29.01.99.E1.01 Information Resources – Guidelines on Network Scanning

Approved September 17, 2009
Revised June 5, 2013
Next Scheduled Review: June 5, 2016

Supplements TEES Rule 29.01.99.E1

Standard Administrative Procedure Statement
Network scanning is frequently used in an attempt to penetrate information resource security which furthers responsible computing.

Reason for Standard Administrative Procedure
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.

Procedures and Responsibilities

1. CONTROLS AND RESPONSIBILITIES

1.1 The TAMU Computing and Information Services (CIS) Network group will, from time to time, conduct network scans and network vulnerability scans of devices attached to the Texas A&M University network. 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.

1.2 The owner of the information resource may perform network and vulnerability scans as long as the network scanning traffic does not transit a router maintained by the CIS Network group.

1.3 Network scans and network vulnerability scans may only be conducted by agency employees designated by the division head responsible for the information resource.

1.4 Other exceptions to these guidelines may be authorized only by the Chief Information Officer.

Related Statutes, Policies, or Requirements
TAMU SAP 29.01.99.M1.01, Guidelines on Network Scanning
TEES Rule 29.01.99.E1, Security of Electronic Information Resources
Contact Office
Information Technology Services
(979) 847-8585