State of Wisconsin
Mobile Device Policy

Effective Date: 11/26/2012
Review Date: One year from Effective Date

Background and Context

Mobile devices are a valuable tool in conducting business. They provide authorized users with the ability to send and receive e-mail or calls, remotely access files, browse the web, and run various applications. Use of mobile devices purchased by the State shall be for enterprise business. However, the State will permit the use of personally owned devices if approved by the employee's State agency. During such use, State of Wisconsin policy will dictate the protection of data and information assets.

Purpose

The purpose of this policy is to define accepted practices, responsibilities, and procedures for the use of mobile devices that State agencies authorize to connect to enterprise systems. In addition, this policy is necessary to protect the confidentiality, availability, and integrity of State of Wisconsin data accessed or stored on mobile devices regardless of State or employee ownership.

As a matter of policy and best practice, data should always be secured where it resides. Users should avoid storing State data on mobile devices. State business requirements may, on occasion, justify accessing and/or storing State data on mobile devices. In these cases, users are required to ensure they adhere to the user responsibilities in this policy.

Scope

This policy applies to all mobile devices, regardless of ownership, connecting to or accessing State network resources and/or data. This policy will not supersede any other existing State policies, but agencies may introduce more stringent requirements than this policy dictates.

State Agency Responsibilities

- Distributing this policy and storing signed acknowledgement of receipts.
- Administering agency mobile device management policies.

- Determining eligibility for State owned or personally owned mobile devices.
- Procuring and supporting devices and wireless services.
- Conducting periodic reviews of devices and wireless services.
- Reviewing, and approving or denying exceptions to this policy.

Mobile Device User Responsibilities

All users of mobile devices connecting to State networks must adhere to the following:

1. **Data and Security**
   - Obtain agency approval to connect to State networks.
   - Have mobile device management software installed and accept all security policies pushed to the device.
   - Must not store sensitive State data, including but not limited to, Personally Identifiable Information (PII), Health Insurance Portability and Accountability Act (HIPAA), and other data identified as sensitive by agencies (unless the data is encrypted).
   - Users must take precautions to prevent others from obtaining access to their mobile devices, including not sharing credentials and/or passwords.
   - Agree that agencies may restrict access to State networks by any mobile device if the device violates this policy.

2. **Loss or Theft**
   Users must report compromised, lost or stolen mobile devices immediately to their designated agency point of contact. In addition, stolen devices must be reported to the authorities.

3. **User Safety**
   Users must not operate devices while driving and must abide by all applicable State laws addressing safe use of mobile devices.

4. **Records Management**
   Records created from the use of any mobile device for State business may be subject to the Wisconsin Public Records Law and must comply with State laws and agency specific retention and disposal guidelines.

5. **Termination of Use**
   Upon disposal, upgrade or changes in employment, the agency will completely wipe all devices with State information stored on them. State owned devices must be returned to the user's agency.

6. **Users of Personally Owned Mobile Devices must also agree to:**

   a. **Condition of Devices**
      - Keep devices in good working order and install manufacturer software updates.
      - Not modify manufacturer built-in protections (e.g. jailbreaking or rooting devices).
      - Ensure that all devices meet the minimum technical requirements for use. The State will update these policies every year.

   b. **Reimbursement**

Cover all costs related to the device, services, upgrades and/or applications.

c. **Data and Security**
   - Give State agencies the right to remotely lock the device. At its discretion, the agency can wipe the device completely.
   - Be responsible for backing up all personal information on the device. The State shall not be held liable for data loss.
   - Users may not back up State information on media other than what is provided by the State.
   - Allow the State access, for discovery and record request purposes, to the content stored on the device.
   - All devices must have a complex password with periodic changes.

d. **Technical Support**
   The State will not answer questions or provide support for personally owned devices unless directly related to the mobile device management software on the device. End users must obtain support for all on-board applications from the provider of the device.

e. **Responsibility**
   Agree the State is not responsible for damaged, lost or stolen personally owned devices while the employee is conducting State business.

Exceptions

Exceptions to this policy must be approved by the mobile device user's agency.

Definitions

Mobile Device

Any type of device designed to be moved and capable of collecting, storing, transmitting, or processing electronic data. Movement in this case refers to the device generally not having a fixed connection to the network. Examples of mobile devices include, but are not limited to, a tablet (e.g. iPads), iPhone, Blackberry, Android, or mobile network connected storage device.

Mobile Device Management

Mobile device management (MDM) includes software that provides the following functions: software distribution, policy management, inventory management, security management and service management for smartphones and media tablets.

Health Insurance Portability and Accountability Act (HIPAA)

HIPAA is a federal law designed to allow portability of health insurance between jobs. In addition, it required the creation of a federal law to protect individually identifiable health information. HIPAA regulations define individually identifiable health information as information that is a subset of health information, including demographic information collected from an individual, and:

- "[i]s created or received by a health care provider, health plan, public health authority, employer, life insurer, school or university, or health care clearinghouse"; and

- "[r]elates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual; and that identifies the individual; or with respect to which there is a reasonable basis to believe the information can be used to identify the individual."

Personally Identifiable Information (PII)

An individual's last name and the individual's first name or first initial, in combination with and linked to any of the following elements, if that element is not publicly available information and is not encrypted, redacted, or altered in any manner that renders the element unreadable: (a) the individual's Social Security number; (b) the individual's driver's license number or state identification number; (c) the number of the individual's financial account, including a credit or debit card account number, or any security code, access code, or password that would permit access to the individual's financial account; (d) the individual's DNA profile; or (e) the individual's unique biometric data, including fingerprint, voice print, retina or iris image, or any other unique physical representation, and any other information protected by state or federal law.

Sensitive Data

Any individually identifiable information about State of Wisconsin employees, citizens, or other who do business with the State, and such other information designated as confidential under applicable Federal and State laws; and agency guidelines.

State Network

The State Network is inclusive of all agencies wired and secured wireless networks.

Compliance

Individuals using mobile devices that connect to State network resources, shall abide by the rules of this policy and all applicable enterprise and agency policies. Use of mobile devices in violation of this policy may result in revocation of privileges and/or disciplinary action.

Related References, Policies and Guidelines

Wisconsin Public Records Law, §§19.31-19.39 Wis. Stats
Inattentive Driving, 346.89 Wis Stats
DOA Acceptable Use Policy
DOA Wireless Services Policy

Acknowledgement of Receipt of State of Wisconsin Mobile Device Policy

I acknowledge that I have received the enterprise policy covering the use of mobile devices. I also understand that I am responsible for reviewing the policy and complying with all of its provisions.

The State of Wisconsin can, at anytime and at its discretion, revise this user acknowledgement and require device users to reconfirm their agreement.

Employee Name (Please Print)	State Agency
Employee Signature	Date

Authority

Wisconsin State Statute 16.97 (2)(a) provides that the department [Department of Administration] shall establish policies, procedures and planning processes for the administration of information technology services.

Authorized By:

State of Wisconsin
Department of Administration
Deputy Secretary

11/20/2012
Date

State of Wisconsin
Chief Information Officer

11/21/2012
Date