PORTABLE COMPUTING DEVICES DATA SECURITY

POLICY DM005, EFFECTIVE 2012-08-08

POLICY STATEMENT

Portable computing devices constitute a unique risk to MnDOT's data, and must be authorized, managed and used so that there so no disclosure of *not public* data occurs and that the use of these devices does not pose a security threat to any of MnDOT's information resources. Use of these devices must comply with records management, data practices and litigation related obligations and activities.

This policy applies to portable computing devices (whether MnDOT-owned or personally-owned) which connect to the MnDOT network or access MN.IT Services messaging services (such as email, contacts, calendar and reminders) via mobile data synchronization technology.

REASON FOR POLICY

Information is a vital MnDOT asset and requires protection from unauthorized access, disclosure, or alteration, and protection from interruptions in access and use. Portable computing devices can provide increased flexibility for employee productivity and to the delivery of MnDOT services.

Because of their size and value, the use of these devices also results in an increased risk of theft or loss. The disclosure of not-public data through theft or loss poses a significant risk to the public's trust in MnDOT. In addition, the use of these devices presents increased security issues, such as computer viruses, worms, Trojan Horses, and other malware to MnDOT's network and other information technology resources.

WHO NEEDS TO KNOW THIS POLICY?

All MnDOT employees and other users of MnDOT resources must follow State of Minnesota policy, MnDOT policy and any additional standards, procedures, and other guidance regarding the use of portable computing devices in MnDOT so that the security, confidentiality, integrity and availability of MnDOT data is ensured.

DEFINITIONS

Authorized
Authorized portable computing devices are restricted to those devices that MnDOT has determined to meet all of the following requirements.

- Technical capability (natively or through third party products) to

SENIOR OFFICER

Tracy Hatch
Deputy Commissioner/CFO/COO

POLICY OWNER

Karin van Dyck
Director, Human Resources

POLICY CONTACT

Jodi Mathiason
Labor Relations Manager
Jodi.Mathiason@state.mn.us
651-366-3404

POLICY HISTORY

2012-08-08, Established

MnDOT Policy Website

comply with MnDOT security requirements
- Device selection requirements (e.g., type, manufacturer, features)
- Cost effectiveness requirements
- Securely managed in the current MnDOT IT infrastructure

Not Public Data
Any data collected, created, maintained or disseminated by a state agency which is classified other than *public.* This includes *confidential, private, nonpublic or protected nonpublic data* as defined in the Minnesota Government Data Practices Act, **Minnesota Statute §13.02.**

Portable Computing Device
For purposes of this policy, the term means portable devices such as PDAs (personal digital assistants) or other such devices capable of storing and processing data, and connecting to a network. This includes tablet computers or tablets (example iPad) and smartphones (examples Android, iPhones, and Blackberries).

Security Requirements
- **Portable Computing Device Authorization** – Portable computing devices must be authorized by MnDOT *(see definition for Portable Computing Devices)*
- **Authentication/password** – Must follow all MN.IT Services requirements, **Enterprise Security Portable Computing Device Standard (MN.IT Services)**
- **Encryption of Data** – All MnDOT data stored on portable computing devices must be encrypted by one of the following means:
    - An approved, third part product that is enforce through a controlled configuration and cannot be disabled by the user.
    - Through a technical policy or localized applications that cannot be overwritten by the user.
- **Remote Data Wipe and Automatic Erase of Data** – Portable computing devices 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 failed authentication attempts

PROCEDURES

Use the links below to find information on topics relating to IT policies and security **MnDOT IT Security Awareness and Appropriate Use.**

RESPONSIBILITIES

Division Directors
- Determine acceptable business risk for the use of portable computing devices and MnDOT's records management, litigation hold, and other regulatory or legal requirements.
- Ensure incorporation of the requirements of the MN.IT Services standard on portable computing devices into agreements with third parties to ensure proper controls are in place for the protection of state information assets.
- Assign MnDOT managers and staff to develop any necessary standards, guidance, process, or business procedures necessary for the appropriate management of portable computing devices in MnDOT.

MN.IT Services
- Provide awareness of the requirements of this policy to users and administrators of portable computing devices.
- Maintain an escalation process to ensure prompt action regarding lost or stolen devices.
- Create and maintain policies, standards, and procedures for secure use of portable computing devices.

Supervisors
- Follow any special guidance on employees assigned to MnDOT owned portable computing devices.
- Authorize usage and approve connectivity to entity resources for portable computing devices for employees as appropriate.
- As directed, submit and/or keep copies of signed agreements/acknowledgement forms from supervisors in the appropriate location(s).

- Take appropriate disciplinary or corrective action whenever persons they supervise violate MnDOT or state policy on portable computing devices.

IT Service Desk, Local IT Support Staff, Administrative Staff

- Refrain from enabling connectivity or access for any portable computing device that does not meet the requirements of this policy or other standards or guidance.
- Take appropriate steps to ensure that lost or stolen portable computing devices are located, disabled, or suspended from service as needed.
- Refrain from engaging in any activity to circumvent the security or other requirements for the use of portable computing devices.

Users

- Follow this policy and any standards or guidance regarding the use of portable computing devices in MnDOT.
- Follow the **Statewide Policy on Appropriate Use of Electronic Communication and Technology**
- Follow proper escalation and notification procedures when a portable device is lost or stolen (*detailed guidance is included in MnDOT's iHUB, A to Z, under "lost electronic devices" and under "stolen electronic devices").*
- Follow all approval requirements and sign agreement before using a personally owned device.
- Secure portable computing devices in a locked location.
- Refrain from engaging in any activity to circumvent the security or other requirements for the use of portable computing devices.
- Personally owned devices may not be connected to MnDOT's network or access the MN.IT Services mail message system unless the employee has supervisory approval, the device meets all security and other requirements, and the employee has signed the **Agreement for End User** **http://ihub.dot.state.mn.us/itweb/policy_and_security.html**

FREQUENTLY ASKED QUESTIONS

Q: ***If I use my personal smartphone for Webmail or Web portal, does that mean that I have to sign a user agreement and MnDOT could wipe my device?***

A: No. Webmail and Web portal have a secure connection, and none of the information is stored on a personal phone.

Q: ***Many organizations are moving toward a "Bring Your Own Device" environment where employees use their own personally owned devices for work. It seems like it would save MnDOT money because MnDOT would not have to purchase devices for employees, and employees would be more careful with their own devices. In addition, it would simplify things for employees, not having to carry two devices all the time at work.***

A: Some organizations are moving toward having employees use their personal devices at work. The primary growth in this area is in the private sector. In those businesses, the use of personal devices is often limited to a specific work area, such as sales.

Because it is a state agency, MnDOT has responsibilities and restrictions to protect data and to provide data when requested under the Data Practices Act, which do not apply to private businesses.

The necessary infrastructure to protect and manage portable computing devices is substantial, and the funds to buy, test, implement, and support the use of personally owned devices must be prioritized along with other important activities such as the consolidation of data centers, and the IT consolidation mandated by the State legislature.

Q: ***Why is it such a challenge to manage the security of devices like smartphones (iPhones, Droids)?***

A: A primary benefit of mobile devices such as smartphones is the ability to communicate with other technology sources (connectivity). It is also the primary risk. Connectivity makes the device powerful and useful. It also provides new and difficult to control access to MnDOT and State resources.

MnDOT and the State of Minnesota regulate access to these resources to known devices that meet minimum-security requirements. Mobile device management also provides the ability to remotely wipe and control applications on remote devices. This is important when the devices may contain sensitive data or access to

sensitive data. Controlling applications installed on mobile devices also reduces our exposure to malware such as keystroke loggers, data mules, and viruses. However, the ability to manage applications requires an access control infrastructure that is not currently in place.

FORMS/INSTRUCTIONS

Use the links below to find information on topics relating to IT policies and security **MnDOT IT Security Awareness and Appropriate Use.**

RELATED INFORMATION

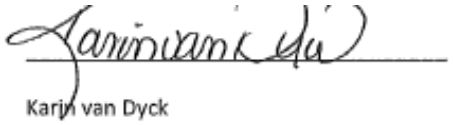
Enterprise Security Portable Computing Device Standard (MN.IT Services)
Statewide Policy on Appropriate Use of Electronic Communication and Technology
Mobile Devices Use Addendum to the Statewide Policy, Acknowledgement of Receipt, Mobile Device Services, and Equipment form
MnDOT Code of Ethics Policy
MnDOT Legal & Litigation Holds Policy
MnDOT Records Retention and Disposal Policy

PLAIN LANGUAGE *(READABILITY SCORE FOR THIS POLICY)*

Active Voice = 100% *(≥ 90%)*	**Grade Level = 14.2** *(Grades 12-14)*	**Words per Sentence = 20.4** *(≤ 18 words)*

MnDOT must ensure the use of **plain language** for all policies. All MnDOT policies use the Flesch Reading Ease formula for calculating the approximate reading level of English-language content. Microsoft Word for Windows© offers an automatic readability score. The measures MnDOT uses include, **active voice** (greater than 90% of the time), **grade level** (grades 12-14), **words per sentence** (less than or equal to 18 words).

POLICY OWNERSHIP AND AUTHORIZATION



Karjn van Dyck
Acting Director, Office of Human Resources

Date Signed 7-18-12

Tracy Hatch *(on behalf of the Board)*
Board Chair and Chief Financial Officer

Date Signed 8-1-2012

Bernard J. Arseneau
Deputy Commissioner and Chief Engineer

Date Signed 8-8-12