THE UNIVERSITY OF TENNESSEE HEALTH SCIENCE CENTER

UT Health Science Center: PS-001-Personnel Security	
Version 5	**Effective Date: 03/17/2018**

Responsible Office: Office of Cybersecurity	Last Review: 09/29/2022 Next Review: 09/29/2024
Contact: Chris Madeksho	Phone: 901.448.1579 Email: mmadeksh@uthsc.edu

Purpose

To ensure that UTHSC IT Resources are protected from the adverse actions of personnel.

Scope

This Standard applies to all employees, contractors, members, users, and third parties who access, use or support UTHSC IT 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.

Responsibilities

System owners 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.
2. For new employees, contractors, interns, members, friends, students, or volunteers (aka users):
   a. Verify that background checks are completed and documented before access to UTHSC IT Resources is granted.
   b. Roles and responsibilities within the UTHSC Information Security Program

are defined, documented, and communicated.

c. If appropriate, a Confidentiality Agreement shall be signed before access is granted to UTHSC data or information with a classification rating of 3 in any area.
d. 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 is 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 classification rating of 3 in any area.
   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.

Non-compliance with information security policies is addressed appropriately as outlined in HR0525 - Disciplinary Action

References

1. IT0124 - Risk Assessment
2. GP-002-Data & System Classification
3. HR0525 - Disciplinary Action