THE UNIVERSITY OF TENNESSEE HEALTH SCIENCE CENTER

UT Health Science Center: IT0311-HSC-D.01 Disposal or Destruction of Electronic & Non-Electronic Media	
Version 4	Effective Date: 01/09/2022

Responsible Office: Office of Cybersecurity	Last Review: 03/01/2025 Next Review: 03/01/2027
Contact: Chris Madeksho	Phone: 901.448.1579 Email: mmadeksh@uthsc.edu

Purpose

To establish the minimum standard security requirements and responsibilities for the University of Tennessee Health Science Center (UTHSC) media through the disposal or destruction of said media.

This practice is also designed to meet compliance requirements for data regulated by federal or state law. This includes, but is not limited to, security requirements and safeguards for the Family Educational Rights and Privacy Act (FERPA), Health Insurance Portability and Accountability Act (HIPAA), or Gramm-Leach-Bliley Act (GLBA).

Scope

This Practice applies to any form of data, including paper documents and digital data stored on any type of media. It applies to all UTHSC employees, students, and third-party agents authorized to access UTHSC data.

Definitions

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.

Information System - A major application or general support system for storing, processing, or transmitting University Information. An Information System may contain multiple subsystems. Subsystems typically fall under the same management authority as the parent Information System. Additionally, an Information System and its constituent subsystems generally have the same function or mission objective, essentially the same operating characteristics, the same security needs, and reside in the same general operating environment.

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

Responsibilities

Data Owner is ultimately responsible for the data and information being collected and maintained by their department or division, usually a member of senior management. They are responsible for the sanitization of the data and/or media.

Office of Cybersecurity is responsible for establishing security controls and procedures to protect UTHSC intellectual property and data. The classification of data is per IT0005-HSC-A-Data & System Classification. The security of the data is based on IT0311-HSC-D-Data Security.

Third-party media destruction services physically inventory the surplus devices to be destroyed and execute the destruction.

Practice

1. As per IT0311-HSC-D-Data Security, data must be properly managed from its creation, through authorized use, to proper disposal.
2. Data Owners must ensure University information, information systems, and related resources of any classification, as defined in IT0005-HSC-A-Data & System Classification, are protected and monitored in a manner that reduces the risk to the confidentiality, integrity, and availability, while ensuring UTHSC is enabled to conduct research, work, and daily tasks consistent with UTHSC standards.
3. At the end of life of all UTHSC-owned equipment, it must be processed by UTHSC Surplus Process.
4. Data destruction follows the recommendations of NIST 800-88, Rev. 1, Guidelines for Media Sanitization, Minimum Sanitization Recommendations.
5. Destruction of information shall be in accordance with the applicable records-retention schedule under the University of Tennessee System Records Management Policy (UTSA FI0120–Records Management)
6. Examples of the methods of sanitization on specific device types are found on the Sanitization webpage.

Below are specific sections of NIST 800-88

Methods of Media Sanitization

The following table depicts the three types of sanitization methods and the impact of each method.

Sanitization Method	Appropriate Use	Description
Clear	If the media will be reused and will not be leaving the entity's control.	Protects confidentiality of information against an attack by replacing written data with random data. Clearing must not allow information to be retrieved by data, disk or file recovery utilities.
Purge	If the media will be reused and leaving the entity's control.	Protects confidentiality of information against an attack through either degaussing or Secure Erase.
Physical Destruction	If the media will not be reused at all.	Intent is to completely destroy the media.

Reference NIST 800-88, Rev. 1, Guidelines for Media Sanitization, Minimum Sanitization Recommendations Appendix A for specific examples of media types and sanitization options.

Use of Cryptography and Cryptographic Erase

If the media or storage device has integrated encryption and access control capabilities, known as self-encrypting drives (SEDs), cryptographic erase can be used.

Cryptographic erase leverages the encryption of target data by enabling sanitization of the target data's encryption key. This leaves only the ciphertext remaining on the media, effectively sanitizing the data by preventing read-access.

Reference NIST 800-88, Rev. 1, Guidelines for Media Sanitization, Minimum Sanitization Recommendations Section 2.6 for more information on the appropriate use of cryptographic erase.

Sanitization Decision Process

The decision process is based on the confidentiality of the information, not the type of media. The data owner sanitized the data based on the data classification, and the method of sanitization is approved by the Information Owner. The technique used may vary by media type and by the technology available to the custodian, so long as the requirements of the sanitization type are met. Recommended Sanitization

techniques for specific types of media are outlined in Appendix A of NIST 800-88, Rev. 1, Guidelines for Media Sanitization, Minimum Sanitization Recommendations.

Disposal without sanitization should be considered only if information disclosure would have no impact on the organizational mission, would not result in damage to organizational assets, and would not result in financial loss or harm or compromise of privacy to any individuals. This data would have a Public classification according to IT0005-HSC-A-Data & System Classification.

The security classification of the information, along with internal environmental factors, should drive the decisions on how to deal with the media. The key is to first think in terms of information sensitivity, then apply considerations based on the media type. The classifications of low, moderate, and high correspond to the classification in IT0005-HSC-A-Data & System Classification in the following way: Low = Public classification, Moderate = Private or Internal Use Only, High = Restricted.

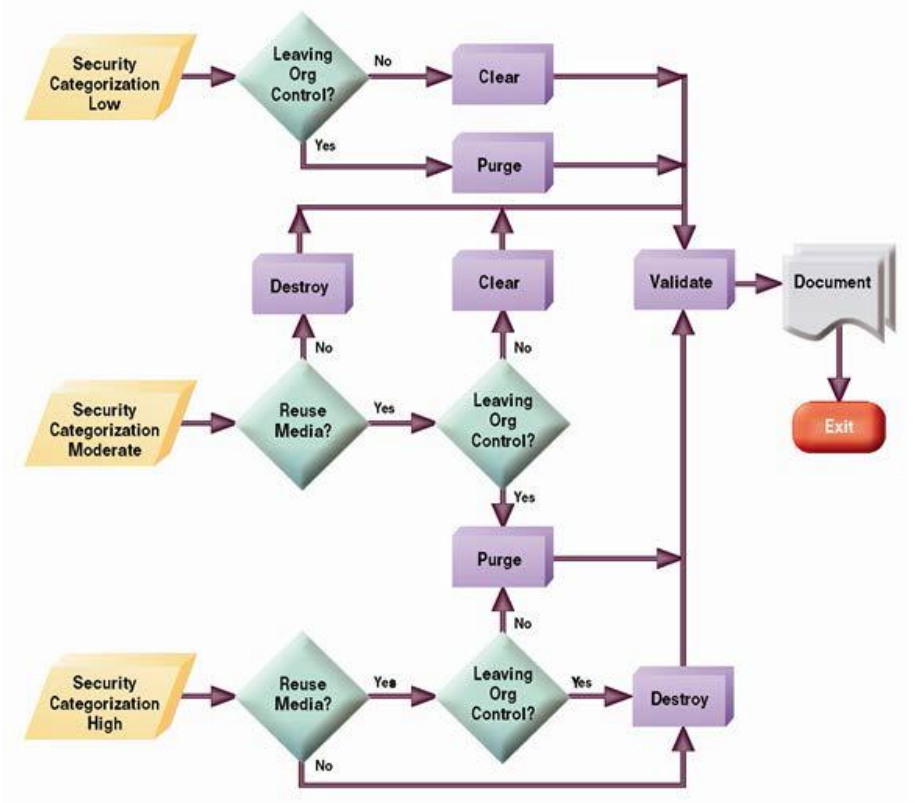

Figure 4.1- Sanitization and Disposition Decision Flow
(*from NIST 800-88, Rev. 1, Guidelines for Media Sanitization*)

The cost versus benefit of a sanitization process should be understood prior to a final decision. The data owner can always increase the level of sanitization applied if that is reasonable and indicated by an assessment of the existing risk. For example, even though Clear or Purge may be the recommended solution, it may be more cost-effective (considering training, tracking, and validation, etc.) to destroy media rather than use one of the other options. Data owners may not decrease the level of sanitization required.

Clear / Purge / Destroy

Method	Description
Clear	One method to sanitize media is to use software or hardware products to overwrite user-addressable storage space on the media with non-sensitive data, using the standard read and write commands for the device. This process may include overwriting not only the logical storage location of a file(s) (e.g., file allocation table) but also should include all user- addressable locations. The security goal of the overwriting process is to replace Target Data with non-sensitive data. Overwriting cannot be used for media that are damaged or not rewriteable and may not address all areas of the device where sensitive data may be retained. The media type and size may also influence whether overwriting is a suitable sanitization method. For example, flash memory-based storage devices may contain spare cells and perform wear levelling, making it infeasible for a user to sanitize all previous data using this approach because the device may not support directly addressing all areas where sensitive data has been stored using the native read and write interface. The Clear operation may vary contextually for media other than dedicated storage devices, where the device (such as a basic cell phone or a piece of office equipment) only provides the ability to return the device to factory state (typically by simply deleting the file pointers) and does not directly support the ability to rewrite or apply media-specific techniques to the non-volatile storage contents. Where rewriting is not supported, manufacturer resets and procedures that do not include rewriting might be the only option to Clear the device and associated media. These still meet the definition for Clear as long as the device interface available to the user does not facilitate retrieval of the Cleared data.
Purge	Some methods of purging (which vary by media and must be applied with considerations described further throughout this document) include overwrite, block erase, and Cryptographic Erase, through the use of dedicated, standardized device sanitize commands that apply media-specific techniques to bypass the abstraction inherent in typical read and write commands. Destructive techniques also render the device Purged when effectively applied to the appropriate media type, including incineration, shredding, disintegrating, degaussing,

	and pulverizing. The common benefit across all these approaches is assurance that the data is infeasible to recover using state of the art laboratory techniques. However, Bending, Cutting, and the use of some emergency procedures (such as using a firearm to shoot a hole through a storage device) may only damage the media as portions of the media may remain undamaged and therefore accessible using advanced laboratory techniques. Degaussing renders a Legacy Magnetic Device Purged when the strength of the degausser is carefully matched to the media coercivity. Coercivity may be difficult to determine based only on information provided on the label. Therefore, refer to the device manufacturer for coercivity details. Degaussing should never be solely relied upon for flash memory-based storage devices or for magnetic storage devices that also contain non-volatile non-magnetic storage. Degaussing renders many types of devices unusable (and in those cases, Degaussing is also a Destruction technique).
Destroy	There are many different types, techniques, and procedures for media Destruction. While some techniques may render the Target Data infeasible to retrieve through the device interface and unable to be used for subsequent storage of data, the device is not considered Destroyed unless Target Data retrieval is infeasible using state of the art laboratory techniques. • *Disintegrate, Pulverize, Melt, and Incinerate*. These sanitization methods are designed to completely Destroy the media. They are typically carried out at an outsourced metal Destruction or licensed incineration facility with the specific capabilities to perform these activities effectively, securely, and safely. • *Shred*. Paper shredders can be used to Destroy flexible media such as diskettes once the media are physically removed from their outer containers. The shred size of the refuse should be small enough that there is reasonable assurance in proportion to the data confidentiality that the data cannot be reconstructed. To make reconstructing the data even more difficult, the shredded material can be mixed with non-sensitive material of the same type (e.g., shredded paper or shredded flexible media). The application of Destructive techniques may be the only option when the media fails and other Clear or Purge techniques cannot be effectively applied to the media, or when the verification of Clear or Purge methods fails (for known or unknown reasons).

Table 5-1 – Sanitization Methods
(*from NIST 800-88, Rev. 1, Guidelines for Media Sanitization*)

Validation

Data owners must test a representative sampling of media for proper sanitization to assure that proper protection is maintained.

Verification of Equipment

If the department is using sanitization tools (e.g., a degausser), the department must have procedures to ensure that the tools are operating effectively.

Verification of Personnel Competencies

Data owners must ensure that equipment operators are properly trained and competent to perform sanitization functions.

Document

Devices sent through the UTHSC Surplus process will be documented by the third-party media destruction service. If devices and media were not disposed of using the UTHSC Surplus process, data owners must maintain a record of their sanitization to document what media were sanitized, when, how they were sanitized, and the final disposition of the media.

Failure to Comply

Failure to comply with this policy will be reported as an information security violation and may result in loss of network and system privileges for the computer and/or disciplinary action per IT0003-HSC-A.03-Information Security Violations for the individual violating the policy.

Exceptions

Exceptions to this Practice should be requested using the process outlined in IT0003-HSC-A.02-Security Exceptions and Exemptions to ITS Standards Practices & Controls.

Policy History

Version #	Effective Date
1	01/09/2022
2	09/27/2022
3	11/13/2023
4	03/01/2025 – new naming convention

References

1. NIST 800-88, Rev. 1, Guidelines for Media Sanitization, Minimum Sanitization Recommendations
2. UTSA FI0120–Records Management
3. UTHSC Surplus Equipment Guidance
4. IT0311-Information Technology Data Access, Management, and Recovery
5. IT0003-HSC-A.02-Security Exceptions and Exemptions to ITS Standards Practices & Controls
6. IT0003-HSC-A.03-Information Security Violations
7. IT0005-HSC-A-Data & System Classification
8. IT0102-HSC-B-Device Life Cycle Security
9. IT0311-HSC-D-Data Security
10. NIST Glossary of Terms