Chapter 5	Information Management & Services	Effective:	June 2002
Section 5.8	Information Security	Revised:	October 2016
Policy 5.8.5	**Information Security Incident Management**	Responsibility:	Chief Information Security Officer

INFORMATION SECURITY INCIDENT MANAGEMENT

Policy

UT Health San Antonio shall adopt 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.

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.

- 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.
- Any computing device that is exhibiting suspicious activity or evidence of misuse must be disconnected from the UT Health San Antonio network.
- 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

Chapter 5	Information Management & Services	Effective:	June 2002
Section 5.8	Information Security	Revised:	October 2016
Policy 5.8.5	**Information Security Incident Management**	Responsibility:	Chief Information Security Officer

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.

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.

- All UT Health San Antonio employees must promptly report unauthorized or inappropriate disclosure of Confidential Data in digital, paper, or any other format.

- 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).

- 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 Technical Support Representative (TSR) who must immediately forward incident information to the Chief Information Security Officer.

- 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.

Chapter 5	Information Management & Services	Effective:	June 2002
Section 5.8	Information Security	Revised:	October 2016
Policy 5.8.5	**Information Security Incident Management**	Responsibility:	Chief Information Security Officer

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.

References

- U.T. System Policy 165 Standard 12
- HIPAA Security Rule 164.308 (a)(6)(ii)