5.8.1 Information Security Program

Chapter 5 - Information Technology	Original Effective Date: June 2002
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 the Information Security Program and related responsibilities.

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. Policy

1. UT Health San Antonio must establish and maintain a Security Program that includes appropriate protections based on risk, for all Information Resources including outsourced resources, owned, leased, or under the custodianship of any governing body or department, operating unit, or employee of the institution.
2. The Information Security Program must include and document the following:
    a. annual risk assessment;
    b. current inventory of institution-owned or managed computing devices deployed throughout the institution and mission critical applications and applications containing confidential data;
    c. strategies to address identified risks to mission critical information resources and confidential data;
    d. annual action plan, training plan and monitoring plan; and
    e. metrics and reports that accurately describe the state of vulnerability, threat and risk to the University.

B. Responsibilities and Accountability

1. UT Health San Antonio shall have designated and documented roles and responsibilities to ensure the availability, confidentiality and integrity of information resources.
2. The UT Health San Antonio President shall:
    a. ensure the institution's compliance with this policy and associated standards;
    b. designate an individual to serve as the Chief Information Security Officer (CISO) with authority to implement, enforce and monitor information security policies and associated standards for the entire institution;
    c. budget sufficient resources to fund ongoing information security remediation, implementation and compliance activities (e.g., staffing, training, tools and monitoring activities) that reduce compliance risk to acceptable levels;
    d. approve the UT Health San Antonio Information Security Program, and
    e. ensure appropriate corrective and disciplinary action is taken in the event of noncompliance.
3. The Information Resources Manager (IRM) shall:
    a. implement security controls in accordance with the UT Health San Antonio Information Security Program, and
    b. review and approve or disallow the purchase or deployment of new decentralized information technology (IT), information systems or services (e.g., electronic mail/web/file servers, file/system backup, storage, etc) that duplicate services provided by the UT Health San Antonio centralized IT department.
4. The Chief Information Security Officer (CISO) is the individual responsible for the UT Health San Antonio Information Security Program and shall:
    a. work in partnership with the institution's user community, constituency groups, and leadership to establish effective and secure processes and information systems and to promote information security as a core institutional value;
    b. provide information security oversight for all centralized and decentralized IT information resources;
    c. develop and maintain a current and comprehensive information security program that includes assessment of IT risks, corrective action plans, training plans, monitoring plans and specific risk mitigation strategies to be used by owners and custodians of information resources to manage identified risks and threats;
    d. develop institutional policies, standards, procedures and/or guidelines to ensure that the protection of information resources is considered during the

development or purchase of new information resources and services used in the planning or design, implementation and support of information resources;

e. develop or adopt a data classification standard that conforms or maps to UT System Policy 165 (UTS165), Standard 9;

f. coordinate risk assessments required by UT System to be reported to the UT System Executive Compliance Committee or Board of Regents, and ensure that information security risk assessments are performed and documented in accordance with risk assessment policies and standards and any state and federal regulations;

g. collaborate with the UT Health San Antonio Internal Audit department on information technology audits and remediation of identified risks;

h. ensure that each owner of mission critical information resources has designated an Information Security Administrator (ISA);

i. establish an institutional Information Security Working Group composed of ISAs and convene meetings at least quarterly;

j. approve and document exceptions to specific elements of the Information Security program, policies or standards and include such exceptions in an annual report to the President;

k. establish reporting requirements, metrics and timelines, and monitor effectiveness of security strategies implemented in both centralized and decentralized IT;

l. perform at a minimum, an annual vulnerability assessment of information resources maintained in both centralized and decentralized IT and track implementation of any remediation required as a result of the assessment;

m. ensure that an annual external network penetration test is performed and track implementation of risk remediation;

n. establish, communicate and monitor implementation of hardened security configuration requirements and guidelines including the use of appropriate security software such as anti-malware, firewall, configuration management, and other security related software on computing devices owned, leased or under the custody of any department operating unit, employee or other individual providing services to UT Health San Antonio;

o. ensure computing devices are administered by appropriately trained staff and in accordance with the UT Health San Antonio Policies, Standards and Procedures;

p. review the security requirements, specifications, and third-party risk assessments of any new computer applications or services that receive, maintain, create and/or share confidential data;

q. approve security requirements for the purchase of information technology hardware, software and services, and third-parties accessing or hosting UT Health San Antonio systems, applications, data or computing hardware;

r. ensure all faculty, staff and students, including all individuals accessing, using, holding or managing information resources on behalf of UT Health San Antonio, receive periodic information security training appropriate to their role and responsibility, including information security awareness training as part of each employee's initial and annually distributed compliance training;

s. communicate instances of noncompliance to appropriate administrative officers for corrective, restorative, and/or disciplinary action;

t. investigate security incidents and inform the President, and Executive Committee of incidents posing significant risk to individuals, the institution or other organizations;

u. report significant information security incidents, as defined by the UT System Security Incident Reporting Requirements, to the UT System CISO and Texas Department of Information Resources (DIR);

v. participate in the UT System CISO Council meetings, workgroups and related activities;

w. report to the UT System CISO in accordance with program reporting guidance and metrics;

x. provide updates to the Executive Committee regarding information security risks and threats, and

y. provide a report, at least annually, to the President with copies to the Chief Information Officer, Chief Compliance Officer and the UT System CISO on the status and effectiveness of information resource security controls for UT Health San Antonio in accordance with reporting instructions provided by the UT System CISO.

5. For information resources and data under their authority, Information Resource Owners, in collaboration with the CISO, shall:

a. grant or approve access to information systems and data;

b. control and monitor access to data based on data sensitivity and risk;

c. classify data based on the UT Health San Antonio data classification policies and standards;

d. conduct risk assessments that identify the information resources under their authority and the level of risk associated with the information resources and the vulnerabilities, if any, to the UT Health San Antonio computing environment;

e. define, recommend, and document acceptable risk levels for the information resources and risk mitigation strategies;

f. document and justify, in collaboration with the CISO, any exceptions to specific program requirements due to extenuating circumstances with the Information Resource Owner's area of responsibility;

g. ensure that data is securely backed up in accordance with risk management decisions;

h. ensure that data is maintained in accordance with the applicable UT Health San Antonio records retention schedule and procedures;

i. provide documented permission and justification for any user who is to store confidential University data on a portable computing device or a non-University owned computing device;

j. ensure that high risk computing devices and confidential data are encrypted in accordance with requirements specified in the UT Health San Antonio policies and standards;

k. ensure that information resources under their authority are administered by qualified Information Resource Custodians;

l. ensure that a risk assessment is performed prior to purchases of any software that has not been previously assessed by the institution for use under similar circumstances;

m. ensure that a third-party risk assessment is performed prior to purchase of vendor services that involve hosting or accessing University data; and

n. ensure that contracts involving products or services that impact information resources contain information security language appropriate to the risk.

6. Information Resource Custodians shall:

a. implement approved risk mitigation strategies and adhere to Information Security Policies, Standards and Procedures to manage risk levels for information resources under their care;

b. implement monitoring controls for detecting and reporting incidents;

c. control and monitor access to information resources under the Information Resource Custodian's care based on sensitivity and risk;

d. implement and adhere to approved institutional change management processes to ensure secure, reliable and stable operations;

e. encrypt high risk computing devices and confidential data in accordance with requirements specified in the UT Health San Antonio policies and standards;

f. report security incidents to the CISO in accordance with UT Health San Antonio policies and standards and provide the CISO with immediate assistance in investigating the incident;

g. assist Information Resource Owners in performing information security risk assessments;

h. provide appropriate technical training to employees providing technology and security administration, help-desk or other technical support of information resources under their responsibility; and

i. ensure technical staff under their authority are qualified to perform their assigned duties.

7. UT Health San Antonio departments with designated responsibility for account management shall manage accounts in accordance with Institutional Policy, Standards and Procedures, UT System policies and Regents' Rules and state and federal laws.

8. All users accessing, creating, using or holding information resources and data shall:

a. comply with the UT Health San Antonio Information Security policies and standards. Users who fail to comply are subject to disciplinary action in accordance with UT Health San Antonio policies; and

b. all Users who are UT Health San Antonio employees, including student employees, or who are otherwise serving as an agent or working on behalf of the institution, must formally acknowledge and comply with the institution's "Information Resources Acceptable Use and Security Policy" as stated in the Handbook of Operating Policies (HOP), Policy 5.8.10. Information Resources Acceptable Use and Security Policy.

IV. Definitions

There are no defined terms used in this Policy.

V. Related References

UT System (UTS) Policy
UTS 165 Standard 1 Information Resources Use and Security Responsibilities and Accountability

Texas Administrative Code
Texas Administrative Code 202 Subchapter A Rule 202.1 - Applicable Terms and Technologies for Information Security Standards

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
06/2002	Policy Origination		
05/2018	Policy Revision		
02/2023	Policy Review/Discretionary Edits		