THE UNIVERSITY OF TENNESSEE HEALTH SCIENCE CENTER

UT Health Science Center: IT0102-HSC-B Device Life Cycle Security	
Version 5	**Effective Date: 08/26/2020**

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) devices throughout the life cycle of the device.

Scope

This Standard applies to all UTHSC-owned devices or Information Technology (IT) resource that has the potential to store and transmit UTHSC data.

Definitions

Device – any hardware component capable of executing code, including but not limited to desktops, laptops, tablets, and other portables, servers, and computing appliances

UTHSC Information Technology (IT) Resource - a broad term for all things related to information technology from a holistic point of view and covers all University-owned or managed information technology services, including cloud-based services, that users have access to.

Responsibilities

Business managers/department representative works with ITS to keep the device inventory current. Working with data owners, they conduct security evaluations on devices in accordance with this Standard.

Data Owner is ultimately responsible for the data and information being collected and maintained by his or her department or division, usually a member of senior management. They assign data classification based on the data's potential impact level and determine if data access is allowed.

Information Technology Services (ITS) maintains an inventory of all devices and IT resources.

Office of Cybersecurity is responsible for establishing security controls and procedures to protect UTHSC intellectual property and data. Categorization of data

is per IT-0005-HSC-A-Data & System Categorization. The security of the data is based on IT0311-HSC-D-Data Security.

Third-party media destruction services physically inventories the surplus devices to be destroyed and executes the destruction.

Standard

All computing devices and systems that are used for UTHSC business and/or are connected to the UTHSC network must have an individual or an operational group responsible for the configuration, maintenance, and administration of these devices and systems throughout the life cycle of the device. 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.

Procurement

1. All devices must be purchased from campus-approved vendors with whom UTHSC has a vendor repair agreement.
2. UTHSC does not purchase any products from manufacturers with known high risks to cybersecurity.
3. The current list of banned products and manufacturers can be found at https://uthsc.edu/its/cybersecurity/banned-manufactures.php
4. All computing devices and systems used for UTHSC business and/or connected to the UTHSC network must have an individual or an operational group responsible for configuring, maintaining, and administering them.
5. New devices purchased with UTHSC funds should meet the minimum hardware requirements in this Knowledge Base article.
6. The Data Owner, Business Manager or department representative must perform a security evaluation on computers that will be used to store data or information with a level 2 or above categorization, and/or will be used to provide concurrent user access to data or information with a level 2 or above categorization (i.e. a server).
    a. The recommendations generated from the security evaluation must be

followed prior to the use of the computer in production, prior to use by users, and prior to interaction with data or information with a level 2 or above categorization unless otherwise stated in the evaluation report.

7. Plan your data disposal requirements as part of the planning process for the devices that will store the data.
    a. If the data is to be stored on a cloud service, make sure that the cloud service provider can meet the data destruction requirements for the data classification level from IT0005-HSC-A-Data & System Categorization.

Installation

1. All devices should be configured by the ITS Hardware team using current and standardized specifications.

In use

1. All UTHSC-owned assets must be managed with approved security and management software. Management is defined as the following:
    a. Windows Operating Systems:
        i. Assets must be joined to the UTHSC Active Directory (AD).
        ii. Assets must use the most recent approved operating system image at the time of joining the network and maintain supported operating systems while on the network.
        iii. Assets will use domain accounts for user access to the computer. Local accounts will only be made with the exception and approved by the UTHSC Office of Cybersecurity.
        iv. Assets must be enrolled in the approved ITS Mobile Device Management (MDM).
    b. MacOS:
        i. Assets must be enrolled in JAMF
        ii. Assets must use the most recent approved operating system image at the time of joining the network and maintain supported operating systems while on the network.
        iii. Assets must have the UT local administrator account.
2. UTHSC-owned assets must have the currently supported UTHSC-approved EDR (Endpoint Defense and Response) software
3. UTHSC-owned assets must also have CISCO AnyConnect unless an approved exception is granted by the UTHSC Office of Cybersecurity.

4. UTHSC-owned assets should be powered ON during the weekend hours. Windows devices should be connected to the UTHSC network via VPN. This is in order to receive security patches and updates.
5. The UTHSC Office of Cybersecurity may require or initiate security validation testing for the purpose of identifying vulnerabilities.
6. Computers determined by the security evaluation process to present an unacceptable security risk to UTHSC are prohibited from accessing or using the UTHSC network, and from interacting with UTHSC data or information with a classification rating of 3 in any area.
7. The UTHSC Office of Cybersecurity may, at any time, disconnect a Computing device from the UTHSC network that has been identified as creating an unacceptable security risk.
8. Do not store contractually restricted or compliance-restricted data on removable media.
9. ITS recommends refreshing or replacing endpoints every three to five years. More information about the refresh cycle is found in this Knowledge Base article.

End of life

1. When hardware can no longer support modern or supported operating systems, or they are no longer needed by the department, college or unit, they must be surplussed using guidelines found at https://www.uthsc.edu/finance/procurement/surplus/index.php.
2. All covered IT Resources when re-used, removed, donated, sold, or disposed of shall have all information removed and/or destroyed in such manner that the information cannot be retrieved, even partially, by conventional means or commercially available processes.
3. Removal and destruction of any (or potential) data shall be in accordance with IT0311-HSC-D.01-Disposal or Destruction of Electronic & Non-Electronic Media. Examples of the methods of sanitization on specific device types are found on the Sanitization webpage.
4. Destruction of data shall be in accordance with the applicable records-retention schedule.
5. A record shall be maintained detailing the property decal number, time and date, a description of the IT Resource, the disposition of the IT Resource, the procedure employed to remove and/or destroy the information, and the individual executing the procedure.

6. Acceptable methods of data destruction include, but are not limited to, the following:
   a. Overwriting: Unlike other data-destruction methods, overwriting preserves the media for re-use after the data-destruction process. This needs to comply with the Department of Defense (DOD) data destruction standard, DOD 5220.00-M. Only industry-standard tools can be used. A minimum of three overwriting passes are required.
   b. Degaussing: Degaussing is exposing magnetic media to a strong magnetic field in order to disrupt the recorded magnetic domains. A degausser is a device that generates a magnetic field used to sanitize magnetic media.
   c. Destruction: Destruction involves the physical dismantling or disablement of the media. UTHSC has contracted with an outside facility for media destruction services. (Note: Electronic media disposal service companies contracted by UTHSC must be certified by the National Association for Information Destruction.)
      i. Shredding can be used to destroy flexible media, such as floppy discs.
      ii. Optical mass storage media must be destroyed by pulverizing, crosscut shredding, or burning. When material is disintegrated or shredded, all residues must be reduced to nominal edge dimensions of five millimeters (5 mm) and surface area of 25 square millimeters (25 mm2).
   d. Further information about the appropriate destruction techniques are explained in IT0311-HSC-D.01-Disposal or Destruction of Electronic & Non-Electronic Media.

Note: Almost all computers and mobile devices, including cell phones, implement some form of storage media. Care must be taken at the time of disposal or recycling to discover the storage within and destroy the data it stores according to these standards. If the existence of internal storage cannot be definitively ruled out, then the device must be destroyed.

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	08/26/2020
2	03/30/2021
3	05/12/2022
4	09/27/2022
5	03/01/2025 – new naming convention

References

1. IT0102-Information Technology Asset Management
2. IT0003-HSC-A.02-Security Exceptions and Exemptions to ITS Standards Practices & Controls
3. IT0005-HSC-A-Data & System Categorization
4. IT0102-HSC-D-Physical Security of Information Resources and Related Facilities
5. IT0311-HSC-D-Data Security
6. IT0311-HSC-D.01-Disposal or Destruction of Electronic & Non-Electronic Media
7. GP-001.04-Information Security Violations
8. UTHSC Surplus Equipment Guidance