

HEALTH SCIENCE CENTER HANDBOOK OF OPERATING PROCEDURES

Chapter 5	Information Management & Services	Effective:	June 2002
Section 5.8	Information Security	Revised:	May 2011
Policy 5.8.6	Computer Incident Response Policy	Responsibility:	Chief Information Security Officer

COMPUTER INCIDENT RESPONSE POLICY

Policy

Based on *Texas Administrative Code*, 1 TAC 202, it is the policy of the Health Science Center that:

1. A “Computer Incident Response Team” (CIRT) shall exist consisting of selected Health Science Center staff members delegated with the responsibility of responding to:
 - a. Information security threats and incidents, and
 - b. Potential misuse of information technology resources.
2. Executive sponsorship of the CIRT is vested in the Vice President and Chief Information Officer (CIO). The President has delegated operational responsibility for the protection of information resources to the CIO who shall approve CIRT membership as recommended by the Health Science Center Information Security Council.
3. Computer incident response procedures shall be developed and maintained by the Information Security Council and submitted for approval to the CIO. This plan defines the CIRT organization and details computer incident responses procedures.
4. The CIRT organization shall include an “Incident Response Management Team” composed of senior Information Management Services management as recommended by the Information Security Council. Any member of the “Incident Response Management Team” may activate the CIRT and may also act as the CIRT leader for the duration of a computer incident.
5. Any computer that is confirmed to have been penetrated and/or is attempting to penetrate/infect other computers in the Health Science Center domain or computers elsewhere on the Internet shall be disconnected from the network. In addition, any computer that is exhibiting suspicious network activity or evidence of misuse of resources may be disconnected from the network.

HEALTH SCIENCE CENTER HANDBOOK OF OPERATING PROCEDURES

Chapter 5	Information Management & Services	Effective:	June 2002
Section 5.8	Information Security	Revised:	May 2011
Policy 5.8.6	Computer Incident Response Policy	Responsibility:	Chief Information Security Officer

-
6. In the performance of incident response duties, the CIRT shall recommend policy and procedure changes to the Information Security function. See the *Handbook of Operating Procedures* (HOP), [Section 2.2.2](#), "Information Security"; that is, the CIRT shall identify security vulnerabilities and/or preventive measures. The purpose of such recommendations is to minimize future vulnerabilities.

 7. This policy is in accordance with the policy stated in the HOP, [Section 2.2.2](#), "Information Security".
-