TEXAS A&M UNIVERSITY
SAN ANTONIO

# 29.01.03.00.01 INFORMATION SECURITY

Approved: August, 2013
Revised: April, 2019
Revised: August, 2019
Next Scheduled Review: August, 2024

## PROCEDURE STATEMENT

Texas A&M University-San Antonio (A&M-San Antonio) will monitor access to and security of information and information resources as required by Texas A&M University System (System) Regulation 29.01.03 *Information Security*.

## REASON FOR PROCEDURE

Owners, Custodians, and Users shall comply with the Texas Administrative Code, Title 1 (TAC 202), Gramm Leach Bliley Act of 1999 (GLB Act), Family Educational Rights and Privacy Act of 1974 (FERPA) and the Health Insurance Portability and Accountability Act of 1996 (HIPAA).

This Procedure applies to all information resources owned, stored, processed, transmitted, managed or maintained by A&M-San Antonio.

A&M-San Antonio electronic information resources are vital academic and administrative assets which require appropriate safeguards. Computer systems, networks, and data are vulnerable to a variety of threats. These threats have the potential to compromise the integrity, availability, and confidentiality of the information. Effective security management programs must be employed to eliminate or mitigate the risks posed by potential threats to the University's information resources. Measures shall be taken to protect these resources against unauthorized access, disclosure, modification, or destruction, whether accidental or deliberate.

A&M-San Antonio, as a state university, is required to comply with the Texas Administrative Code, which assigns responsibility for protection of information resources to the University President. For the purposes of this procedure, the authority and responsibility regarding the university's compliance with the Texas Administrative Code on Information Security Standards has been delegated by the President to the Chief Information Officer (CIO).

## OFFICIAL PROCEDURE

1. RESPONSIBILITIES

1.1 The Information Security Officer (ISO) has been designated as the individual responsible for administering the provisions of this procedure and the TAC Information Security Standards.

1.2 The ISO shall ensure that University-wide electronic information resources security risk management plans are completed, and reviewed annually. The head or director of each department shall ensure that a departmental electronic information resources security risk management plan is in effect.

1.3 For systems that are not centrally managed by Information Technology Services (ITS), the head or director of a department or the owner of the information resource shall be responsible for ensuring that an appropriate security program is in effect and that compliance with this procedure and TAC Standards is maintained for information systems owned and operationally supported by the department. Information resource owners will be required to sign an acknowledgement of the awareness of this procedure.

1.4 Information resource owners must report any violations of TAC 202 information security standards to the ISO, in writing, within 24 hours of the violation occurrence. Information resource owners are also required to report any compromises of information resources, such as loss or unauthorized access, to the ISO.

1.5 Operational responsibility for compliance with TAC Standards and University procedures may be delegated by the department head to the appropriate information system support personnel (e.g. System Administrators) within the department. These delegations must be communicated in writing to the ISO.

1.6 Mission critical or confidential information maintained on information resources must be afforded the appropriate safeguards stated in TAC 202 and A&M-San Antonio's standards. It is the responsibility of the information resource owner or user to ensure that adequate security measures are in place.

2 COMPLIANCE ASSESSMENT REPORTING

An administrative unit having ownership or custodial responsibility for electronic information systems shall ensure that on an annual basis, a risk assessment report is filed with the ISO, via System-approved risk management system. The report shall be filed by the data owner or designee. The ISO will manage this process.

3 STANDARDS

The ISO may issue binding and enforceable IT protocols in the form of documented standards. Any A&M-San Antonio user may propose new Standards, edits to existing Standards, or the deletion of existing Standards, by submitting such proposals in writing to the ISO. The ISO will present proposals to the CIO and ITS Managers. If a proposal is approved by a simple majority of the CIO and the IT Senior Staff, then the ISO will send the proposal to the CFO and all ITS employees, who will have 10 working days to respond. Any edits submitted during the 10-day response period will be accepted or rejected based on a simple majority vote of the CIO and IT Managers. At the end of the 10-day period the proposal will become official and will be posted on a website accessible to all University users. The ISO will review all ITS Standards at least annually.

## Related Statutes, Policies, or Requirements

System Regulation 29.01.03 *Electronic Information Services Access and Security*

Texas Administrative Code (TAC) 202 as amended or supplemented.

Gramm Leach Bliley Act (GLB Act)

Family Educational Rights and Privacy Act (FERPA)

Health Insurance Portability and Accountability Act (HIPAA)

## DEFINITIONS

**Confidential Information** - Information that is exempted from disclosure requirements under the provisions of applicable state or federal law, e.g., the Texas Public Information Act.

**Mission Critical Information** - Information that is defined by the University or information resource owner to be essential to the continued performance of the mission of the University or department. An event causing the unavailability of mission critical information would result in consequences such as significant financial loss, institutional embarrassment, non-compliance with regulations or legal obligations, or closure of the University or department.

**Information Security Officer (ISO)** - Responsible to the executive management for administering the information security functions within the agency. The University ISO is the University's internal and external point of contact for all information security matters.

**Information Resource Owner** - an entity responsible for:

- a business function; and
- determining access controls to information resources supporting that business function.

**User** - An individual or automated application or process that is authorized to the resource by the owner, in accordance with the owner's procedures and rules.

**Appropriate security assessment and awareness system** - Used to assess the security posture of information systems and measure compliance with the Information Security Standards. It also provides guides for creating a disaster recovery plan and performing a physical security check. Additionally, an information security training course and assessment is assigned to University staff on an annual basis.

## Contact Office

Business Affairs, Information Technology Services (210) 784-4357 (HELP)