



Handbook of Operating Procedures

Section: 8.9.1
Originally Approved: 03/23/1995
Last Amended: 06/30/2009
Last Reviewed: 06/30/2009
Page: 1 of 6

POLICY FOR THE USE AND PROTECTION OF INFORMATION RESOURCES

A. Purpose

[Title 1 Texas Administrative Code \(TAC\) 202.70 \(1\)](#) states that it is the policy of the state of Texas that Information Resources residing in the various agencies of State government are strategic and vital assets belonging to the people of Texas. Assets of The University of Texas-Pan American must be available and protected commensurate with their value and must be administered in conformance with federal and state law and The University of Texas System Board of Regents' *Rules and Regulations*. This policy provides requirements and guidelines to establish accountability and prudent and acceptable practices regarding the use and safeguarding of University Information Resources; protect the privacy of personally identifiable information contained in the Data that constitutes part of its Information Resources; ensure compliance with applicable policies and state and federal laws regarding the management and security of Information Resources; and, educate individual Users with respect to the responsibilities associated with use of University Information Resources.

This policy serves as the foundation for the University's information security program, and provides the UTPA Information Security Office the authority to implement policies, practice standards, and/or procedures necessary to implement a successful information security program in compliance with [UTS165 Information Resources Use and Security Policy](#).

NOTE: A companion document to this policy, The University of Texas-Pan American Information Resources Security Operations Manual <http://infosecurity.utpa.edu/manual> which is incorporated by reference into this policy details security practices and requirements relating to each policy topic.

These two documents comprise the policy and procedures foundation for the University's computer security program.

B. Persons Affected

This policy equally applies to all individuals that have, or may require, access to the University's Information Resources and those with responsibility for maintaining the Information Resources at the University.

C. Policy

The policy of The University of Texas-Pan American is to:

1. Protect Information Resources based on risk against accidental or unauthorized access,



Handbook of Operating Procedures

Section: 8.9.1
Originally Approved: 03/23/1995
Last Amended: 06/30/2009
Last Reviewed: 06/30/2009
Page: 2 of 6

POLICY FOR THE USE AND PROTECTION OF INFORMATION RESOURCES

disclosure, modification or destruction and assure the availability, confidentiality, and integrity of data;

2. Appropriately reduce the collection, use or disclosure of all social security numbers contained in any medium, including paper records;
3. Apply appropriate physical and technical safeguards to the conduct University business while meeting the guidelines of applicable state laws, federal laws and System guidelines.
4. Comply with applicable state and federal laws and U. T. System rules governing information resources.

D. Definitions

The most current definitions are located at:

1. <http://infosecurity.utpa.edu/glossary>;
2. UTPA Information Resource Security Operations Manual <http://infosecurity.utpa.edu/manual>; and
3. UT System Administration Policy UTS-165 <http://www.utsystem.edu/policy/policies/uts165.html>

E. Responsibilities

1. The President shall be responsible for the following:
 - a. The University's compliance with this policy;
 - b. Budget sufficient resources to fund ongoing and continuous information security remediation, implementation, and compliance activities that reduce compliance risk to an acceptably low level;
 - c. Approve the UTPA Information Security Program, or designate someone to provide approval; and
 - d. Ensure that appropriate corrective and disciplinary action is taken in the event of non-compliance.
2. The Vice President for Information Technology is charged with oversight of



Handbook of Operating Procedures

Section: 8.9.1
Originally Approved: 03/23/1995
Last Amended: 06/30/2009
Last Reviewed: 06/30/2009
Page: 3 of 6

POLICY FOR THE USE AND PROTECTION OF INFORMATION RESOURCES

information technology for UTPA, shall serve in the functional role of Information Resources Manager (IRM) as defined by the state and will have authority for the entire University.

3. The President shall designate an individual other than the Information Resources Manager (IRM) to serve as the University Chief Information Security Officer (CISO) who shall serve in the capacity as required by state law and with authority for all of UTPA. The responsibilities of the University CISO shall include the following:
 - a. Assure information security for all information resources including centrally maintained and all distributed systems and computer equipment;
 - b. Develop an institutional Information Security Compliance Program. This program shall include institutional action plans, training plans, and monitoring plans;
 - c. Conduct and document an information security assessment annually in accordance with [1 TAC 202.72](#) that identifies Mission Critical Information Resources in the central and decentralized areas;
 - d. Ensure an annual information security risk assessment is performed (using the process defined above) by each Owner of Mission Critical Information Resources;
 - e. Require each Owner of Mission Critical Information Resources to designate an Information Security Administrator (ISA);
 - f. Establish an Institutional Information Security Working Group composed of ISAs and hold meetings at least quarterly;
 - g. Document and maintain an up to date Institutional Information Security Program. The program shall identify specific mitigation strategies to be used by each Owner of Mission Critical Information Resources to manage identified risk;
 - h. Establish reporting guidance, metrics, and timelines and monitor effectiveness of security strategies in both central and decentralized operations;
 - i. Communicate instances of non-compliance to appropriate administrative officers for corrective, restorative and/or disciplinary action; and
 - j. Report quarterly to the U. T. System CISO the current status of the information security risk assessment and Information Security Program, including any significant incidents, situations of non-compliance, barriers to program execution, and planned



Handbook of Operating Procedures

Section: 8.9.1
Originally Approved: 03/23/1995
Last Amended: 06/30/2009
Last Reviewed: 06/30/2009
Page: 4 of 6

POLICY FOR THE USE AND PROTECTION OF INFORMATION RESOURCES

- remedies. The report is to include a certification that best efforts have been made to ensure appropriate strategies are in place to manage identified risks, that the strategies are being applied consistently over time, and that all security incidents have been reported.
4. Owners of Mission Critical Information Resources at the University shall designate an individual to serve as an Information Security Administrator (ISA) to implement information security policies and procedures and for reporting incidents to the University CISO. The responsibilities of the ISA shall include the following:
 - a. Implement and comply with all UTPA information technology policies and procedures relating to assigned systems;
 - b. Report general computing and security incidents to the University CISO;
 - c. Assist, as a member of the ISA Working Group, the University CISO in developing, implementing, and monitoring the Information Security Program.
 - d. Establish reporting guidance, metrics, and timelines for the University CISO to monitor effectiveness of security strategies in both the centralized and decentralized operations; and
 - e. Report at least annually to the University CISO about the status and effectiveness of information resources security controls.
 5. Department Heads and Principal Investigators (PI) at the University shall be responsible for compliance with this policy as it relates to Non-Research and Research Data respectively under their control including when holding subcontracts for projects in which the prime award is at another institution or agency.
 6. The Offices of Institutional Compliance and Internal Audit at the University shall provide high-level monitoring of the Information Security Compliance Program through inspections and verifications of reported information and periodic audits respectively.
 7. All Users must comply with this policy. Users who fail to comply are subject to disciplinary action in accordance with subsection F.2.

F. Procedures

1. Information Resources Acceptable and Secure Use



Handbook of Operating Procedures

Section: 8.9.1
Originally Approved: 03/23/1995
Last Amended: 06/30/2009
Last Reviewed: 06/30/2009
Page: 5 of 6

POLICY FOR THE USE AND PROTECTION OF INFORMATION RESOURCES

All individuals granted access to technology resources of the University must acknowledge the rules of use of these resources annually. Each individual is responsible for exercising good judgment regarding the reasonableness and security of their behaviors and their use of Information Resources.

As a convenience to individuals, limited incidental personal use of Information Resources is permitted. Incidental use of Information Resources must not result in direct cost to the University or expose the University to unnecessary risks.

2. Disciplinary Actions

Pursuant to [Title 1 TAC Section 202](#) and to ensure compliance with this policy and state laws and regulations related to the use and security of Information Resources, the University has the authority and responsibility to monitor Information Resources. If there is a reasonable basis to believe that this policy or state laws or regulations regarding the use and security of Information Resources have been violated, the contents of User files may be accessed for purposes of investigation with the written approval of a University executive officer.

Violation of this policy may result in disciplinary action for employees, including but not limited to termination in accordance with the *Handbook of Operating Procedures*. For contractors and consultants this may include a termination of the work engagement. For interns and volunteers, this may include dismissal. Any student who violates this policy will be referred to student judicial services at the student's home campus. Additionally, individuals are subject to possible civil and criminal prosecution.

3. All Other Procedures

For all other procedures and mechanisms outlined in this policy consult the Information Resources Security Operations Manual <http://infosecurity.utpa.edu/manual>. Compliance with these procedures will be enforced as outlined in the Disciplinary Actions outlined in this policy.

G. Review

The Divisional Head for this policy is the Vice President for Information Technology and this policy shall be reviewed every two years or sooner if necessary by the following Stakeholders:

1. Chief Information Security Officer Senior Reviewer
2. Assistant Chief Information Security Officer



Handbook of Operating Procedures

Section: 8.9.1
Originally Approved: 03/23/1995
Last Amended: 06/30/2009
Last Reviewed: 06/30/2009
Page: 6 of 6

POLICY FOR THE USE AND PROTECTION OF INFORMATION RESOURCES

3. Associate Vice President for IT Support
4. Associate Vice President for Data Center
5. Technology Assessment Officer
6. Institutional Information Security Administrator Working Group
7. Faculty Senate Chair
8. Registrar
9. Staff Senate Chair
10. Council of Deans
11. Student Government Association President