THE UNIVERSITY OF TENNESSEE
HEALTH SCIENCE CENTER

UT Health Science Center: PS-001-Personnel Security	
Version 6	Effective Date: 03/17/2018

Responsible Office: Office of Cybersecurity	Last Review: 07/27/2023 Next Review: 07/27/2025
Contact: Chris Madeksho	Phone: 901.448.1579 Email: mmadeksh@uthsc.edu

Purpose

To ensure that UTHSC Information Technology (IT) Resources are protected from the adverse actions of personnel.

This standard is also designed to meet compliance requirements for data regulated by federal or state law. This includes, but 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 Standard applies to all employees, contractors, members, users, and third parties who access, use, or support UTHSC Information Technology Resources, regardless of physical location.

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.

Insider Threat – The threat to an organization that comes from people within the organization, such as employees, former employees, contractors, or business associates, who have inside information concerning the organization's security practices, data, and computer systems.

Responsibilities

Office of Cybersecurity is responsible for the daily monitoring of specific systems, i.e. firewalls, endpoint detection and response (EDR) application, data loss prevention (DLP) tools, email environment, and others, to track activity in the UTHSC environment.

System owners or delegates are responsible for maintaining an inventory of individuals who have access to their systems and at what level of authorization, i.e. admin or privileged access.
UTHSC Human Resources is responsible for the policies and procedures used in onboarding and termination due to non-compliance.

Standard

1. UTHSC shall take actions to ensure that UTHSC IT Resources are protected from adverse actions of employees, contractors, members, users, and third parties who access, use, or support UTHSC IT Resources, regardless of physical location, unless an exception is granted.
2. For new employees, contractors, interns, members, friends, students, or volunteers (aka users):
   a. Roles and responsibilities within the UTHSC Information Security Program are defined, documented, and communicated.
   b. If appropriate, a Confidentiality Agreement shall be signed before access is granted to UTHSC data or information with a level 3 classification rating per GP-002-Data & System Classification.
   c. Appropriate training for the individual is made available in a timely fashion.
3. Reassignment of employment or role:
   a. All University security/system-related information and property pertaining to the previous assignment are retrieved.
   b. All access and credentials to UTHSC IT Resources are reviewed and terminated, changed, or granted as appropriate for the reassignment.
   c. Terminate/revoke any credentials associated with the individual pertaining to the previous assignment.
   d. If appropriate, a Confidentiality Agreement shall be signed before access is granted to UTHSC data or information with a level 3 classification rating.
   e. Roles and responsibilities within the UTHSC Information Security Program are defined, documented, and communicated.
   f. Appropriate training for the individual is made available in a timely fashion.
4. Separation of employment or role:
   a. Retrieve all pertinent University security/system-related information and property.
   b. Disable access to UTHSC IT Resources no longer required upon separation.
   c. Terminate/revoke appropriate credentials associated with the individual.

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.
6. Non-compliance with UTHSC policies is addressed appropriately as outlined in UTSA Human Resources Policy HR0525.

References

1. GP-001.02 Security Exceptions and Exemptions to ITS Standards and Practices
2. GP-002-Data & System Classification
3. UTSA Human Resources Policy HR0525