Chapter 5	Information Management & Services	Effective:	December 2005
Section 5.8	Information Security	Revised:	October 2016
Policy 5.8.26	**Information Security Risk Management**	Responsibility:	Chief Information Security Officer

INFORMATION SECURITY RISK MANAGEMENT

Overview

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.

Policy

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

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.

    a. The timing of Risk Assessments shall be:

        i. annually for all Mission Critical Information Resources and Information Resources containing Confidential Data; and

        ii. 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.

    b. The risk assessment shall, at a minimum, document:

        i. the type and value of the Information Resource;

ii. the potential threats, both internal and external, or vulnerabilities of the Information Resource;

iii. the likelihood of those threats or exploit of vulnerabilities occurring; and

iv. the impact to UT Health San Antonio if the Information Resource is breached or its availability restricted.

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.

Chief Information Security Officer. The Chief Information Security Officer shall:

1. Ensure that annual Information Security Risk Assessments are performed and documented by each Owner of Mission Critical Information Resources or Information Resources containing Confidential Data;

2. Ensure Information Security Risk Assessments of Third-Parties are performed and documented;

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. Perform additional security efforts when minimum security standards have not been established or documented;

5. Define minimum security controls to mitigate assessed risk;

6. Initiate vulnerability scans and tests of security configurations and controls;

7. Request documentation pertaining to an Information Resource Owner's risk management efforts;

8. Direct and/or actively participate in risk management efforts; and

9. Assist with the development and execution of remediation plans.

Principal Investigators. Principal Investigators (PI's) must perform reviews, in collaboration with the Chief Information Security Officer, of the implementation of required security controls (e.g., control objectives, controls, policies, processes, and procedures for information security) for sponsored projects under their authority. Assessments for sponsored projects must be performed annually based on risk.

Third-Party or Vendors. A third-party risk assessment is required in the following situations:

1. When purchasing services that result in exchange of UT Health San Antonio data; or

2. Hosting of UT Health San Antonio Information Resources with a vendor or other organization; or

3. When purchasing systems or software, whether it is to be hosted on UT Health San Antonio's premise or at a vendor's facility, if Confidential Data will be stored within or processed by the system or software.

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

1. The Information Resource Owner, in consultation with the Chief Information Security Officer or designee, for resources having a Residual Risk of Low or Moderate;

2. The Chief Administrative Officer, or designee, considering recommendations of the Owner and Chief Information Security Officer, for resources having a Residual Risk of High.

This policy applies to all Information Resources owned, leased, operated, or under the custodial care of UT Health San Antonio.

Chapter 5	Information Management & Services	Effective:	December 2005
Section 5.8	Information Security	Revised:	October 2016
Policy 5.8.26	**Information Security Risk Management**	Responsibility:	Chief Information Security Officer

Authority

Violations of this policy are subject to disciplinary action as described in the HOP, Section 2.1.2, "*Handbook of Operating Procedures*".

References

- U.T. System Policy 165 Standard 10
- HIPAA Security Rule 164.308 (a)(1)ii(A)
- HIPAA Security Rule 164.306 (a)