State of Iowa Enterprise Laptop Data Protection Security Standard

April 12, 2012

Purpose

This standard establishes the minimum security requirements for laptop computers and the data stored on, processed by, or transmitted via laptops.

Overview

Laptop computers provide portability allowing users to work outside of the office. Laptop computers also come with risks. Confidential information may be disclosed as a result of the loss or theft of a device. Laptop devices may be exposed to malware when they connect to insecure network.

Scope

This standard sets minimum security and encryption requirements for laptops that hold state-owned data or connect to internal state-owned or managed networks. Laptops of contractors, state business partners and individuals connecting to internal state networks or storing state data are covered by this standard.

For the purpose of this standard, security is defined as the ability to protect the integrity, confidentiality and availability of information processed, stored and transmitted by an agency.

This standard applies to all agencies as defined by Iowa Code Chapter 8A, Section 101. Non-participating agencies are encouraged to follow this and other enterprise level policies, standards, guidelines, processes and procedures.

Definitions

Selected terms used in the Enterprise Laptop Data Protection Standard are defined below:

- **Laptop Computer:** Laptop computers are lightweight, portable devices designed to operate for extended periods of time with a self-contained power source. For the purpose of this standard, a laptop computer includes a tablet computer, netbook, iPad and similar device.

- **Encryption:** The process of making information indecipherable to protect it from unauthorized viewing or use, especially during transmission or storage. Encryption is based on an algorithm and at least one key. Even if the algorithm is known, the information cannot be decrypted without the key(s).

Enterprise Laptop Standard

The following minimum standards must be met for all laptop computers:

1. **Laptop Inventory.** Agencies will maintain an inventory of all laptop computers and their assigned user.

2. **Data Encryption and Authentication.** All laptop computers shall be encrypted. The encryption software must meet the following criteria:
    a. Pre-boot: Pre-boot user authentication must be used by the encryption software.
    b. Whole-disk: The entire hard drive, excluding the master boot record, shall be encrypted.
    c. Encryption Strength: 256-bit Advanced Encryption Standard (AES) or stronger encryption must be used.
    d. Audit Trail: An audit trail shall be maintained to demonstrate that a device was encrypted and the type of encryption software used.
    e. Central Management: The encryption process and procedures shall be centrally managed at the agency and/or enterprise level.
    f. Hibernation: Laptop encrypts upon hibernation requiring the user to re-authenticate.

3. **Loss/Theft Procedures.** Loss or theft of any laptop computer shall be reported to the Chief Information Security Officer within 24 hours. The notification shall include:
    a. Agency name and contact.
    b. Date of theft/loss.
    c. Description of the theft/loss.
    d. Whether confidential/sensitive information was stored on the device.
    e. Whether the laptop was encrypted.
    f. Whether the password or token was stored with the laptop.

    Procedures shall also be in place to change authentication credentials to any systems the device\user may have accessed.

4. **Physical Protection.** Users responsible for the physical protection of their laptops.
    a. Laptops shall not be left unattended in a public area unless secured by a cable lock or other anti-theft device.

5. **Passwords**: Strong passwords must be used with laptops. Passwords must be:
    a. At least 8 characters.
    b. A mix of numbers and letters.
    c. Have at least one special character.

    Written passwords, smart cards, or tokens shall not be stored with the laptop.

6. **Primary Storage/Data Backups.** To ensure data availability in the event of device loss or theft, a laptop computer shall not be the primary storage device for State of Iowa data. Regular backups of data stored on laptops must be made, according to agency policy.

7. **Client security maintained.** All laptop computers must have:
    a. A properly-configured host-based firewall;
    b. Up-to-date anti-malware software; and
    c. All laptops shall have the latest critical security patches installed within 5 business days of release.
    .

8. **Assessment.** The ISO will periodically conduct assessments of agency compliance with this standard. Agencies will provide access to inventory information and systems as required to determine compliance. If violations of the laptop computer standard are identified, the agency will receive written notification pursuant to IAC 11--25.11(8A).

9. **Awareness Training:** Laptop computer users shall be provided with mobile device security awareness training. At a minimum, users shall be provided with documentation describing mobile computing risks.

10. **Erase Data and Disable Device**: Laptops shall be erased and/or disabled:
    a. After 10 unsuccessful password attempts.
    b. When reported lost or stolen.
    c. Before disposal\return to the lessor.

11. **Inactivity**: The laptops shall be set to lock after a maximum of 15 minutes of inactivity.

12. **Usage Policy**: Agencies shall:
    a. Have a policy covering the use of laptops, and
    b. Ensure that staff receive and acknowledge the policy.

13. **Personally Owned Devices**: Personally owned laptops shall not connect to internal state-owned networks.

14. **Third Party Applications**: Users may not download third-party applications to their laptop without agency management approval.

15. **Wireless:** Laptops shall:
    a. Disable peer-to-peer (ad-hoc) networking capabilities.
    b. Disable Bluetooth unless required for a legitimate business need. If Bluetooth is required for a legitimate business need the laptop shall:
        i. Only pair with agency approved devices.
        ii. Disable discoverable mode.
    c. Use an encrypted vpn solution when remotely connecting to an internal agency network using public wireless. The vpn solution shall:
        i. Use two factor authentication
        ii. Not allow two simultaneous connections to different networks (i.e., no split tunneling and no multi-homed connections).

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

Effective Date This standard shall be effective May 1, 2012.

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.