

SAP 29.01.03.T0.08 Information Technology Services – Network/Wireless Access



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

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 electronic equipment (i.e., multiplexers, hubs, routers, etc.) 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.

Reason for Procedure

The purpose of this Standard Administrative Procedure (SAP) is to provide a set of measures that will mitigate information security risks associated with network access. This SAP applies to all university network information resources.

Procedures and Responsibilities

1. Network aggregation devices (e.g., hubs, switches, routers, wireless access points) shall not be connected to network infrastructure without prior approval by Information Technology Services.
2. Management of network addresses and name space may be delegated to system administrators. Users are permitted to use only those network addresses issued to them by their designated system administrator.

3. Network scans and network vulnerability scans of devices attached to the Tarleton network as well as the appropriate remediation are occasionally necessary to ensure the integrity of Tarleton computing systems. Network scans and network vulnerability scans may only be conducted by university employees designated by the organizational unit head responsible for the information resource.
4. Individuals controlling right-to-use for systems attached to the network infrastructure will ensure only authorized persons are granted access.
5. Allowing anonymous write capability to university systems or anonymously originating network traffic requires Information Technology Services permission.
6. Users shall not alter university-owned network hardware in any way.

Related Statutes, Policies, or Requirements

Supplements [SAP 29.01.03.T0.19 Security of Electronic Information Resources](#)

Definitions

1. **Anonymous write capability:** the ability of people to save (on Tarleton computers) information they create without their identity being known (to system administrators).
 2. **Anonymously originating network traffic:** causing a (Tarleton) computer system to send traffic via the network where the custodian/owner is not known.
 3. **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