Electronic Data Disposal and Media Sanitization

Standard number: DS-11
Date issued: 5/4/2017
Date last updated: 2/28/2025
Date last reviewed: 2/28/2025
Date of next review: 2/28/2027
Version: 1.1
Approval authority: Vice President for Information Technology and CIO
Responsible office: Information Assurance

This Standard supports and supplements Information Security (SPG 601.27). The Standard is mandatory and enforced in the same manner as the policy. It will be periodically reviewed and updated as necessary to meet emerging threats, changes in legal and regulatory requirements, and technological advances.

I. Overview

When files are improperly or inadequately purged from storage media, it is often still possible to reconstruct or retrieve data. In order to mitigate the potentially significant risk of unauthorized disclosure of U-M data classified as Restricted, High, or Moderate, storage media must be appropriately sanitized to prevent unauthorized access to or disclosure of sensitive institutional data.

In addition to being a widely accepted security and privacy practice, effective media sanitization is required by some regulations that the university is obligated to follow, including HIPAA, GLBA, and ITAR and EAR (export control), as well as by government-funded research grants.

Data must be permanently erased or purged from devices (e.g., computer, server, laptop, multi-function printer, medical equipment, cell phone, digital communications equipment) or storage media (e.g., CD, USB drive, workstation/server hard drives, external hard drives) prior to transfer within the university or other disposition. Effective media sanitization requires the application of certified techniques to prevent recovery or reconstruction of residual stored data on the media appropriate to the classification level of the data and type of media.

II. Scope

This standard applies to the Ann Arbor campus, Michigan Medicine, UM-Dearborn, UM-Flint, all affiliates, and all faculty, staff, workforce members, and sponsored affiliates. It further applies to:

- All units, faculty, principal investigators, staff, and workforce members that maintain or store data classified as Restricted, High, or Moderate on any university-owned device, whether or not it is connected to the campus network;
- Personally owned devices that have stored Restricted, High, or Moderate data, in accordance with provisions of Security of Personally Owned Devices That Access or Maintain Sensitive Institutional Data (SPG 601.33); this provision specifically applies when a U-M employee changes positions from one department to another or leaves the university;
- Any storage media that has been used to store Restricted, High, or Moderate digital or electronic university information or data (this Standard does not apply to any paper records), even temporarily;
- Storage media that maintain data exclusively classified as Low can utilize the least rigorous technique of sanitization prior to transfer or disposal;
- Storage media being transferred within the university, returned or disposed of at the conclusion of a lease, or disposed of at the end of its useful life;
- Any third-party provider with a contractual relationship with the university that maintains the same data types.

III. Standard

Sanitization is defined as the erasure, overwriting, or destruction of storage media to the extent that data cannot be recovered using normal system functions or software data recovery utilities.

It is assumed that all U-M owned devices have stored at a minimum data classified as Moderate. Consequently, all U-M owned devices must be sanitized according to this Standard at their end-of-

life or prior to disposal as surplus. Specifically, no device or storage media containing personally identifiable information or any data classified as Restricted, High, or Moderate can be transferred or disposed of as surplus unless the appropriate UM-approved sanitization methodology has been completed and certified.

U-M Property Disposition has sole responsibility for the disposition of university-owned property, per Acquisition, Use and Disposition of Property (SPG 520.01). Units, departments, or individuals with U-M owned devices must either a) sanitize the devices using the procedure and method described below, or b) have Property Disposition do the sanitizing and be charged for their sanitization service.

For storage media containing data that is subject to regulation or contractual agreement requiring either (a) specific sanitization procedures or (b) a level of assurance of sanitization above that described in this Standard, the requirements in this Standard are superseded by the regulatory or contractual requirements, and responsible parties should employ methods that meet their specific, elevated requirements.

The primary responsibility for sanitizing computer systems, electronic devices and media rests with the units, departments, or individuals that purchased them. Appropriate sanitization can be accomplished by one of the following methods (additional guidance is available on Safe Computing):

Unit, Department, or Individual

The university has licensed tools for secure wiping or sanitization of all university-owned storage media and devices that have maintained Restricted, High, or Moderate data. Satisfactory execution of this software results in media and devices meeting NIST compliance standards for data destruction, which then allows for the safe recycling or other disposition of the media.

- *U-M-Owned Devices:* Units, departments, or individual faculty and staff that do their own sanitization of U-M-owned media and devices are required to print a Certificate of Destruction, maintain a copy for three years, and attach another copy to all media transferred as surplus to U-M Property Disposition. In the absence of a Certificate of Destruction, U-M Property Disposition will assume that a device has not been properly sanitized. It will erase the device using appropriate tools and assess the unit its standard fee for such service.
- *Personally Owned Devices:* Individual faculty and staff members who access or maintain sensitive institutional data on their personal devices in compliance with provisions of Security of Personally Owned Devices That Access or Maintain Sensitive Institutional Data (SPG 601.33) are required to securely wipe or sanitize such devices prior to their disposition. For more information on tools and services available for personal devices, visit Safe Computing. It is strongly recommended to sanitize personal devices before disposal, transfer, or resale to protect personal information and data, even if never used to store U-M data.

U-M Property Disposition

Storage media declared by units as surplus must be sent to U-M Property Disposition for reuse, disposal or destruction. In the absence of a Certificate of Sanitization/Physical Destruction provided by the unit, U-M Property Disposition will assume that a device has not been properly sanitized. It will erase or destroy the device using appropriate tools and assess the unit its standard fee for such service according to a service level agreement. Property Disposition will maintain the Certificate of Sanitization/Physical Destruction.

Physical Data and Device Destruction

In instances where secure erasure is not possible (e.g., hard drive is inoperable), storage media should be physically destroyed using a NIST 800-88 certified physical destruction method. U-M Property Disposition maintains a contract with a third-party vendor, which units can use, for a fee, to physically destroy hard drives and receive a Certificate of Sanitization/Physical Destruction. Units are strongly discouraged from attempting to physically destroy storage media themselves.

Copiers, Fax Machines, Scanners, and Printers

Multifunction office devices usually retain a cached digital copy on the device's hard drive of some or all the documents printed, scanned, or processed.

It is important to take appropriate hardening steps to minimize the risk of loss or unauthorized disclosure of Restricted, High, or Moderate data that may be retained on both standalone and networked devices while in use by a unit or department. The physical security of removable hard drives must be properly accounted for when devices are undergoing maintenance work.

Once a machine has reached the end of its useful life or lease, its transfer, return, or disposal must be preceded by rendering any cached sensitive information or data unrecoverable.

- U-M Procurement Services' vendor for the Managed Copier Program will handle such sanitization prior to reuse or disposal for equipment leased by units.
- Units that own their equipment must first determine whether the device retains digital copies on its hard drive. If so, units should determine if vendor-provided tools offer adequate sanitization to meet this Standard. Otherwise, units should request that U-M Property Disposition handle the sanitization of the equipment.

Licensed Software

In accordance with provisions of Software Procurement and Licensing Compliance (SPG 601.03-3), units and individuals should appropriately reuse, transfer, return, remove, or delete licensed software

in compliance with licensing agreements before transferring or disposing of any storage media to ensure that no software is disposed of or transferred in violation of its license. Specifically, all non-transferable licensed software should be permanently deleted before any electronic device or media is disposed of or transferred within or external to U-M.

Documentation

Units and individuals are required to document and retain for a period of three years a record of storage media data removal or destruction for all media that stored Restricted, High, or Moderate data.

- This requirement applies to destruction carried out at the unit or individual level, by U-M Property Disposition, or by a third-party vendor.
- A sample Certificate of Sanitization/Physical Destruction is provided here for units and individuals that handle sanitization and physical destruction on their own.
- Unit or university IT staff as well as Property Disposition will routinely provide a Certificate of Destruction for any storage media provided to them for disposal or destruction.
- Some laws, regulations, or contractual agreements may require that Certificates of Sanitization/Physical Destruction be retained for periods of time different from the above three-year retention period; in which case, such requirements supersede the retention period as stipulated by this Standard.
- Obtaining a Certificate of Sanitization/Physical Destruction for media that stored data classified as Low is optional.

IV. Violations and Sanctions

Failure to properly purge data in a manner that renders the data unrecoverable may pose a significant risk to the university since data often can easily be recovered with readily available tools.

Violations of this Standard may result in disciplinary action up to and including suspension or revocation of computer accounts and access to networks, non-reappointment, discharge, dismissal, and/or legal action.

Discipline (SPG 201.12) provides for staff member disciplinary procedures and sanctions. Violations of this policy by faculty may result in appropriate sanction or disciplinary action consistent with applicable university procedures. If dismissal or demotion of qualified faculty is proposed, the matter will be addressed in accordance with the procedures set forth in Regents Bylaw 5.09. In addition to U-M disciplinary actions, individuals may be personally subject to criminal or civil prosecution and sanctions if they engage in unlawful behavior related to applicable federal and state laws.

Any U-M department or unit found to have violated this Standard may be held accountable for the financial penalties, legal fees, and other remediation costs associated with a resulting information security incident and other regulatory non-compliance.

V. Implementation

Information Assurance is responsible for the implementation, maintenance and interpretation of this Standard.

VI. References

- NIST SP 800-53r5: *Security Controls Catalog*
- NIST SP 800-88r1: *Guidelines for Media Sanitization*
- FIPS Publication 140-2: *Security Requirements for Cryptographic Modules*
- Acquisition, Use and Disposition of Property (Exclusive of Real Property) (SPG 520.01)
- Identification, Maintenance, and Preservation of Digital Records Created by University of Michigan (SPG 601.08-1)
- Security of Personally Owned Devices That Access or Maintain Sensitive Institutional Data (SPG 601.33)
- Software Procurement and Licensing Compliance (SPG 601.03-3)
- Safe Computing: Erase or Destroy U-M Devices

VII. Related NIST Security Controls

- NIST SP 800-53 Revision 5
  - MA-02 (d) Controlled Maintenance
  - MA-03 (3)(b) Maintenance Tools
  - MA-05 (1)(a)(2),(1)(b) Media Transport
  - MP-04 (b) Media Storage
  - MP-06 Media Sanitization
  - MP-7 (2) Media Use
  - MP-8 (4) Media Downgrading
  - SC-4 (2) Information in Shared Resources