29.01.03.Z1.11 Guideline: Network Configuration

Approved September 1, 2010
Revised February 13, 2013

Supplements System Regulation 29.01.03 and TAMU SAP 29.01.03.M1.13

Reason for the Guidelines

The Texas A&M University System Health Science Center (HSC) network infrastructure is provided as a central utility for all users of HSC information resources. It is important that the infrastructure, which includes cabling and the associated equipment such as routers and switches, continues to develop with sufficient flexibility to meet user demands while at the same time remaining capable of exploiting anticipated developments in high speed networking technology to allow the future provision of enhanced user services.

1. Official Guideline

1.1 HSC Office of Information Technology (OIT) owns and is responsible for the HSC network infrastructure and will continue to manage further developments and enhancements to this infrastructure.

1.2 To provide a consistent HSC network infrastructure capable of exploiting new networking developments, all cabling must be installed by HSC OIT or an approved contractor.

1.3 All network connected equipment must be configured to a specification approved by HSC OIT.

1.4 All hardware connected to the HSC network is subject to HSC OIT management and monitoring standards.

1.5 Changes to the configuration of active network management devices must not be made without the approval of HSC OIT.

1.6 The HSC network infrastructure supports a well-defined set of approved networking protocols. Any use of non-sanctioned protocols must be approved by HSC OIT.

1.7 The networking addresses for the supported protocols are allocated, registered and managed centrally by HSC OIT.

1.8 All connections of the network infrastructure to external third party networks are the responsibility of HSC OIT. This includes connections to external telephone networks.
1.9 HSC OIT firewalls must be installed and configured following the HSC Firewall Implementation Standard documentation.

1.10 The use of departmental firewalls is not permitted without the written authorization from HSC OIT.

1.11 Users must not extend or re-transmit network services in any way. This means you must not install a router, switch, hub, or wireless access point to the HSC network without HSC OIT approval.

1.12 Users must not install network hardware or software that provides network services without HSC OIT approval.

1.13 Users are not permitted to alter network hardware in any way.

2. Disciplinary Actions

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