

Security of Electronic Information Resources

Approved: May 4, 2006
Reviewed: February 28, 2009
Next Scheduled Review: February 28, 2011



Procedures and Responsibilities

1. GENERAL

1.1 Tarleton State University'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. 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 Tarleton State University, 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 Executive Director of Information Resources (EDIR).

2. Definitions

2.1 Confidential Information - Information that is excepted 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 Mission Critical Information - Information that is defined by Tarleton State University or any division thereof (department, etc.), 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 a University function and for determining controls and access to electronic information resources supporting that University function.

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 has been designated as the individual responsible for administering the provisions of this rule and the 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 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 Tarleton State University department shall have the responsibility for ensuring that an appropriate security program is in effect and that compliance with TAC Standards is maintained for the supported information systems.

3.4 Operational responsibility for compliance with TAC Standards may be delegated by the department head or director to the appropriate information system support personnel (e.g. System Administrators) within the department.

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

4. INTERPRETATION OF POLICIES, REGULATIONS, AND RULES

4.1 The procedures determining the electronic security of University information resources are addressed in the following University Rules/SAPs.

Related Statutes, Policies, or Requirements

Supplements System Regulation 29.01.03

Contact Office

Responsible Office: Information Technology Services