

HEALTH SCIENCE CENTER HANDBOOK OF OPERATING PROCEDURES

Chapter 2	General Policies and Procedures	Effective:	April 2000
Section 2.2	Information Management	Revised:	June 2002
Policy 2.2.2	Information Security	Responsibility:	Vice President and Chief Information Officer

INFORMATION SECURITY

Policy

Based on *Texas Administrative Code* (TAC), [Section 202](#), it is the policy of the Health Science Center that:

1. Information resources residing in the Health Science Center are strategic and vital assets belonging to the people of Texas. These assets must be available and protected commensurate with the value of the assets. Measures shall be taken to protect these assets:

- a. against accidental or unauthorized access;
- b. disclosure; and,
- c. modification or destruction.

Measures shall also be taken to assure:

- a. the availability;
- b. integrity;
- c. utility;
- d. authenticity; and,
- e. confidentiality of information.

Access to state information resources must be appropriately managed.

2. The President is responsible for the protection of the resources.
3. All individuals are accountable for their actions relating to information resources. Information resources shall be used only for intended purposes as defined by the Health Science Center and consistent with applicable laws.

HEALTH SCIENCE CENTER HANDBOOK OF OPERATING PROCEDURES

Chapter 2	General Policies and Procedures	Effective:	April 2000
Section 2.2	Information Management	Revised:	June 2002
Policy 2.2.2	Information Security	Responsibility:	Vice President and Chief Information Officer

-
4. Risks to information resources must be managed. The expense of security safeguards must be commensurate with the value of the assets being protected.
 5. The integrity of data, its source, its destination, and processes applied to it must be assured. Changes to data must be made only in authorized and acceptable ways.
 6. Information resources must be available when needed. Continuity of information resources supporting critical governmental services must be ensured in the event of a disaster or business disruption.
 7. Security requirements shall be identified, documented, and addressed in all phases of development or acquisition of information resources.
 8. The Health Science Center must ensure adequate controls and separation of duties for tasks that are susceptible to fraudulent or other unauthorized activity.

Information Security Function

In accordance with The University of Texas System policy [UTS165](#), the President maintains ultimate responsibility for security and risk management programs to protect information resources. Procedural responsibility has been delegated to the Vice President and Chief Information Officer, as The University of Texas Health Science Center at San Antonio's Information Resources Manager (IRM). Implementation consists of an Information Security "function" headed by the Chief Information Security Officer. The Information Security function reports directly to the Vice President and Chief Information Officer.

The Information Security function is responsible for directing policy and procedures designed to protect information resources through:

1. identification of security vulnerabilities;
2. identification of confidential [defined in TAC 202], critical and sensitive information resources;
3. development and maintenance of a risk management program;

HEALTH SCIENCE CENTER HANDBOOK OF OPERATING PROCEDURES

Chapter 2	General Policies and Procedures	Effective:	April 2000
Section 2.2	Information Management	Revised:	June 2002
Policy 2.2.2	Information Security	Responsibility:	Vice President and Chief Information Officer

-
4. development and maintenance of contingency plans for the service resumption of information resources;
 5. development and maintenance of an adequate security awareness program; and
 6. development and maintenance of mechanism to investigate suspected security incidents and reported misuse of information resources.

Information Security Policy development is supported by the Information Security Council (ISC), a subcommittee of the Computing Resources Committee (CRC). As a standing Health Science Center committee, the CRC serves as the vehicle to present security policies to the Executive Committee for institutional approval and commitment.
