Information Technology Services
Network Configuration

Approved: February 11, 2020

Contact for Interpretation: Chief Information Officer

Procedure Statement

The information resources network infrastructure is provided by Tarleton State University for use by Tarleton students, faculty and staff. 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. Tarleton owns and is responsible for the university network infrastructure.

Reason for Procedure

The purpose of the implementation of this standard operating procedure is to provide a set of measures that will mitigate information security risks associated with network configuration and establish the process for change of the network infrastructure. 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 procedure 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).

This procedure applies to all university network infrastructure information resources.

Procedures and Responsibilities

1. All network connected equipment must be configured to a specification approved by Tarleton Information Technology Services.

2. All hardware connected to the Tarleton network is subject to Information Technology Services management and monitoring standards.

3. Changes to the configurations of active network management devices must not be made without the approval of Information Technology Services.

4. The university network infrastructure supports a well-defined set of approved networking protocols. Information Technology Services must approve the use of any non-sanctioned protocols.

5. The network addresses for the supported protocols are allocated, registered and managed by Texas A&M University and Tarleton Information Technology Services.

6. All connections of the network infrastructure to external third party networks are the responsibility of Tarleton Information Technology Services. This includes connections to external telephone networks.

7. Tarleton Information Technology Services firewalls must be installed and configured following the University Firewall Implementation Standard documentation.

8. The use of departmental firewalls is not permitted without the written authorization from Information Technology Services.

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 network without approval from Information Technology Services.

10. Users must not install network hardware or software that provides network services without Tarleton Information Technology Services approval.

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

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).