SAP 29.01.03.T0.19 Security of Electronic Information Resources

Approved:	May 4, 2006
Revised	February 28, 2009
Revised	July 27, 2012
Reviewed:	May 21, 2014
Next Scheduled Review:	May 21, 2019

Procedure Statement

It is the responsibility of the information owner or designee to ensure that adequate security measures are in place and that an annual risk assessment is performed.

Reason for Procedure

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 standard administrative procedure (SAP), 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 and chief information officer (CIO) of Information Technology Services (ITS).

Procedures and Responsibilities

1.1 The information security officer has been designated as the individual responsible for administering the provisions of this SAP and the TAC Information Security Standards.

1.2 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 SAP and TAC Standards is maintained for information systems owned and operationally supported by the department.

1.3 The head or director of a department which provides operational support (custodian) for information systems owned by another Tarleton 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.

1.4 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.

1.5 Mission Critical or Confidential Information maintained on information resources such as servers, individual workstations, and portable devices must be afforded the appropriate safeguards stated in the TAC Standards and applicable university rules and standard administrative procedures. It is the responsibility of the information resource owner or designee to ensure that adequate security measures are in place.

1.6 The information owner, or their designee, is responsible for ensuring that the risk mitigation measures described in applicable university rules and SAPs are implemented. Based on risk management considerations and business functions, the information owner may determine that it would be appropriate to exclude certain risk mitigation measures. All exclusions must be in accordance with SAP *29.01.99.T1.27 Exclusions from Required Risk Mitigation Measures.*

Related Statutes, Policies, or Requirements

This SAP supersedes Rule 29.01.03.T1

Supplements System Policy 29.01 and System Regulation 29.01.03

TAC 202, Information Security Standards

Tarleton *SAP 29.01.99.T1.27, Exclusions from Required Risk Mitigation Measures* (not yet written)

Definitions

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.

Mission Critical Information – Information that is defined by Tarleton or any information owner 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. An event causing the unavailability of mission critical information would result in consequences such as significant financial loss, institutional embarrassment, failure to comply with regulations or legal obligations, or closure of the university or department.

Information Owner - A person with statutory or operational authority for specified information (e.g., supporting a specific business function) and responsibility for establishing the controls for its generation, collection, processing, access, dissemination, and disposal. The information owner may also be responsible for other information resources including personnel, equipment, and information technology that support the information owner's business function.

Custodian of an Information Resource - A person responsible for implementing owner-defined controls and access to an information resource. Custodians may include state employees, vendors, and any third party acting as an agent of, or otherwise on behalf of the state entity.

User of an Information Resource - An individual or automated application authorized to access an information resource in accordance with the information resource owner's defined controls and access rules for the purpose specified by the owner; complying with controls established by the owner; and preventing disclosure of confidential or sensitive information.

Information Resources (IR) - The procedures, equipment, and software that are designed, employed, operated, and maintained to collect, record, process, store, retrieve, display, and transmit information or data.

Contact Office

Information Technology Services
Executive Director and CIO of Information Technology Services
254-968-9395