State of Iowa Enterprise Removable Storage Device Security Standard

June 22, 2011

Purpose

This standard establishes minimum requirements for secure use of removable storage devices.

Overview

Removable storage devices allow portability of data and programs. They are easy to use and capable of holding large quantities of data. These same characteristics present security concerns. Their small size makes them easy to lose or steal. Their portability facilitates removal of confidential data from secure systems.

This standard identifies steps that must be taken to reduce the risks associated with the use of removable storage devices.

Scope

This standard sets minimum requirements for the secure use of removable storage devices and encryption of confidential data on removable storage devices. This standard does not apply to files written to tape or other media as part of an agency's regular backup process when the software being used is intended solely for the purpose of creating and managing backups.

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 policies, standards, guidelines, processes and procedures.

Definitions

Select terms in the Enterprise Removable Storage Encryption Standard are defined below:

- **Removable Storage Devices:** Devices designed to store and transfer electronic information from one computer to another. Removable storage devices include, but are not limited to:
  - USB-based flash drives (thumb drives)
  - Portable hard drives
  - Memory cards
  - DVDs, CDs, and floppy disks
  - Cell phones, iPods and MP3 players
  - Magnetic tapes not part of an agency's backup process

Updates

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

Enterprise Removable Media Encryption Standard

The following minimum standards must be met for all removable storage devices:

1. **Policy:** Agencies shall establish a policy covering the use of removable storage devices. At a minimum the policy shall cover:
    a. The types of data permitted on removable storage devices
    b. The types of devices permitted

2. **Data Encryption:** Confidential data stored on removable storage devices must be encrypted. The encryption shall use 256 bit (AES) Advanced Encryption Standard or stronger encryption.

3. **Devices**: The following apply to removable storage devices.
    a. Employees may not copy confidential State data onto personal devices
    b. Devices of unknown ownership may not be plugged into State computers
    c. Devices provided by agency customers must be scanned for malware
    d. Agencies shall implement settings or policy to prohibit use of unauthorized removable devices
    e. Use a strong password:
        i. At least 8 characters
        ii. A mix of numbers and letters
        iii. At least one special character
        iv. Biometrics may be used in conjunction with passwords for strong authentication
        v. Written passwords shall not be stored with the device
    f. Devices shall be centrally managed by the agency.
        i. Agencies shall maintain an inventory of issued devices with whom the device is issued to and the encryption status of the device

4. **Physical Protection:** Employees are responsible for physical protection of encrypted removable storage devices containing confidential information.

5. **Primary Storage:** Removable storage devices shall not be the primary storage device for any confidential State of Iowa data.

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

7. **Awareness Training:** Staff shall be provided with removable storage device and media security awareness training. At a minimum, users shall be provided with documentation describing removable storage devices and risks.

8. **Reporting**: Lost or stolen removable storage devices containing confidential information must be reported to the DAS-Information Security Office within 24 hours. The notification shall include:
    a. Agency name and contact
    b. Date of theft/loss
    c. Description of the theft/loss.
    d. Description of information stored on the device
    e. Whether the device was encrypted

9. **Auditing**: Agencies shall log the attachment of removable storage devices to agency computers.

Effective Date This standard shall be effective June 22, 2011.

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.