UT Health San Antonio

INSTITUTIONAL HANDBOOK OF OPERATING POLICIES

5.8.17 Information Security Training and Awareness Policy

Chapter 5 - Information Technology	Original Effective Date: June 2003
Section: 5.8 Information Security	Date Last Reviewed: February 2023
Responsible Entity: Chief Information Security Officer	Date Last Revised: May 2018

I. Purpose

To define required Information Security training.

II. Scope

This policy applies to all current and former faculty, staff, students, residents, healthcare providers, researchers, contractors, or any other third party entities who have direct or indirect access to Information Resources created, held or maintained by UT Health San Antonio or any controlled affiliate, including, but not limited to its clinics, hospitals, and research operations.

III. Policy

All Users (including, but not limited to, faculty, staff, students, residents, temporary employees, volunteers, contractors, third-parties, guests and other affiliated users) with credentials (provisioned user ID and password) to Information Resources must receive information security training as defined for their role and responsibilities by the Chief Information Security Officer.

A. The Chief Information Security Officer shall ensure that security training is delivered and tracked. Initial and recurring training:

1. should, at minimum, identify User responsibilities, common threats, regulatory and institutional requirements regarding the acceptable use and security of Information Resources, proper handling of Confidential Data, behaviors that may increase and reduce risk and incident notification; and

2. is to be administered in accordance with the following schedule:

a. Each new, temporary, contract, assigned, or engaged employee or worker must complete initial training within 30 days after the date that such a person is hired or otherwise engaged or assigned to perform such work; and

b. Recurring training on topics based on responsibility and access to Information Resources shall take place at least annually.

B. Users with privileged or special access (e.g., Administrator or Super-User Accounts) or with responsibilities to perform technical support (including, but not limited to, Help Desk and Desktop Support staff and IT Partners) must receive on a regular basis appropriate security technical training equivalent to current industry standards for security administrators and technology support users.

C. Information Resource Owners and Custodians shall receive periodic training on risk assessment procedures and responsibilities to implement security configuration controls as defined by UT Health San Antonio policies and standards.

D. Information security training provided to contractors or third-parties by their own organizations may satisfy the requirements of this policy if deemed substantially similar to UT Health San Antonio's standards by the Chief Information Security Officer and evidence of training is provided to UT Health San Antonio when requested.

E. All Users must acknowledge they have read and understood UT Health San Antonio's Information Security Policies including the "Information Resources Acceptable Use and Security Policy" as stated in the Handbook of Operating Policies (HOP), policy 5.8.10, at time of hire, assignment or engagement, and recurring on an annual basis.

IV. Definitions

There are no defined terms used in this Policy.

V. Related References

UT System (UTS) Policy
UTS 165 Information Resources Use and Security, Standard 18: Security Training

VI. Review and Approval History

A. The approving authority of this policy is the University Executive Committee.

B. The review frequency cycle is set for three years following the last review date, a time period that is not mandated by regulatory, accreditation, or other authority.

Effective Date	Action Taken	Approved By	Date Approved
06/2003	Policy Origination		
05/2018	Policy Revision		
02/2023	Policy Review/Discretionary Edits		