Texas A&M Health Science Center Guidelines

29.01.99.Z1.04 Guideline: Vulnerability Assessment

Approved February 13, 2013

Supplements System Regulation 29.01 and TAMU SAP XX.XX.XX.MX.XX

Reason for the Guidelines

A vulnerability assessment is frequently used in attempts to penetrate information resource security. To further responsible computing, these guidelines restrict network scanning activity except in limited circumstances. This policy applies equally to all individuals who use any Texas A&M University Health Science Center (HSC) information resource.

1. Vulnerability Assessment Policy

1.1 The Office of Information Technology (OIT) will regularly conduct network vulnerability assessments of the HSC network. Information gathered will be used for network management, including notifying owners of vulnerabilities, determining incorrectly configured systems, and validating firewall access requests.

1.2 Network vulnerability assessments 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).

1.3 Network vulnerability assessments must be compliant with all applicable laws and policies including HSC privacy policies.

2. Violations

Violations of this policy may result in disciplinary action, which may include termination for employees and temporary workers; a termination of employment relations in the case of contractors or consultants; dismissal for interns and volunteers; or suspension or expulsion in the case of a student. Additionally, individuals are subject to loss of HSC information resources access privileges, civil, and criminal prosecution.

OFFICE OF RESPONSIBILITY:

Vice President for Finance and Administration