

Chapter 5	Information Management & Services	Effective:	June 2003
Section 5.8	Information Security	Revised:	May 2018
Policy 5.8.17	Information Security Training and Awareness Policy	Responsibility:	Chief Information Security Officer

INFORMATION SECURITY TRAINING AND AWARENESS POLICY

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.

1. The Chief Information Security Officer shall ensure that security training is delivered and tracked. Initial and recurring training:
 - a. 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
 - b. is to be administered in accordance with the following schedule:
 - i. Each new, temporary, contract, assigned, or engaged employee or worker must complete initial training within 30 days after the data that such a person is hired or otherwise engaged or assigned to perform such work; and
 - ii. Recurring training on topics based on responsibility and access to Information Resources shall take place at least annually.
2. 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 Technical Support Representatives (TSRs)) must receive on a regular basis appropriate security technical training equivalent to current industry standards for security administrators and technology support users.

UT HEALTH SAN ANTONIO HANDBOOK OF OPERATING PROCEDURES

Chapter 5	Information Management & Services	Effective:	June 2003
Section 5.8	Information Security	Revised:	May 2018
Policy 5.8.17	Information Security Training and Awareness Policy	Responsibility:	Chief Information Security Officer

-
3. 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.
 4. 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.
 5. 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 Procedures* (HOP), [Section 5.8.10](#), at time of hire, assignment or engagement, and recurring on an annual basis.

Reference

- U.T. System Policy 165 Standard 18
-