

SAP 29.01.03.T0.01 Information Resources – Acceptable Use



Approved: May 4, 2006
Revised: February 28, 2012
Revised: July 1, 2014
Next Scheduled Review: July 1, 2019

Procedure Statement

Under the provisions of the Information Resources Management Act, information resources are strategic assets of the State of Texas that must be managed as valuable state resources. Tarleton State University (Tarleton) has developed rules and procedures that address acceptable use of information resources.

Reason for Procedure

This SAP provides a set of measures that will mitigate information security risks associated with acceptable use of university information resources. There may be other or additional measures that will provide appropriate mitigation of the risks. The assessment of potential risks and the application of appropriate mitigation measures will be determined by the information resource owner or their designee.

Procedures and Responsibilities

1. **APPLICABILITY** - This SAP applies to all university information resources.
2. The information resource owner or designee (e.g. custodian, user) is responsible for ensuring that the risk mitigation measures described in this SAP are implemented. In accordance with Texas Administrative Code 202 - Information Security Standards, an information resource owner may elect not to implement some or all of the risk mitigation measures provided in this SAP based on information security risk management decisions and business functions. Such risk management decisions must be documented and reported to the designated ISO.
3. The rules and procedures for determining acceptable use of university information resources are addressed as follows:

[SAP 29.01.03.T0.02 Account Management](#)
[SAP 29.01.03.T0.03 Administrator/Special Access](#)
[SAP 29.01.03.T0.04 Backup Recovery](#)
[SAP 29.01.03.T0.05 Email Use](#)
[SAP 29.01.03.T0.06 Intrusion Detection](#)
[SAP 29.01.03.T0.07 Malicious Code](#)
[SAP 29.01.03.T0.08 Network/Wireless Access](#)
[SAP 29.01.03.T0.09 Network Configuration](#)
[SAP 29.01.03.T0.10 Password Authentication](#)
[SAP 29.01.03.T0.11 Physical Access](#)
[SAP 29.01.03.T0.12 Privacy](#)
[SAP 29.01.03.T0.13 Security Awareness and Training](#)
[SAP 29.01.03.T0.14 Security Monitoring](#)
[SAP 29.01.03.T0.15 Server Hardening](#)
[SAP 29.01.03.T0.16 Vendor Access](#)
[SAP 29.01.03.T0.17 Use of Peer-to-Peer Sharing Software](#)
[SAP 29.01.03.T0.18 Portable Computing](#)
[Rule 29.01.03.T2 Incidental Computer Use](#)
[Rule 29.01.03.T3 Electronic Information Resources Complaints](#)

Related Statutes, Policies, or Requirements

[Texas Administrative Code 202 - Information Security Standards](#)
[Tarleton SAP 29.01.03.T0.19 Security of Electronic Information Resources](#)

Definitions

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.

Information Security Officer (ISO): responsible for administering the information security functions within Tarleton and reports to the information resources manager (IRM).

Contact Office

Information Technology Services
Executive Director and CIO of Information Technology Services
254.968-9395