State of Iowa Enterprise Mobile Device Security Standard

August 27, 2013

Purpose

This standard establishes the minimum requirements for secure use of mobile devices and tablets\slates, including the BlackBerry, iPhone, iPads, Android devices, and other smartphones.

Overview

Mobile devices are capable of making phone calls, sending\receiving email, browsing the web, storing\modifying documents, remotely accessing data, recording audio\video, and serving as navigation aids. The decision of whether or not to allow the use of mobile devices should be based on an assessment of the risks and business benefits of access. This standard provides a minimum set of security requirements for use of mobile devices.

Scope

This standard applies to mobile devices and tablets\slates, including the BlackBerry, iPhone, iPads, Android devices, and other smartphones. Laptops and netbooks are covered by the Enterprise Laptop Data Protection Standard.

This standard applies to all agencies as defined by Iowa Code Chapter 8A, Section 101. Non-participating agencies are encouraged to follow the guidelines in this and other enterprise level standards, as well as participate in enterprise level security programs.

Definitions

Selected terms used in the Mobile Device Standard are defined below:

- **Bluetooth:** Low power radio technology that allows devices to pair and connect wirelessly.
- **Mobile Device:** Device designed to support mobile computing using an operating system such as iOS, Android, S40 OS, Windows, and BlackBerry OS. Mobile devices include tablets, BlackBerrys, iPhones, iPads, Android devices, and other smartphones.
- **Near Field Communication:** A wireless personal area network (WPAN) interface that requires no infrastructure to operate. Devices share data by touching together or being in close proximity.
- **Unauthenticated Public Wi-Fi**: Free public Wi-Fi typically offered at coffee shops, libraries, rest stops, airports, and other public venues.
- **USB Mass Storage**: Storage devices that transfer files via the Universal Serial Bus.

Elements of the Standard

The following elements apply to all agency staff\contractors\volunteers\interns conducting state business on a mobile device.

1. **Central Management**: Mobile devices shall be centrally managed. Agencies shall maintain a list of devices authorized to connect to the state email system.

2. **Passwords\PINs**: Passwords\PINs shall be enabled for each device. The password\PIN shall have at least 6 characters.

3. **Erase Data and Disable Device**: Devices shall be disabled after 10 unsuccessful password attempts and wiped:
    a. When reported lost or stolen.
    b. Before disposal\return to the provider.

4. **Inactivity**: The device shall be set to lock after 15 minutes, or less, of inactivity.

5. **Encryption**: Data shall be encrypted using strongest encryption available for the device. Encryption shall cover:
    a. Data in transit,
    b. Data in device memory, and
    c. Data in a media card attached to the device.

6. **Bluetooth**: Devices shall disable Bluetooth by default unless approved by the agency for hands free operation. If enabled for hands free operation devices shall:
    a. Disable Discoverable Mode.
    b. Only pair with agency approved hands free devices that meet this standard.

7. **Device Security.** All mobile devices and management systems shall have the latest critical security patches installed. Unsupported devices with critical vulnerabilities shall not connect to the state email system.

8. **Usage Policy**: Agencies shall:
    a. Have a policy covering the use of mobile devices, including personal devices, and
    b. Ensure that staff receive and acknowledge the policy.

9. **Training**: Users shall receive annual security awareness training covering secure use of mobile devices. At a minimum training shall cover passwords, phishing, malware and reporting incidents.

10. **Personally Owned Devices**: Personally owned devices connected to state\agency email systems shall:
    a. Be approved by agency management.
    b. Be centrally managed using the ITE or agency mobile device management system.
    c. Follow the mobile device management system's configuration settings.
    d. Meet all of the requirements set out in this standard.
    e. Have all state data wiped from the device when the device is no longer used for state business or the employee leaves the agency.
    f. Be compliant with the agency\enterprise BYOD policies.

11. **Reporting**: Users shall report lost, stolen or missing devices to: their agency, the ITE Service Desk, and the Information Security Office. Notification shall take place as soon as possible, but within 24 hours, after the device is discovered to be missing. The notification shall include:
    a. Agency name and contact,
    b. Date of theft\loss,
    c. Description of the theft\loss, and
    d. Description of information stored on the device.

12. **Third Party Applications**: Users may only install agency approved third-party applications on their device.

13. **Wi-Fi:** Agency devices shall not connect to unauthenticated public Wi-Fi networks or networks using WEP and WPA.

14. **Malware:** Devices shall have up-to-date malware protection if available.

15. **Physical Protection.** Users of mobile devices are responsible for their physical protection. Mobile devices shall be secured when not in use.

16. **Synchronization\Storage:**
    a. State issued devices shall not sync with a non-state owned\personal computer.
    b. State data shall not be synched to a non-state approved system.
    c. Devices shall not connect to public charging stations\kiosks.

17. **Location Services**: Location services shall be disabled when outside of the United States.

18. **Near Field Communication**: Near Field Communication (NFC) shall be disabled by default unless approved by the agency.

Updates

This document will be reviewed at least every two years and updated as needed.

Effective Date This standard shall be effective August 27, 2013.

Enforcement This standard shall be enforced pursuant to Iowa Administrative Code 11—25.11(8A).

Variance Iowa Administrative Code 11 - 25.11(2) provides for variances from security standards. Requests for a variance from any of the requirements of this policy will be submitted in writing to the Chief Information Security Officer prior to implementation.