University Procedure
Texas A&M University-Kingsville

29.01.03. K1.01 Security of Electronic Information Resources
Approved June 1, 2011
Revised June 19, 2013
Next Scheduled Review June 1, 2015

Procedure Statement

This procedure defines the responsibilities of various members of Texas A&M University-Kingsville management with respect to information security technology issues.

Reason for Procedure

The responsibilities of various members for the management and security of information technology services at Texas A&M University-Kingsville should be delineated.

Procedures and Responsibilities

---

1. GENERAL

1.1 Texas A&M University-Kingsville's 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 from both internal and external sources. These threats have the potential to compromise the integrity, availability, and confidentiality of the information.

1.2 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 Texas A&M University-Kingsville, as a state university, is required to comply with the Texas Administrative Code (TAC) on "Information Security Standards". The Texas Administrative Code assigns responsibility for protection of informational resources to the President. For the purposes of this rule, 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).

2. DEFINITIONS

2.1 Confidential Information - Information that is exempted from disclosure requirements under the provisions of the Texas Public Information Act or other applicable state or federal laws. Most student records as well as employee records are considered confidential information.

2.2 Critical Information - Information that is defined by Texas A&M University-Kingsville to be essential to its function(s) and would cause severe detrimental impact if the data/system were lost and unable to be restored in a timely fashion.

2.3 Owner - A person responsible for the function which is supported by the resource, the individual upon whom responsibility rests for carrying out the program that uses the resources. The owner is responsible for establishing the controls that provide the functional security. The owner of a collection of information is the person responsible for the business results of that system or the business use of the information.

2.4 Custodian - A person (or department) providing operational support for an information system and having responsibility for implementing owner-defined controls and access privileges.

2.5 User- The user of the data or record has the responsibility to use the resource only for the purpose specified by the owner; comply with controls established by the owner; and prevent disclosure of confidential or sensitive information.

3. RESPONSIBILITIES

3.1 The Information Security Officer (ISO) has been designated as the individual responsible for administering the Texas A&M University System (TAMUS) and Texas A&M University-Kingsville (TAMUK) polices rules and procedures, and the Texas Administrative Code (TAC) Information Security Standards.

3.2 The head or director of a department shall be responsible for ensuring that an appropriate security program is in effect and that compliance with this rule, other applicable TAMUS and TAMUK rules, and TAC Standards is maintained for information systems owned and operationally supported by the department.

3.3 The head or director of a department which provides operational support (custodian) for information systems owned by another TAMUK department shall have the responsibility for ensuring that an appropriate security program is in effect and that compliance with TAC Standards and other applicable rules and regulations is maintained for the supported information systems.

3.4 Operational responsibility for compliance with TAC Standards and other applicable rules and regulations may be delegated by the department head or director to the appropriate information system support personnel within the department.

3.5 Critical or Confidential Information maintained on an individual workstation or personal computer must be afforded the appropriate safeguards stated in the TAC Standards and other applicable rules and regulations. It is the responsibility of the operator, or owner, and/or departmental personnel responsible for that workstation or personal computer to insure that adequate security measures are in place.

4. COMPLIANCE ASSESSMENT REPORTING

4.1 Departments having ownership or custodial responsibility for electronic information systems will be subject to an annual security assessment performed by iTech. The risk assessment report is kept on file by iTech.

Related Statutes, Policies or Requirements

Texas A&M System Rule 29.01.03 Electronic Information Services Access and Security

Texas Administrative Code 202 as amended or supplemented

Contact Office

For interpretation or clarification, contact iTech, Information Security Officer, or Chief Information Officer, Texas A&M University-Kingsville