State of Minnesota

THE OFFICE OF
ENTERPRISE TECHNOLOGY
STATE OF MINNESOTA
www.oet.state.mn.us

MINNESOTA STATE **STANDARD**

From the Office of Carolyn Parnell
Chief Information Officer, State of Minnesota

Version: 1.00
Approved Date: 4/29/2011
Approval: Signature on file

Enterprise Security Portable Computing Device Standard

Standard Statement

Government entities must prevent the unauthorized disclosure of not public data on portable computing devices. Management of those devices must include:

Reason for the Standard

The disclosure of not public data poses a significant risk to the loss of the public's trust in the State. Recently there has been a notable increase in the use of portable devices by individuals and entities. These devices can provide increased flexibility for employee's productivity and to the delivery of State services. However, with the increase of the use of these devices comes an increased risk of devices being stolen or lost.

To enable the option for agencies to use of portable computing devices (government or personally owned) this standard is necessary to reduce the risk of disclosure of not public data to an acceptable level. While there are a number of other issues government entities must consider (records management, litigation holds, etc.), this standard is designed to help the entities make a more informed decision around the information security risks. Individual government entities may have additional requirements for protecting their most sensitive information.

Portable Computing Device Authorization

Agencies must authorize the computing devices allowed to process or store not public data. Authorized portable computing devices are restricted to those devices that have the technical capability (natively or through third party products) to comply with the requirements of this standard. Authorized devices include those purchased by the State of Minnesota. Authorized devices can also include those that are personally owned, if permitted by the government entity.

Encryption of Not Public Data

All not public data stored on portable computing devices must be encrypted by one of the following means:

- An approved, third party product that is enforced through a controlled configuration and cannot be disabled by the user
- Encryption that is enforced through a technical policy or localized applications that cannot be overwritten by the user

Password / Authentication Requirements

All portable computing devices that contain not public data or synchronize with services that can access not public data must protect the data with user authentication. See **Appendix A** for authentication requirements by device type.

Remote Data Wipe

Portable computing devices that only use a Personal Identification Number (PIN) for authentication must have the capability to:

- Be remotely erased (or "wiped) by the agency or service provider
- Automatically erase all data after a set amount of authentication attempts

User Agreements

All users of portable computing devices must sign-off and agree to the following requirements

- To physically protect the portable device when away from a secure location
- Proper escalation and notification procedures for when a portable device is lost or stolen, including the need to notify their agency before notifying a third party (e.g., AT&T, Sprint, etc.)
- For users of personal devices, understanding and agreeing to the terms in a personal use agreement. These terms will give the State the authority to:
    - Remotely wipe data on the device, which potentially could include personal data
    - Monitor activities on non-State devices
    - Recover data or take possession of devices when legally necessary

Records Management and Data Practices Considerations

To be in compliance with statutory requirements, government entities extending data to portable computing devices must address record retention, record administration, and data practices requirements.

2.0 Roles & Responsibilities

Office of Enterprise Technology (OET)

- Maintain this document
- Provide guidance to government entities on any conflicts or questions pertaining to compliance with this standard
- Provide subject matter expertise to MMD on matters pertaining to this standard and appropriate product selection
- Fulfill the requirements of the Government Entity for OET

Government Entity

- Provide awareness of the requirements of this standard to users and administrators of portable computing device
- Authorize usage and approve connectivity to entity resources from portable computing devices
- Maintain signed agreements from users
- Maintain an escalation process to ensure lost or stolen devices are addressed promptly
- Create and maintain policies and procedures for using portable computing devices
- Determine and accept additional business risk for records management, litigation hold, and other regulatory or legal requirements

Related Information

Applicability and Exclusions

This standard is applicable to the government entities in the Executive Branch identified in the Enterprise Security Program Applicability Standard 2009-06. It is also offered as guidance to other government entities outside the Executive Branch.

Agency Heads, Responsible Authorities, Chief Information Officers, Chief Information Security Officers, Data Practices Compliance Officials, and their designees who are responsible for responding to, management of, and reporting on entity security controls and/or compliance with data practices and records management laws must be aware of this standard.

The requirements of this standard must be incorporated into agreements with third parties to ensure proper controls are in place for protection of state information assets.

Devices connecting directly (wired or wirelessly) to an agency's secure network may have additional security control requirements that are beyond the scope of this standard.

Devices connecting to government entity services that do not process or store Not Public data on the device are excluded from this standard.

This standard supersedes the "**Enterprise Security Policy on Portable Computing Devices 2006-04**" policy.

Regulatory, Policy, Standards, & Guideline References

Minnesota Statutes 2007 Chapter 16E (Office of Enterprise Technology)

Minnesota Statutes, Chapter 13 (Data Practices Act)

Minnesota Statutes, section 15.17 (Official Records Act)

Minnesota Statutes, section 138.17 (Administration of Government Records)

Enterprise Security Information Handling Policy

Enterprise Security Authentication and Access Control Policy

Forms, Templates, and Procedures

Italicized terms can be found in the Enterprise Security Glossary of Terms

Enterprise Security Exception Request Form

User Agreement Form Template

Compliance

Compliance with this standard is required with approval date of the standard.

Terms in *italics* can be found in the Enterprise Security Glossary document.

Appendices

Appendix A:

The following chart defines the authentication requirements for different device types:

Device Type	Authentication Requirements
Laptop / Tablet (Broad Remote Access)	Users must authenticate to the device with the following password requirements: • Length of 6 or more characters • Contains at least one letter and one number • Expires at least every 90 days • Cannot be changed by user for 7 days • Cannot be reused for at least 15 changes • Locks account after 10 attempts • Requires administrative support to unlock account • Inactivity lockout at 15 minutes Devices used to gain Remote Access must also: • Use two-factor authentication to connect users to the network • Connect through an approved, encrypted VPN solution
Smart-Phone / Tablet (Limited Access)	Users must authentication to the device with the following personal identification number (PIN) requirements: • Length of 4 or more numbers • Automatically wipes the stored data after 10 attempts • Inactivity lockout at 15 minutes

“Broad Remote Access” is defined as the portable devices that have remote access to State resources which is equivalent to the user’s access while on a government entity’s internal, secure network (e.g., IPSec VPN, SSL VPN).

“Limited Remote Access” is defined as the portable devices that have access to a limited set of resources and leverages additional controls to ensure the security of State data (e.g., SSL encrypted data transmission by application, additional authentication by application, etc.)

History

Revision History – record additions as Major releases, edits/corrections as Minor

Date	Author	Description	Major #	Minor #
05/05/2011	Eric Breece	Initial Release	1	00

Review History – periodic reviews to ensure compliance with program

Date	Reviewer	Description	Compliance
n/a			
n/a			

Approval History – record of approval phases

Phase	Description	Date
SME	ESO Approval	02/22/2011
ISC	Information Security Council Approval	03/02/2011
CIOC	CIO Council Approval	04/28/2011