



State of Minnesota CIO POLICY

Enterprise Security Policy on Electronic Mail *Security Policy 2006-05*

Policy Statement

The Office of Enterprise Technology shall work with all state agencies to implement controls to protect electronic mail (i.e. email) containing not public data from unauthorized disclosure and tampering and reduce the risk of computer viruses and other email-based security threats.

1. The Office of Enterprise Technology shall maintain a centralized mail solution that will examine all email sent or received for computer viruses and other email-based security threats. All email traffic coming into or going out of an agency must flow through and be examined by the state's central mail solution.
2. The Office of Enterprise Technology shall maintain a central email encryption solution. All outgoing email messages containing not public data must be encrypted.
3. State agencies shall train users to:
 - a. Recognize common email-based security threats.
 - b. Understand that personal (e.g. AOL, Hotmail/MSN, etc.) email accounts will not be used to conduct official state business.
 - c. Understand that manual or auto-forwarding state email to personal email accounts is prohibited.
 - d. Understand what type of information is considered not public and when encryption is required.

Reason for the Policy

Email is a valuable communication tool that enhances productivity. However, without proper security controls, email can expose the State of Minnesota to security breaches that could lead to significant legal, financial and reputation issues.

Who Should Know about this policy

Any individual or entity employed by or working on behalf of the State of Minnesota who is authorized to make use of State of Minnesota information technology resources and uses email or who provides technical administrative support.

Related information

[Minnesota Statutes 16E.01 Subdivision 3](#) Office of Enterprise Technology Security Duties
[Minnesota Statutes 16E.03 Subdivision 7](#) Cyber Security Systems
[Statewide Policy: Appropriate Use of Electronic Communication and Technology](#)

Contacts

Enterprise Chief Information Security Officer
Chris Buse
651-201-1200
Chris.Buse@state.mn.us

History

This policy is effective on January 31, 2007.

Applicability and Exclusions

All departments, agencies, offices, councils, boards and commissions in the executive branch of Minnesota State Government must comply with this policy.

Definitions

Electronic Mail (Email): Messages transmitted electronically over a network, typically with assistance from a software package such as Microsoft Outlook. For purposes of this policy, this definition includes files attached to or embedded within email messages.

“Not Public” data: Any data collected, created, maintained or disseminated by a state agency which has a classification other than public. This includes *confidential*, *private*, *nonpublic* or *protected nonpublic* data as those terms are defined in the Minnesota Governmental Data Practices Act or any other relevant state or federal statute.

Responsibilities

Office of Enterprise Technology Responsibilities

1. Maintain a central mail solution that will examine all email for computer viruses and other email-based security threats.
2. Maintain a central email encryption solution for use by all agencies.
3. Disseminate email security statistics to agencies to help them promptly identify and respond to threats.

Agency Responsibilities

- 1. Ensure that all agency email solutions flow into and out of the state's central mail solution.
- 2. Provide email security best practices training to users.
- 3. Provide guidance to users on when it is necessary to encrypt email.

User Responsibilities

- 1. Encrypt all email messages that contain not public data.
- 2. Follow email security best practices established by agency leaders.

Procedures

Not applicable

Forms and Instructions

Not applicable

Appendices

Not applicable