Texas A&M Health Science Center Guidelines

29.01.03.Z1.17 Guideline: Platform Management

Approved September 1, 2010
Revised February 13, 2013

Supplements System Regulation 29.01.03 and TAMU SAP 29.01.03.M1.20

Reason for the Guidelines

Servers are necessary to deliver data in a secure, reliable fashion. There must be assurance that data integrity, confidentiality and availability are maintained. One of the required steps to attain this assurance is to ensure that the servers are installed and maintained in a manner that prevents unauthorized access, unauthorized use, and disruptions in service. Additionally, desktop computing systems must be secured and maintained to prevent similar unauthorized use and access. This guideline applies to all individuals that are responsible for the installation of new information resources, the operations of existing information resources, and individuals charged with information resource security.

1. Platform Management

1.1 A server must not be connected to the Texas A&M University System Health Science Center (HSC) network until it is in an Office of Information Technology (OIT) accredited secure state and the network connection is approved by OIT.

1.2 Information required to harden a server is made available by software manufacturers, and must be implemented for OIT accreditation. Some of the general steps included in these server hardening procedures include:
   - Applying vendor supplied patches,
   - Removing unnecessary software, system services, and drivers,
   - Setting security parameters, file protections and enabling audit logging, and
   - Disabling or changing the password of default accounts.

1.3 OIT will monitor security issues, both internally and externally, and will manage the release of security patches.

1.4 OIT will test security patches, where practical, against OIT core resources before release.

1.5 OIT may make hardware resources available for testing security patches in the case of special applications.

1.6 Security patches must be implemented within the OIT specified timeframe.
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