UT Health San Antonio

INSTITUTIONAL HANDBOOK OF OPERATING POLICIES

5.8.5 Information Security Incident Management

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: October 2016

I. Purpose

To establish Incident Management Procedures to ensure that each security incident is reported, documented and resolved in a manner that meets legal requirements and restores operations quickly.

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. Incident Response

A Computer Incident Response Team (CIRT) shall be established consisting of selected UT Health San Antonio staff delegated with the responsibility to security incidents and investigation of potential misuse of Information Resources.

1. Any computing device that is detected to have a vulnerability that is actively being exploited or confirmed to have been breached must be disconnected from the UT Health San Antonio network.
2. Any computing device that is exhibiting suspicious activity or evidence of misuse must be disconnected from the UT Health San Antonio network.
3. The CIRT shall create and document an Incident Response Plan that describes procedures for:
   a. formally identifying, classifying, and reporting security incidents;
   b. responding to security incidents;

c. assessing potential damage of security incidents;

d. gathering and preserving physical and electronic evidence;

e. assigning responsibility for gathering, maintaining and reporting detailed information regarding security incidents; for actions taken to remediate; and for documentation of a management action plan to prevent a recurrence;

f. notifying appropriate UT Health San Antonio and U.T. System officials, affected residents of Texas, Data Owners, federal and State agencies and consumer reporting agencies as required by applicable state and federal law and U.T. System policy;

g. determining and adhering to timing requirements for incident disclosure and notification; and

h. determining and adhering to an appropriate medium to provide notice based on incident significance, number of individuals adversely impacts, University policy, applicable federal and State law and regulations, and any contractual obligations with third-party organizations.

B. Reporting

Information Security incidents must be reported in a timely manner and as required by UT Health San Antonio, U.T. System Policy, Standards and Procedures and state and federal law and regulations.

1. All UT Health San Antonio employees must promptly report unauthorized or inappropriate disclosure of Confidential Data in digital, paper, or any other format.
2. Information Resource Owners, Custodians and any supervisor or manager who becomes aware of a security incident is to report the incident to the Chief Information Security Officer (CISO).
3. An incident that involves personal safety, lost or stolen University computing devices (computers, laptops, servers, smartphones, tablets, etc.) must be reported to University Police. Users are also required to report security incidents to their assigned departmental IT Partner who must immediately forward incident information to the Chief Information Security Officer.
4. The Chief Information Security Officer must report significant security incidents, as defined by the U.T. System Security Incident Reporting Requirements, and unauthorized disclosure of University data to the U.T. System CISO.

C. Monitoring

The Chief Information Security Officer in consultation with Information Resource Owners and Custodians must implement monitoring controls and procedures for detecting, reporting, and investigating incidents.

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 12: Security Incident Management

HIPAA Security Rule 164.308 (a)(6)(ii)

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		
10/2016	Reviewed/Revised		
02/2023	Reviewed/Discretionary Edit		