

Procedure 29.01.03.T1.09 (Effective 5/4/2006)
(Supplements [Rule 29.01.03.T1](#))
Information Resources –Network Configuration

PROCEDURE:

1. GENERAL

The information resources network infrastructure in Stephenville, Texas is provided by Tarleton State University for tenants of University facilities. It is important that the infrastructure, which includes media, active electronics and supporting software, be able to meet current performance requirements while retaining the flexibility to allow emerging developments in high speed networking technology and enhanced user services. The purpose of the network configuration procedure is to establish the process for change of the network infrastructure.

Tarleton State University owns and is responsible for the University network infrastructure and will continue to manage further developments and enhancements to this infrastructure.

2. APPLICABILITY

This Standard Administrative Procedure (SAP) applies to all University network infrastructure information resources.

3. PURPOSE

The purpose of the implementation of this SAP is to provide a set of measures that will mitigate information security risks associated with network configuration. There may also 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 are to be determined by the information resource owner or their designee. In accordance with *Texas Administrative Code 202 - Information Security Standards*, each department and/or 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 Information Security Officer (ISO).

The intended audience is all network system administrators of University information resources.

4. DEFINITIONS

4.1 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.

4.2 Information Security Officer (ISO): responsible for administering the information security functions within Tarleton State University and reports to the Information Resources Manager (IRM).

5. PROCEDURES

5.1 All network connected equipment must be configured to a specification approved by Tarleton State University Information Resources.

5.2 All hardware connected to the Tarleton State University network is subject to its Information Resources management and monitoring standards.

5.3 Changes to the configurations of active network management devices must not be made without the approval of Information Resources.

5.4 The University network infrastructure supports a well-defined set of approved networking protocols. Any use of non-sanctioned protocols must be approved by Information Resources.

5.5 The network addresses for the supported protocols are allocated, registered and managed centrally by Texas A&M University and Tarleton State University Information Resources.

5.6 All connections of the network infrastructure to external third party networks is the responsibility of Tarleton State University Information Resources. This includes connections to external telephone networks.

5.7 Tarleton State University Information Resources firewalls must be installed and configured following the University Firewall Implementation Standard documentation.

5.8 The use of departmental firewalls is not permitted without the written authorization from Information Resources.

5.9 Users must not extend or re-transmit network services in any way. Devices such as routers, switches, hubs, or wireless access points cannot be installed on the Tarleton State University network without approval from Information Resources.

5.10 Users must not install network hardware or software that provides network services without Tarleton State University Information Resources approval.

5.11 Users are not permitted to alter network hardware in any way.

OFFICE OF RESPONSIBILITY: Department of Information Resources

CONTACT: Executive Director of Information Resources