

**THE TEXAS A&M UNIVERSITY SYSTEM
HEALTH SCIENCE CENTER INTERNAL POLICIES**

29.01.03.Z1.11 Network Configuration

Approved September 1, 2010

Supplements System Regulation 29.01.03

1. GENERAL

1.1 Introduction

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.

1.2 Audience

The HSC Network Configuration Policy applies equally to all individuals with access to any HSC information resource.

1.3 Ownership of Electronic Files

Electronic files created, sent, received, or stored on information resources owned, leased administered, or otherwise under the custody and control of the HSC are the property of the HSC.

1.4 Privacy

Electronic files created, sent, received, or stored on information resources owned, leased, administered, or otherwise under the custody and control of the HSC are not private and may be accessed by HSC information system employees at any time without knowledge of the information resources user or owner. Electronic file content may be accessed by appropriate personnel in accordance with the provisions and safeguards provided in the Texas Administrative Code 202, Information Security Standards.

1.5 Definitions

- **Information Resources (IR):** Any and all computer printouts, online display devices, magnetic storage media, and all computer-related activities involving any device capable of receiving email, browsing Web sites, or otherwise capable of receiving, storing, managing, or transmitting electronic data including, but not limited to, mainframes, servers, personal computers, notebook computers, hand-held computers, personal digital assistants (PDA), pagers, distributed processing systems, network attached and computer controlled medical and laboratory equipment (i.e. embedded technology), telecommunication resources, network environments, telephones, fax machines, printers and service bureaus. Additionally, it is the procedures, equipment, facilities, software, and data that are designed, built, operated, and maintained to create, collect, record, process, store, retrieve, display, and transmit information.
- **Information Resources Manager (IRM):** Responsible to the State of Texas for management of the institution's information resources. The designation of an institution information resources manager is intended to establish clear accountability for setting policy for information resources management activities, provide for greater coordination of the state institution's information activities, and ensure greater visibility of such activities within and between state agencies. The IRM has been given the authority and the accountability by the State of Texas to implement Security Policies, Procedures, Practice Standards, and Guidelines to protect the information resources of the institution. If an institution does not designate an IRM, the title defaults to the institution's President, and the President is responsible for adhering to the duties and requirements of an IRM.
- **Information Security Officer (ISO):** Responsible to executive management for administering the information security functions within the institution. The ISO is the institution's internal and external point of contact for all information security matters.
- **Office of Information Technology (OIT):** The name of the institution department responsible for computers, networking and data management.

2. NETWORK CONFIGURATION POLICY

- 2.1 HSC OIT owns and is responsible for the HSC network infrastructure and will continue to manage further developments and enhancements to this infrastructure.
- 2.2 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.

- 2.3 All network connected equipment must be configured to a specification approved by HSC OIT.
- 2.4 All hardware connected to the HSC network is subject to HSC OIT management and monitoring standards.
- 2.5 Changes to the configuration of active network management devices must not be made without the approval of HSC OIT.
- 2.6 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.
- 2.7 The networking addresses for the supported protocols are allocated, registered and managed centrally by HSC OIT.
- 2.8 All connections of the network infrastructure to external third party networks are the responsibility of HSC OIT. This includes connections to external telephone networks.
- 2.9 HSC OIT firewalls must be installed and configured following the HSC Firewall Implementation Standard documentation.
- 2.10 The use of departmental firewalls is not permitted without the written authorization from HSC OIT.
- 2.11 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.
- 2.12 Users must not install network hardware or software that provides network services without HSC OIT approval.
- 2.13 Users are not permitted to alter network hardware in any way.

3. 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 Information Technology and Chief Information Officer