

I.T. DIVISION
STANDARD ADMINISTRATIVE PROCEDURES

SAP No. 24.99.99.W1.01

Information Resources – Guidelines on Network Scanning

Approved: December 29, 2009

Last Revised: August 30, 2011

Next Scheduled Review: August 2012

Supplements [University Rule 24.99.99.W1](#)

1. General

Network scanning is frequently used in attempts to penetrate information resource security. To further responsible computing, these guidelines restrict network- scanning activity except in limited circumstances.

2. Applicability

This Standard Administrative Procedure (SAP) applies to all University information resources. The purpose of this Standard Administrative Procedure is to provide a set of measures that will mitigate information security risks associated with network use. There may also be other or additional measures that department heads or deans will provide to further mitigate risks. The assessment of potential risks and the application of appropriate mitigation measures are to be determined by the department heads and their identified information security administrators. 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 documented information security risk management decisions and business functions. Such risk management decisions must be documented and approved by the designated Information Security Officer (ISO).

The intended audience is all users of University information resources.

3. Definitions

- 3.1 Network scanning is the process of transmitting data through a network to elicit responses in order to determine configuration state about an information system.
- 3.2 Network vulnerability scanning is the process of network scanning to determine the presence of security vulnerabilities in an information system.

4. Guidelines

- 4.1 Network Services will, from time to time, conduct network scans and network vulnerability scans of devices attached to the West Texas A&M University network, including remote offices located in Amarillo. Information gathered will be used for network management, including notifying owners of vulnerabilities, determining incorrectly configured systems, validating firewall access requests, and gathering network census data.
- 4.2 Except as provided in 4.1, network scans or network vulnerability scans may only be conducted by the information security officer (ISO), network services personnel or third parties that have been authorized by the information resources manager (IRM).
- 4.3 Network scans and network vulnerability scans may not be conducted by students or student systems in the West Texas A&M University residence halls.

OFFICE OF RESPONSIBILITY: Information Technology

CONTACT: Chief Information Officer