State of Michigan
Technical Standard

1340.00.110.04 Secure Disposal of Installed and Removable Digital Media Standard

Issued: 02/26/2014
Revised: 10/21/2015
Reviewed:
Next Review Date (1 yr): 10/21/2016

Authoritative Policy: 1340.00 Information Technology Information Security Policy (http://www.michigan.gov/documents/dmb/1340_193162_7.pdf)
Associated Procedures: n/a
Distribution: Statewide

Purpose

To establish a statewide standard for the secure disposal of installed and removable state of Michigan (SOM) digital media.

The purpose of this standard is to prevent the unintentional and unauthorized use or misuse of SOM information and promote the privacy and security of sensitive and/or confidential information resources within the SOM by defining the minimum requirements for the removal of data from an Agency's computer hard drives and electronic media resources prior to their being surplused, transferred, traded-in, disposed of, or the hard drive is replaced. The procedure will also foster SOM Agency compliance with federal regulations dealing with the confidentiality of personally identifiable information; such as the Health Insurance Portability and Accountability Act, the Gramm-Leach-Bliley Act (also known as, Financial Services Modernization Act), and the Family Educational Rights and Privacy Act (FERPA).

Contact/Owner

Department of Technology, Management and Budget (DTMB)
Cybersecurity and Infrastructure Protection (CIP)
Michigan Cyber Security (MCS)

Scope

Executive Branch Departments and Sub-units, Agencies, Boards or Commissions and contractors, vendors and third party providers that use digital media of any kind to store information, including all equipment owned or leased by the Agency that has memory such as personal computers (PC), Personal Digital Assistants (PDAs), routers, firewalls and switches and other media, such as, tapes, diskettes, CDs, DVDs, Write Once-Read Many (worm) devices, printers, mobile devices (e.g., smart phones, etc.), laptops, tablets, and Universal Serial Bus (USB) data storage devices.

STANDARD

This standard requires proper disposal, transfer, or destruction of SOM information contained in removable, portable, or installed media containing protected data by defining minimum requirements for the removal of data from a storage device or other electronic media resources prior to their being surplused, transferred, traded-in, disposed of, or the hard drive is replaced.

INFORMATION SECURITY RISKS

Information security risks can be created by reassigning, surplusing, transfer, trade-in, disposal of computers, or replacement of electronic storage media, and computer software without ensuring the proper disposal of installed and removable digital storage. These risks may include:

- Violation of software license agreements.
- Unauthorized release of sensitive and/or confidential information.
- Violation of federal laws including but not limited to the GrammLeach-Bliley Act (GLBA), the Health Insurance Portability and Accountability Act of 1996 (HIPAA), The Family Educational Rights and Privacy Act (FERPA), etc.
- Unauthorized disclosure of trade secrets, copyrights, and other intellectual property that might be stored on the hard disks and other storage media.

AGENCY RESPONSIBILITIES

1. Ensure compliance with the Record Retention and Disposal Schedule before following this procedure.
2. Whenever licensed software on any computer media being surplused, transferred, traded-in, disposed of, or the hard drive is replaced, the terms of the license agreement shall be followed.
3. Ensure all electronic storage media shall have all SOM data properly removed prior to disposal (this does not apply where the equipment is being transferred or re-assigned within the same agency with a specific intent to also transfer the software and data).
4. Data removal procedures shall be properly documented in accordance with this standard and in accordance with any software manufacturers' guidelines to prevent unauthorized release of sensitive and/or confidential information that may be stored on that equipment and other electronic media.
5. Agencies may comply with this standard by:
    - Disposing of the data themselves.
    - Using a media disposal vendor certified to ensure adequate security controls and destruction of data.
    - Coordinate with DTMB to ensure adequate security controls and destruction of data.

6. Maintain a record of compliance with this standard, and tag equipment as having had the data removed. The record shall include the following information:
    - The method(s) used to expunge the data from the storage media.
    - The type of equipment/media from which data was removed.
    - The name of the person responsible for the removal of the data.
    - The name and signature of their supervisor.
7. Make contractors, vendors and third party providers of data operations and services to the SOM aware of the requirements of this standard and require their compliance by contract language and oversight.
    a. Ensure proper disposal of digital information contained on the media installed on equipment is accomplished.
        i. Agencies may meet this requirement by mandating the return of the storage media. Use of registered mail or process to establish chain of custody is required to ensure adequate accountability during transit.

DTMB RESPONSIBILITIES

1. Define acceptable methods to remove and cleanse digital media of data in a manner that gives assurance that the information cannot be recovered.
    a. Agencies may use the following methods to completely erase or make data unreadable:
        i. When clearing data use three passes with a disk wiping utility using the DoD 5220.22-M (E) method.
            - Writes zero bytes (0x00).
            - Writes high bytes (0xFF).
            - Writes pseudo-random bytes.
        ii. Optional last pass verification.
        iii. When purging the data, use a National Security Agency/Central Security Service (NSA/CSS)-approved degausser except for optical media such as CDs/DVDs where it must be physically destroyed.
        iv. Physical destruction includes:
            - Incineration.
            - Shredding.
            - Disintegrating.
            - Cutting, drilling, or grinding.

        This must be used for all devices such as personal computers, laptops, printers, PDAs, routers, firewalls and switches where DTMB is satisfied that the method will cleanse all SOM protected data.

b. Before the removal process begins, the computer shall be disconnected from any network to prevent accidental damage to the network operating system or other files on the network.

c. An "erase" feature (e.g., putting a document in a trash can icon) or deleting a file is not sufficient for sensitive information because the information may still be recoverable.

   Disposal of digital media shall be done in accordance with all applicable state or federal surplus property and environmental disposal laws, regulations or policies.

d. When contractors, vendors or third party providers are used to accomplish disposal, a log shall be maintained for audit containing, at a minimum:

   - The serial numbers and asset tag numbers of the equipment.
   - Tag numbers of all media delivered.
   - The name of the person receiving the SOM assets for disposal.
   - A signed receipt.

2. Certify fully functioning implementation of access as authorized.
3. Certify compliance with established IT security policies, standards and procedures.
4. Through MCS, review and monitor procedure to ensure appropriate authorization methods are implemented and take actions necessary to ensure compliance with SOM IT security policies, standards, and procedures.
5. Through Internal Auditor, conduct periodic audits of IT Resources for appropriate controls to maintain compliance with policy and standards.

UNIQUE STORAGE SITUATIONS

Unique digital data storage situations not obviously covered by this standard should be coordinated with DTMB Michigan Cyber Security, Risk Management Division.

CONFORMANCE

The policy described in this section sets a minimum level of conformance that will be implemented across the enterprise. SOM departments desiring to implement more stringent practices and procedures for their information technology environments may do so with the approval of Michigan Cyber Security (MCS).

AUTHORITY

Authority is The Department of Management and Budget Act, Public Act 431 of 1984, as amended, § 203.

DEFINITIONS

Data/System Owner

Senior management of the Agency that is ultimately responsible of ensuring the protection and appropriate use of their business' data.

Encryption

The translation of data into a secret code. Encryption is the most effective way to achieve data security. To read an encrypted file, you must have access to a secret key that enables you to decrypt it.

Mobile Devices

Any mobile device (state-owned or privately-owned) capable of storing data. Examples include, but are not limited to: laptops, tablet PCs, BlackBerrys, cell phones, PDAs, iPods, iPads, smart phones, digital cameras and players.

For the purpose of this standard, all non-state-owned computing or data storage equipment (e.g., PC, server, Network Attached Storage (NAS), and Storage Area Network (SAN) are considered mobile devices.

Portable Media

Any portable media (state-owned or privately-owned) capable of storing data. Examples include, but are not limited to: external hard drives, USB thumb drives, flash drives, memory sticks and cards, CDs, DVDs, and floppy disks.

Sensitive Information and Data

Sensitive data is defined as information that is protected against unwarranted disclosure. Access to sensitive data must be safeguarded. Protection of sensitive data may be required for legal or ethical reasons, for issues pertaining to personal privacy, or for proprietary considerations.

Sensitive Information includes but is not limited to all data which contains:

- Personal Information, as defined by the Michigan Identity Theft Protection Act, ACT 452 of 2004.
- Protected Health Information, as defined by the Health Insurance Portability and Accountability Act of 1996 (HIPAA).
- Student education records, as defined by the Family Educational Rights and Privacy Act (FERPA).
- Card holder data, as defined by the Payment Card Industry (PCI) Data Security Standard (DSS).
- Information that is deemed to be confidential in accordance with Internal Revenue Service Publication 1075 Section 8.0, Disposing Federal Tax Information (FTI).
- Information that is deemed to be confidential by the Criminal Justice Information Service (CJIS) Section 5.8.3 Electronic Media Sanitization and Disposal; Section 5.8.4 Disposal of Physical Media.

- Information that is protected, governed or restricted in some manner by a federal or state statute, agreement, rule, policy or requirement by SOM policy from unauthorized access.

In addition to above, Agencies may assign data classifications to their data elements. Encryption would be required for all Agency-specific information labeled sensitive.

APPROVING AUTHORITY

David B. Behen, Director Revised: 10/21/2015