STANDARD ADMINISTRATIVE PROCEDURE

29.01.03.M1.01 Network Scanning and Vulnerability Assessments

Approved October 1, 2002
Revised March 7, 2007
Revised May 28, 2010
Revised February 10, 2012
Revised August 14, 2013
Next scheduled review: August 14, 2018

Statement and Reason for Standard Administrative Procedure

The purpose of this standard administrative procedure (SAP) is to mitigate the risks that vulnerabilities to Texas A&M University information resource systems may pose. This SAP seeks to ensure that vulnerabilities are adequately addressed and minimized; and, that guidelines are in place to restrict network scanning activity except in limited circumstances. Additionally, all operating systems for all information resource systems must undergo a regular vulnerability assessment as required by Texas Administrative Code, Title 1, Section 202.

To ensure that vulnerability assessments for University information resources are conducted, the Texas A&M IT security team may scan any operating system attached to the University network system at any time.

Definitions

CISO – Chief Information Security Officer

Network Scanning – the process of transmitting data through a network to elicit responses in order to determine the configuration state of an information system.

Network Vulnerability Assessments – assessing network scanning data to determine the presence of security vulnerabilities in the information system.

Official Procedure/ Responsibilities/ Process

1. APPLICABILITY

All Unit heads will ensure that all systems that connect to the University's information resources network undergo periodic vulnerability assessments of network systems, operating systems, and applications.

2. GUIDELINES

2.1 A vulnerability assessment may include assessment(s) of any of the following information resources:

- network(s)
- operating system(s)
- application(s)

2.2 A vulnerability assessment will be conducted by Texas A&M IT security team biennially (every two years) based on a risk analysis developed by the Office of the Chief Information Security Officer and at other times as needed by current threats.

2.3 The Texas A&M IT security team is authorized to conduct network scanning of devices attached to the University network. Information gathered from such scans will be used for network management which includes:

- notifying owners of vulnerabilities,
- determining incorrectly configured systems,
- validating firewall access requests, and
- gathering network census data.

2.4 Custodians of information resources found to be vulnerable in any way will be contacted concerning any identified risk(s). The custodian is responsible for ensuring that the identified risk(s) is mitigated in a timely manner.

2.5 If known vulnerabilities are not resolved, access for the affected information resource(s) may be disabled from the network by the Texas A&M IT security team.

2.6 Network scanning may only be conducted by University or Texas A&M System employees designated by the organizational unit head responsible for the information resource being scanned. Network scanning conducted by entities other than Texas A&M IT security team may not transit a router maintained by the Texas A&M IT security team without permission from Texas A&M security team.

2.7 Network scanning may not be conducted by student systems in the Residence Halls. Guidelines for appropriate scanning can be found at http://it.tamu.edu/Security/Security_Services/Network_Vulnerability_Scanning/Guidelines.php.

2.8 Exclusions from this SAP may be requested by submitting a request in accordance with SAP *29.01.03.M1.27 Exclusions from Required Risk Mitigation Measures*.

Related Statutes, Policies, or Requirements

1 Texas Administrative Code §202

System Policy *29.01 Information Resources*

University SAP *29.01.03.M0.01 Security of Electronic Information Resources*

University SAP *29.01.03.M1.27 Exclusions from Required Risk Mitigation Measures*

Contact Office

CONTACT: Office of the Chief Information Security Officer

OFFICE OF RESPONSIBILITY: Associate Vice President for Information Technology & Chief Information Officer