THE UNIVERSITY OF TENNESSEE HEALTH SCIENCE CENTER

UT Health Science Center: PE-001.08-Physical Security End-User IT Recourse	
Version 4	**Effective Date: 03/17/2016**

Responsible Office: Office of Cybersecurity	Last Review: 03/24/2021 Next Review: 03/24/2023
Contact: Chris Madeksho	Phone: 901.448.1579 Email: mmadeksh@uthsc.edu

Purpose

To establish the minimum physical security requirements as well as responsibility for end-user UTHSC Information Technology (IT) Resources and related facilities/work areas.

Scope

This Practice applies to all UTHSC Information Technology (IT) Resources, end-users, and work areas.

Definitions

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.

UTHSC Workforce: employees, volunteers, trainees, and other persons whose conduct, in the performance of work for a covered entity or business associate, is under the direct control of such covered entity or business associate, whether or not they are paid by the covered entity or business associate.

Responsibilities

UTHSC User is responsible for adhering to this practice and the security controls set forth in it.

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

Practice

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

References

1. PE-001-Physical Security
2. GP-001.02 Security Exceptions and Exemptions to ITS Standards and Practices.