



Handbook of Operating Procedures

Section: 8.9.3
Originally Approved: 03/10/00
Last Amended: 03/22/02

INFORMATION SECURITY INCIDENT HANDLING POLICY

A. Purpose

To provide policy and procedures for expeditious reporting and response to information security incidents at The University of Texas - Pan American.

B. Authority and Requirements

University of Texas System Guidelines BPM 53 and the Texas Department of Information Resources (DIR) "Information Security and Risk Management Policy Standards and Guidelines" as published in the Texas Administrative Code 1 TAC 201.13(b) and as authorized by the Information Resources Management Act (Vernon's Ann. Civ. St. Article 4413(32j)).

C. Scope

This policy applies to all users of UTPA computing resources, including, university administrators, faculty, staff, students, and all others authorized to use such resources through their association with The University. This policy applies to all methods of accessing these resources including, but not limited to, campus network connections in academic units, administrative offices, academic laboratories, The University Library, and student dormitories, and remote network connections via dial-up, telnet, internet, and other access means.

D. Definition

An Information Security Incident is the unauthorized use of a computer or information system, or the use of a computer or information system in a violation of laws or pertinent policies. Examples of information security incidents include, but are not limited to: unauthorized account use, password stealing or cracking attempts, virus or Trojan horse program placement, computer or network system intrusion attempts.

E. Statement of Policy

1. Each user of UTPA computing and information resources has a responsibility to report incidents which constitute an information resources security incident or violation of The University of Texas System policies and the laws of the State of Texas and the federal government.
2. All information security incidents will be reported to the University's Information Security Officer as soon as an incident comes to the attention of a university employee or other person charged with responsibility for information resources within the scope of this policy. Information security incidents involving student owned and operated servers



Handbook of Operating Procedures

Section: 8.9.3
Originally Approved: 03/10/00
Last Amended: 03/22/02

INFORMATION SECURITY INCIDENT HANDLING POLICY

connected to university resources via campus network, university library, SLIP, or other method must be reported in the same manner as incidents involving university owned and operated servers.

3. The Information Security Officer will oversee information security incident handling in cooperation with designated Technical Managers, University Police Criminal Investigative Division, Dean of Students (only where students are involved), and designated University Managers and support staff. The University's Information Security Officer will formalize and forward reports of information resources security incidents through organizational channels to executive management in accordance with University of Texas System BPM 53.
4. Failure to comply with this policy will result in disciplinary action as is appropriate under the circumstances in compliance with University or University of Texas System policies.

F. Responsibilities

Information security incident handling and response duties are outlined below:

- a. Information Security Officer (ISO): The Computer Center Information Security Manager oversees information security activities within The University and provides consultation for incident investigations. The ISO must be notified of all information security incidents in order to maintain accurate incident data and to insure consistent information is communicated internally and externally.
- b. Technical Manager: The Computer Center Assistant Director for Systems guides security incident responses for mainframe systems, campus network systems, and Administrative departments within the University. The Director of Technology Resources guides security incident responses for centrally managed student/academic facilities, and Academic departments within the University.
- c. System Owner: The owner of an information resource will be called by the ISO or the responsible Technical Manager for information regarding incidents affecting University information resources.
- d. System Managers/Administrators: Persons assigned by the system owner to configure, maintain, and support an affected University system or server not managed by Computer Center or Technology Resources support staff may be called to assist information security incident response as required.



Handbook of Operating Procedures

Section: 8.9.3
Originally Approved: 03/10/00
Last Amended: 03/22/02

INFORMATION SECURITY INCIDENT HANDLING POLICY

- e. Student Server Owners: Students who own and operate an affected server connected to university resources may be called to assist information security incident response as required.
- f. Dean of Students: The Dean of Students will be notified of all information security incidents involving enrolled students' use of University information resources.
- g. University Police: The University Police Criminal Investigative Division (CID) may be called to investigate criminal incidents involving information security related events.

G. Reporting Procedures

Any person who suspects, receives notification of, or discovers an information security incident must contact the Information Security Officer and/or responsible Technical Manager prior to taking action as described in the call list which is maintained and published by the Information Security Officer.

H. Review

This policy should be reviewed every five years by the University's designated Information Resources Manager with the advice of campus technology management and committees and councils concerned with technology issues.