5.8.26 Information Security Risk Management

Chapter 5 - Information Technology	Original Effective Date: December 2005
Section: 5.8 Information Security	Date Last Reviewed: February 2023
Responsible Entity: Chief Information Security Officer	Date Last Revised: May 2018

I. Purpose

Assessment of risks that may impact the integrity, confidentiality and availability of UT Health San Antonio's Information Resources must be conducted on a regular basis. The objective of this policy is to determine areas of vulnerability, to initiate appropriate remediation, to increase awareness, and to communicate shared responsibility at all levels of the organization.

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

A. UT Health San Antonio (UTHSA) shall maintain an accurate inventory of Information Resources and identify Owners.

B. Information Resource Owners

For Information Resources under the Owner's authority, Owners must:

1. in consultation with the Chief Information Security Officer, define, approve, and document acceptable levels of risk and risk mitigation strategies; and
2. conduct and document Risk Assessments to determine risk and the inherent impact that could result from their unauthorized access, use, disclosure, disruption, modification, or destruction.
3. The timing of Risk Assessments shall be:

a. annually for all mission critical information resources and Information Resources containing confidential data; and

b. at periodic time intervals to be defined by the Information Resource Owner in consultation with the Chief Information Security Officer for non-mission critical information resources and Information Resources not containing confidential data.

C. Information Resource Custodians

Custodians of mission critical information resources must implement approved risk mitigation strategies and adhere to Information Security policies and procedures to manage risk levels for information resources under their responsibility.

D. Chief Information Security Officer

The Chief Information Security Officer shall:

1. ensure that annual Information Security Risk Assessments are performed and documented on each mission critical information resources and Information Resources containing confidential data;
2. execute assessments of third-party service providers;
3. ensure Information Security Risk Assessments as required by U.T. System policy, and state and federal law and regulations are performed and documented;
4. define minimum security configuration controls to mitigate critical and high risks;
5. execute vulnerability and security configuration scans. Document and communicate critical and high vulnerabilities and risk to Information Resource Owners and Custodians; and
6. assist with the Information Resource Owner's and Custodian's development and execution of remediation plans.

E. Third-Party or Vendors

A third-party risk assessment is required in the following situations:

1. when purchasing services that result in exchange of UTHSA data; or
2. hosting of UTHSA Information Resources with a vendor or other organization; or
3. when purchasing systems or software, whether it is to be hosted on UTHSA's premise or at a vendor's facility, if confidential data will be stored within or processed by the system or software.

F. U.T. System Risk Assessment Framework

Information Security Risk Assessments that are to be aggregated for systemwide reporting to the U.T. System Executive Compliance Committee and/or the U.T.

System Board of Regents shall be conducted using a risk management framework and process defined by U.T. System Office of Information Security and shall be coordinated at the institutional level by the Chief Information Security Officer.

G. Risk Acceptance

Decisions relating to acceptance of risk must be documented and are to be made by:

1. Information Resource Owner, in consultation with the Chief Information Security Officer or designee, for resources having a Residual Risk of Low or Moderate; and
2. Chief Administrative Officer, or designee, considering recommendations of the Owner and Chief Information Security Officer, for resources having a Residual Risk of High.

IV. Definitions

There are no defined terms used in this Policy.

V. Related References

U.T. System (UTS) Policy
UTS 165 Information Resources Use and Security, Standard 10: Risk Management

HIPAA Security
45 CFR 164.308(a)(1)(ii)(A)
45 CFR 164.306(a)

VI. Review and Approval History

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

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

Effective Date	Action Taken	Approved By	Date Approved
12/2005	Policy Origination		
05/2018	Policy Revision		
02/2023	Policy Review/Discretionary Edit		