Procedure Statement

This Procedure ensures that Texas A&M University-San Antonio (TAMU-SA) will effectively monitor access and security for information resources in accordance with System Regulation 29.01.03 Electronic Information Services Access and Security.

Reason for Procedure

This Procedure is required by System Regulation 29.01.03 Electronic Information Services Access and Security. It is the responsibility of owners, custodians, and users to comply with the Texas Administrative Code, Title 1 (TAC 202), Gramm Leach Billey 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).

Procedures and Responsibilities

1. GENERAL

1.1 This Procedure applies to all information resources owned, stored, processed, transmitted, managed or maintained by TAMU-SA.

1.2 TAMU-SA 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 appropriately 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.

1.3 TAMU-SA, as a state university, is required to comply with the Texas Administrative Code (TAC) on “Information Security Standards.” (See Texas Administrative Code Chapter 202) The Texas Administrative Code assigns responsibility for protection of informational 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 Information Resource Manager (IRM).

1.4 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.

1.5 The ISO shall ensure that University-wide electronic information resources security risk management plans are completed, at least on an annual basis. The head or director of a department shall ensure that a departmental electronic information resources security risk management plan is in effect on a regular basis.

1.6 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.

1.7 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 comprises of information resources such as loss or unauthorized access.

1.8 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 to the ISO.

1.9 Mission Critical or Confidential Information maintained on information resources must be afforded the appropriate safeguards stated in the TAC 202 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

2.1 An administrative unit having ownership or custodial responsibility for electronic information systems shall ensure that on an annual basis, a security assessment report is filed with the Information Security Officer (ISO), via the ISAAC reporting system. The report shall be filed by the data owner or designee. The reporting requirements of this subsection will become effective in the Fall Semester of 2012.
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.

ISAAC (Information Security Awareness Assessment and Compliance) - A web-based 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.

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

Information Technology Services – (210) 784-4357