Status Draft PolicyStat ID 21278714

UNIVERSITY OF WEST GEORGIA

Last Approved N/A
Effective N/A
Next Review N/A

Area IT/ Management (Procedures)
Responsible Party Information Technology Services

Hardware and Electronic Media Disposal

Authority for Procedure granted by UWG Policy #5002, Data Security.

A. Procedure

This procedure establishes the requirements for the secure Sanitization and Disposal of University-owned devices or managed Electronic Storage Media. Its purpose is to prevent unauthorized access to institutional data and ensure compliance with applicable legal, regulatory, and contractual obligations.

B. Scope

This procedure applies to:

- All University employees, contractors, and affiliates.
- All University-owned, leased, or managed devices and Electronic Storage Media, including but not limited to:
    - Desktop and laptop computers, servers, tablets, and mobile devices
    - Copiers, printers, and POS equipment
    - Hard drives, solid-state drives, USB drives, optical Media, backup tapes
    - Any device or component capable of storing institutional data
- Personally owned devices used to store or process University data.
- Devices and Media transferred, repurposed, returned from lease, or disposed of at end-of-life.

C. General Requirements

- Devices and Electronic Storage Media must be **Sanitized prior to reuse or transfer.**

- Devices and Electronic Storage Media **not** Sanitized must be Destroyed**.**
- Media shall be presumed to contain Sensitive or Confidential Information unless verified otherwise
- Where stricter legal, regulatory, or contractual requirements exist, those requirements take precedence

D. Roles and Responsibilities

Units and/or employees that purchase or manage University-owned devices or Electronic Storage Media are responsible for:

- Ensuring device/Media is Sanitized prior to transfer or Disposal
- Maintaining custody and security of device/Media until Sanitization or destruction is complete
- Completing and submitting any required documentation (i.e. Transfer of Equipment form)
- Complying with institutional, regulatory, and/or contractual requirements for enhanced sanitization or Sensitive data.

Information Technology Services (ITS) is responsible for

- Maintaining approved Sanitization tools and vendor Disposal contracts
- Providing guidance and performing Sanitization or destruction when required
- Maintaining records of Sanitization and destruction activities

Asset Management is responsible for

- Managing equipment surplus and disposition processes
- Verifying sanitization documentation prior to accepting devices

Contractors and Affiliates must comply with this procedure by

- Protecting University data, devices, and Electronic Storage Media under their control
- Immediately reporting suspected data security incidents or improper Disposal to ITS

Third-Party Vendors must

- Follow recognized standards (e.g., NIST SP 800-88)
- Provide written certification of Sanitization or Destruction
- Ensure environmentally responsible Disposal

Media Handling and Security

- Electronic Storage Media must be stored in a **secure, access-controlled environment** until

Sanitized or Destroyed

- If data classification is unknown, Media must be treated as Confidential and/or Sensitive.
- Media must remain tracked and controlled throughout the Disposal process.

Sanitization Standards

Sanitization shall be performed using one of the following approved methods:

- **Clear:** Overwriting data using approved software tools
- **Purge:** Advanced techniques such as Cryptographic erase or Degaussing
- **Destruction:** Physical destruction of Electronic Storage Media (e.g., shredding, pulverizing)

Method Selection

- Clear or Purge methods shall be used when device/Media is intended for reuse
- Physical destruction shall be used when device/Media cannot be Sanitized or is no longer needed.

  Physical destruction shall be performed by ITS or an approved vendor.

E. Sanitization and Destruction Process

Phase 1: Pre-Sanitization Review and Approval

1. **Data Verification**
   Units **shall** confirm that data stored on the device or Electronic Storage Media is expired or no longer required for business use in accordance with USG Records Retention Schedules prior to sanitization or destruction.
2. **Management Approval**
   Management or Data Owner approval **shall** be obtained (can be in the form of an email) **when required** by data classification, regulatory obligation, contractual requirement, or institutional policy before the device or Media is removed from service.
3. **Secure Custody**
   Units **shall** secure the device or Media in a locked or access-controlled location until transfer.

Phase 2: Request, Clearing, and Submission

1. **Initial Data Clearing and Documentation**
   Units **shall** perform initial data Clearing using University-approved methods before submitting the device or Media for sanitization or destruction.
   A **Certificate of Destruction Form must** be completed when records **or Media are permanently Destroyed.**
2. **Service Desk Ticket Submission**

Units **must** submit a request through the ITS Service Desk, indicating **"Device/Media Disposal."**
The Service Desk ticket number **shall** be clearly recorded on the device or Media.

Units **shall** maintain custody of and **must** safeguard Media at all times during transport to prevent unauthorized access or disclosure.

Phase 3: Inventory, Tracking, and Completion

1. **Inventory and Secure Storage**
   ITS **shall** inventory received device/Media, update the Service Desk ticket, and store the Media in a secure, access-controlled environment until sanitization, shipment, or destruction is completed.
2. **Notification and Completion**
   ITS **shall** notify the submitting unit of Media shipment and final sanitization or destruction through the Service Desk ticket.

F. Transfer or Disposal

Devices Submitted for Surplus

- All University-owned devices must be processed through Asset Management
- Required documentation (i.e., **Media Disposal Form)** must accompany the device
- Devices submitted without verification may be returned or forwarded to ITS for sanitization or destruction.

Media Sanitized by Departments

Departments or employees that perform their own sanitization of University-owned Media must:

- Complete a **Certificate of Destruction Form**
- Include the form when submitting the Media to Asset Management or ITS for surplus or to ITS for destruction.

If documentation is not provided, Asset Management or ITS will treat the Media as **unsanitized** and may perform sanitization or destruction to ensure compliance.

G. Special Considerations

- **Personally Owned Devices** used for University business must be Sanitized before Disposal, transfer, or resale.
- **Licensed Software** must be removed or transferred in compliance with licensing terms.
- **Third-Party Destruction:** Only approved vendors may be used to perform device or Media destruction; written certification is required.

H. Recordkeeping

The following records must be maintained in accordance with applicable retention requirements:

- **Certificates of Records Destruction (**Office of Legal Affairs)
- **Sanitation logs** Records must be securely maintained and available for audit or compliance review.

I. Compliance and Enforcement

Failure to comply with this procedure will be treated as an information security violation and may result in:

- Disciplinary action, up to and including termination of employment, non-reappointment, or dismissal for faculty, staff, or contractors.
- Suspension or revocation of information system access.
- Financial liability for damages or data breaches.
- Civil or criminal penalties under applicable laws.

Definitions

Clearing - a level of sanitization by overwriting data with zeros or random characters that renders Media unreadable through normal means by overwriting data.

Confidential Information - information maintained by the institution that is exempt from disclosure under the provisions of the Open Records Act or other applicable state or federal laws.

Cryptographic Erase – a method of sanitization in which the media encryption key (MEK) for the encrypted target data is sanitized, making recovery of the decrypted target data infeasible.

Degaussing – a pPurge-level sanitization method that permanently erases data on magnetic storage Media by applying a powerful magnetic field, rendering the Media unusable.

Destroy– physically **r**endering Media unusable. Destruction techniques include but are not limited to disintegration, incineration, pulverizing, shredding and melting. A common practice when permanently discarding hard drives.

Disposal - discarding Media with no other sanitization considerations (e.g., recycling paper, deleting electronic files, or throwing away electronic Media).

Electronic Storage Media – devices capable of storing data, including but not limited to hard drives, CDs, DVDs, USB drives, SD cards, tapes, ZIP disks, and floppy disks.

Media – tools or communication outlets used to store and deliver information or data, such as, but not limited to print, digital , photography, or publishing.

Personally Identifiable Information (PII) - any information that can be used to identify an individual, either directly or indirectly. This includes names, identification numbers, addresses, and other data linked to a person, regardless of their citizenship or affiliation with the institution.

Purging - advanced sanitization rendering Media unreadable even through specialized attacks; Degaussing is acceptable. For this procedure, Clearing and Purging are treated the same.

Sanitization - the process of securely erasing, overwriting, or the destruction of storage Media to the extent that data cannot be recovered using normal system functions or data recovery software.

Sensitive Information - any data maintained by the institution that requires special precautions to protect it from unauthorized access, use, disclosure, modification, loss, or deletion. This includes both public and Confidential Information that demands a higher-than-normal level of assurance regarding its accuracy, completeness, and security due to its potential impact if compromised.

Sensitive Personally Identifiable Information (Sensitive PII) - a subset of PII that, if disclosed without authorization, could cause significant harm, embarrassment, disruption, or unfairness to the individual, such as Social Security numbers or immigration identification numbers. Sensitive PII requires stricter protection and handling due to the increased risk if compromised.

Forms

Certificate of Destruction Form

Guidelines and Related Materials

National Institute of Standards and Technology (NIST) Special Publication 800-88, Rev. 2, Guidelines for Media Sanitization.

- Family Educational Rights and Privacy Act (FERPA)
- Health Insurance Portability and Accountability Act (HIPAA)
- Gramm-Leach-Bliley Act (GLBA)
- Payment Card Industry Data Security Standards (PCI DSS)
- ISO/IEC 27002: Information Security Controls

Contact Information

For questions or assistance, contact Information Technology Services (ITS):

Email: servicedesk@westga.edu

Phone: (678) 839-6587

Approval Signatures

Step Description	Approver	Date
	Dale Driver	04/2022
	Tara Pearson	08/2021