wish to enter the secure environment will need to agree to technical and procedural methods. IMS will need to collect signed agreements from agency representatives to assure agreement with all standards.

Compliance - Compliance shall be required since security measures must be in place at all times. Methods shall be designed and implemented to monitor and enforce compliance. Each agency will be responsible for training their staff to use the system properly.

Costs - Agencies included in the Secure Email environment should pay annual costs of operating the technical portions of the system.

Liability - State and Federal rules regulate privacy. Liability for employees and agencies is defined there and may have impact on federal funding.

6.0 Related Policies, Standards and Guidelines