THE UNIVERSITY OF TENNESSEE HEALTH SCIENCE CENTER

UT Health Science Center: PE-001-Physical Security of Information Resources and Related Facilities	
Version 6	**Effective Date: 03/17/2016**

Responsible Office: Office of Cybersecurity	Last Review: 05/26/2021 Next Review: 05/26/2023
Contact: Chris Madeksho	Phone: 901.448.1579 Email: mmadeksh@uthsc.edu

Purpose

To ensure that Information Technology (IT) resources are protected by physical and environmental security measures that prevent physical tampering, damage, theft, or unauthorized physical access.

Scope

This standard applies to all UTHSC IT Resources operated both on-site and off-site of UTHSC that can store, transmit, and/or process UTHSC information with a classification ranking anything above a zero (0). In addition, this standard also extends to the related facilities in which these resources are located, as well as to all units, faculty, principal investigators, and staff who process, maintain, transmit, or store data on any device, regardless of whether that device connects to the campus network.

Definitions

Device: any hardware component capable of executing code, including but not limited to desktops, laptops, tablets and other portables, servers, and computing appliances. This encompasses local, fixed and removable storage systems and media including, but not limited to, magnetic, solid state, and optical drives; removable disks; USB disks and other devices; memory cards and sticks; CD-ROMs; DVDs; EPROM; magnetic tape; digital photographs; slides; negatives; and other forms of media or storage devices both currently used and that may become available in the future.

UTHSC Information Technology (IT) Resource: Any data, device, or other component of the information environment that supports information-related activities. Assets generally include hardware (e.g. servers and switches), software (e.g. mission critical applications and support systems) and information.

Responsibilities

The Office of Cybersecurity is responsible for setting basic security standards for the IT resource.

Owner/custodian of the IT Resource is responsible for the physical security of the IT Resource and related facilities according to the referenced standards and practices in collaboration and coordination with UTHSC leadership and other pertinent UTHSC organizations and agencies.

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.

a. Owners of original copies of records must ensure the information has met the records-retention requirements before requesting or authorizing the destruction of media containing original information.
b. Owners of duplicative copies of records may destroy the records when they no longer have value for the University, provided the owner of the copy makes certain an original exists in compliance with applicable retention laws.

Data Custodian is responsible for the removal and/or destruction of any information with a classification rating of 3 in any area in collaboration with the owner's designee or delegate. The custodian is also responsible for ensuring a retrievable and exact copy is made of any information with a classification rating of 3 in any area when required or needed and in collaboration with the owner's designee or delegate.

UTHSC community are responsible for maintaining the physical security of the facility, their work area, and IT Resources to prevent unauthorized access, tampering, and theft.

Standard

1. UTHSC IT Resources that store, process, or transmit UTHSC information with a classification ranking anything above a zero (0) per GP-002-Data & System Classification shall be physically secured from unauthorized access and environmental threats that may compromise the security of the Resource.
    a. Facilities containing UTHSC information with a classification ranking anything above a zero (0) equipment (servers, network wiring closets, etc.) must comply with the sections of this Standard.

b. Physical access to workstations, printers, scanners, fax machines, and other equipment that process and display UTHSC information with a classification ranking anything above a zero (0) shall be restricted to prevent unauthorized individuals from viewing UTHSC information with a classification ranking anything above a zero (0); output devices (e.g., printers and displays) should not be located, whenever possible, in public sections of walkways, hallways, waiting areas, and/or similar environments.

2. UTHSC IT Resources are categorized according to the highest categorization of the information/data stored, processed, or transmitted with the IT Resource.
3. 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 GP-001.04-Information Security Violations for the individual violating the policy.

Servers and Server Rooms

1. Servers are required to be protected by backup and off-site data storage.
2. Data owners/custodians and system owner/custodians are responsible for maintaining the physical security of these devices.
3. Servers shall be located in a room specifically designed for housing server computers and ancillary equipment and secured commensurate with the categorization of the information.
4. Servers and systems that process information with a classification rating of 3 in any area, or that are deemed critical for the operation of UTHSC must be housed in a totally enclosed facility (server room) designed and designated for housing server computers and associated ancillary equipment. The server room will meet the following standards:
    a. Access:
        i. Entry to a server room shall be restricted to authorized personnel having responsibility for installing or maintaining the assets in the server room. Others requiring access shall be escorted and supervised by authorized personnel.
        ii. All entry points affording access to server rooms shall be locked at all times.

iii. Access to server rooms shall be restricted by key, code, or electronic card. An auditable process for issuing keys, codes, and/or cards shall be documented.
iv. Access codes, if used, shall be changed every 6 months.
v. Server rooms shall be continuously monitored by surveillance equipment.

b. Usage:

i. New or refurbished server rooms shall not be shared with electrical service or unrelated services.
ii. Server rooms shall not be used for storage.
iii. Server rooms shall not be used as a "pass-through" to another room.
iv. Provisions for staff performing functions related to server room operations may be located in the Server Room.

c. Physical safeguards:

i. Server rooms will be constructed to meet University of Tennessee facilities standards.
ii. An uninterruptable power source (UPS) with built-in surge suppression must be installed with sufficient duration to switch over to alternative power in case of a power failure.
iii. Emergency power off switches must be installed.
iv. Automated emergency lighting must be installed.
v. A fire detection and suppression system must be installed and maintained.
vi. Server room temperatures and humidity shall be controlled at all times within levels specified by dedicated climate-control equipment separate from the building climate-control equipment.
vii. Water sensors shall be installed in appropriate locations to ensure detection of water intrusion from broken water pipes or other sources of water leakage.
viii. All detection and monitoring systems shall be tested and maintained on a regular basis as recommended by the manufacturer, and the occurrence of the tests documented. Fire

suppression must be tested in compliance with State Fire Marshall requirements and in a manner that does not disrupt operations. All detection and monitoring devices shall alert the appropriate personnel.

ix. UPS systems shall be tested and maintained on a schedule recommended by the manufacturer, and the occurrence of the tests documented.

x. There shall be no eating, drinking, or use of tobacco products allowed in server rooms at any time.

d. Maintenance Records:

i. Documentation of all repairs and modifications to physical components related to security (e.g. doors, hardware, locks, etc.) shall be maintained by the operator of the facility and retained for a period of six years.

End-User IT Resource

1. To prevent unauthorized access, tampering, and/or theft of UTHSC IT Resources, UTHSC workforce members must secure their work area whenever they are not available to monitor the area.
    a. If leaving their device, users will lock the device by whatever means available for the operating system, i.e. using Ctrl+Alt+Delete or Windows+L for Windows devices.
    b. Devices will auto-lock after an inactivity period of ten (10) minutes.
2. End-user UTHSC IT Resources must include physical access controls that limit physical access and protect the equipment when on-site, off-site, at home, or while in transit from one location to another.
    a. The IT Resource must be placed out of view or access of unauthorized individuals.

3. Display devices, i.e. monitors, in public areas need to be equipped with privacy safeguards or located so that unauthorized individuals cannot easily observe displayed information.
4. Physical security controls in clinical facilities must limit physical access to electronic information systems containing Personal Health Information (ePHI).
5. Physical security controls must be implemented based on the classification of data and the risks associated with unauthorized access. In addition, some regulations and contractual obligations with which UTHSC must comply have mandated physical security requirements.

Storage Devices and Media

1. Media will be classified according to the highest data classification stored on the media.
2. Any information with a classification rating of 3 in any area received on media, as defined in the policy scope, shall be handled in one of the following ways:
    a. Stored in a secure storage facility meeting the security requirements commensurate with the categorization of the information (GP-002-Data & System Classification).
    b. Copied to a secured server that stores information per the section above titled Servers & Server Rooms.
    c. Destroyed per CS-001-Device Life Cycle Security.
3. All media containing information with a classification rating of 3 in any area shall be sanitized according to CS-001-Device Life Cycle Security before transferring custody of the media outside of the Unit for re-use or disposal.
4. University, State of Tennessee, and federal records-retention requirements must be met prior to destruction of information or transfer of custody of media for purposes of disposal.

Telecom Rooms

1. Network communications equipment will be installed in communications closets specifically designed and designated as such.
    a. Access:
        i. Communication closets shall be locked at all times.

ii. Entry to a communications closet shall be restricted to personnel having responsibility for installing or maintaining the equipment in, or the safety of, the communications closet. Others requiring access shall be escorted and supervised by authorized personnel.
iii. Access to communications closets shall be restricted by key, code, or electronic card. An auditable process for issuing keys, codes, and/or cards shall be documented.
iv. Access codes, if used, shall be changed every 6 months.

b. Usage:
   i. Telecom rooms shall not be shared with electrical service or unrelated services.
   ii. If not feasible to avoid sharing of current communications closets, communications equipment shall be housed in a locked box appropriate to the purpose or segregated by fencing. Appropriate access controls shall be used.
   iii. Telecom rooms shall not be used for storage.
   iv. Telecom rooms shall be entered from a main corridor and not blocked by any other room.

c. Physical safeguards:
   i. Telecom rooms will be constructed to meet University of Tennessee telecommunication standards.
   ii. Doors should not have intake grills. If necessary for ventilation, grills shall be installed so that they cannot be removed from the outside of the door.
   iii. All detection and monitoring systems shall be tested on a regular basis as recommended by the manufacturer, and the occurrence of the tests documented. Fire suppression must be tested in compliance with State Fire Marshal requirements and in a manner that does not disrupt operations. All detection and monitoring devices shall alert the appropriate personnel.
   iv. An uninterruptible power source (UPS) with built-in surge protection shall be installed.
   v. UPS systems shall be tested on a schedule recommended by the

manufacturer and the occurrence of the tests documented.

vi. A backup plan shall exist in case of an air conditioning failure for those closets that are air-conditioned. All new constructed telecom rooms shall have a split system air conditioner and shall be monitored on the campus BAS system.

vii. There shall be no eating, drinking, or use of tobacco products allowed in the communications closets at any time.

d. Maintenance Records:

i. Documentation of all repairs and modifications to physical components related to security (e.g. doors, hardware, locks, etc.) shall be maintained by the operator of the facility and retained for a period of six years.

2. The following guidelines are suggested in addition to the above standards:

a. Communications closets should not have windows.

b. Water detectors and related infrastructure should be placed in the closet.

c. There should be no external signs making the Communications closets identifiable.

Exceptions

1. Exceptions to this Standard should be requested using the process outlined in GP-001.02 Security Exceptions and Exemptions to ITS Standards and Practices.

References

1. GP-002-Data & System Classification
2. GP-001.02 Security Exceptions and Exemptions to ITS Standards and Practices.
3. GP-001.04-Information Security Violations