



State of Minnesota CIO POLICY

Enterprise Security Policy on **Portable Computing Devices** 2006-04

Policy Statement

State agencies shall implement controls to reduce theft and loss of portable computing devices and data stored on them.

1. Users shall store "Not Public" data on secure state agency networks.
2. Users who have a business need to remotely access Not Public data shall use a secure remote access method provided by the state agency.
3. Users shall refrain from storing Not Public data on a portable computing device unless there is an authorized business need.
4. If Not Public data is temporarily stored on a portable computing device it must be encrypted using approved encryption techniques.
5. All portable computing devices used to store Not Public data shall be secured with a strong password and protected with appropriate physical security.

Reason for the Policy

Portable computing devices enhance productivity, but without proper management and security controls, they can expose the State of Minnesota to security breaches and significant legal compliance issues. Portable computing devices are prone to loss and theft and are frequently used outside the secure network perimeter, making data residing on them vulnerable to attack.

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 portable computing devices or who provides technical support for these devices.

Related information

[Minnesota Statutes 16E.01 Subdivision 3](#) Office of Enterprise Technology Security Duties
[Minnesota Statutes 16E.03 Subdivision 7](#) Cyber Security Systems

Contacts

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

History

This policy is effective on September 1, 2006.

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

Portable Computing Device: Laptop personal computers, tablet personal computers, personal digital assistants or other such devices capable of storing data and/or connecting to a secure state agency network. This definition includes thumb drives and other flash memory devices.

“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

Agency Responsibilities

1. Apply and communicate to staff the appropriate classifications of all data, as defined by the Minnesota Data Practices Act or other legal guidelines.
2. Define and communicate procedures to report and follow-up on losses of portable computing devices.

3. Require strong passwords and encryption for portable computing devices that will be used to store Not Public data.
4. Provide user education regarding the risks associated with portable computing devices and the responsibility to protect the devices.
5. Provide physical security resources to safeguard portable computing devices that will be used to store Not Public data. Examples include, but are not limited to: cable locks for laptop computers, desks or cabinets with locks, and rooms which require key card access.
6. Define procedures to justify when there is a legitimate business need to store “Not Public” data on a portable computing device.

User Responsibilities

1. Users must not store “Not Public” data on a portable computing device unless there is an authorized business need.
2. Users must remove “Not Public” data temporarily stored on a portable computing device after the business use is completed.
3. Users must never leave a portable computing device unattended in an insecure area.
4. Users must report theft or loss of portable computing devices immediately according to agency procedures.

Procedures

Not applicable

Forms and Instructions

Not applicable

Appendices

Not applicable