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 System Offices (SO) 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 202.75 (TAC).

To ensure that vulnerability assessments for SO information resources are conducted, the University Network and Information Security (NIS) team may scan any operating system attached to the SO network system at any time.

Definitions

SO ISO – System Office 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.

Networking and Information Security (NIS) - a unit within the TAMU Office of the Vice President and Associate Provost for Information Technology (VP APIT).

Official Rule/ Responsibilities/ Process

1. APPLICABILITY
The SO ISO will ensure that all systems that connect to the SO 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 NIS biennially (every two years) based on a risk analysis developed by the SO ISO and at other times as needed by current threats.

2.3 The NIS security team is authorized to conduct network scanning of devices attached to the SO 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
- 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.

2.6 Network scanning may only be conducted by University or SO employees designated by the organizational unit head responsible for the information resource being scanned.


2.8 Exclusions from this SAP may be requested by submitting a request in accordance with SAP 29.01.99.S1.27 Exclusions from Required Risk Mitigation Measures.
Related Statutes, Policies, or Requirements

1 Texas Administrative Code §202.75(7)(AA)

System Policy 29.01 Information Resources

SO Rule 29.01.99.S1 Security of Electronic Information Resources

SO SAP 29.01.99.S1.27 Exclusions from Required Risk Mitigation Measures

Contact Office

The Texas A&M University System Chief Information Officer can be contacted for interpretation or clarification.

OFFICE OF RESPONSIBILITY: The Texas A&M University System Chief Information Officer