

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

29.01.03.Z1.09 Internet

Approved September 1, 2010

Supplements System Regulation 29.01.03

1. GENERAL

1.1 Introduction

Under the provisions of the Texas Government Code Chapter 2054, Information Resources Management Act, information resources are strategic assets of the State of Texas that must be managed as valuable state resources. Thus this policy is established to achieve the following:

- To ensure compliance with applicable statutes, regulations, and mandates regarding the management of information resources.
- To establish prudent and acceptable practices regarding the use of the internet.

To educate individuals who may use the internet, the intranet, or both with respect to their responsibilities associated with such use.

1.2 Audience

The Texas A&M University System Health Science Center (HSC) Internet Use Policy applies equally to all individuals granted access to any HSC information resource with the capacity to access the internet, the intranet, or both.

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 the executive management for administering the information security function within the institution. The ISO is the institution's internal and external point of contact for all information security matters.
- **User:** An individual, automated application or process that is authorized to access the resource by the owner, in accordance with the owner's procedures and rules.
- **Internet:** A global system interconnecting computers and computer networks. The computers and networks are owned separately by a host of organizations, government agencies, companies, and colleges. The Internet is the present "information super highway."
- **Intranet:** A private network for communications and sharing of information that, like the Internet, is based on TCP/IP, but is accessible only to authorized

users within an organization. An organization's intranet is usually protected from external access by a firewall.

- **World Wide Web (Web):** A system of Internet hosts that supports documents formatted in HTML (HyperText Markup Language) which contain links to other documents (hyperlinks) and to audio, video, and graphic images. Users can access the Web with special applications called browsers, such as Netscape Navigator, and Microsoft Internet Explorer.
- **Vendor:** A person who supplies goods or a service to a governmental entity or another person directed by the entity. The term does not include a state agency or institution, except for Texas Correctional Industries. The term includes an officer or employee of a state agency or institution when acting in a private capacity to supply goods or a service.

2. INTERNET POLICY

- 2.1 Software for browsing the Internet is provided to authorized users for business and research use only.
- 2.2 All software used to access the Internet must be part of the HSC standard software suite or approved by the ISO. This software must incorporate all vendor provided security patches unless otherwise noted.
- 2.3 All files downloaded from the Internet must be scanned for viruses using the approved Office of Information Technology distributed software suite and current virus detection software.
- 2.4 All software used to access the Internet shall be configured to use the firewall http proxy.
- 2.5 All sites accessed must comply with the HSC Acceptable Use Policies.
- 2.6 All user activity on HSC information resources assets is subject to logging and review.
- 2.7 Content on all HSC Web sites must comply with the HSC Acceptable Use Policies.
- 2.8 No offensive or harassing material may be made available via HSC Web sites.
- 2.9 Non-business related purchases made over the internet are prohibited. Business related purchases are subject to HSC procurement rules.
- 2.10 No personal commercial advertising may be made available via HSC Web sites.

- 2.11 HSC internet access may not be used for personal gain or non-HSC personal solicitations.
- 2.12 No HSC data will be made available via HSC Web sites without ensuring that the material is available to only authorized individuals or groups.
- 2.13 All sensitive HSC material transmitted over external network must be encrypted.
- 2.14 Electronic files are subject to the same records retention rules that apply to other documents and must be retained in accordance with departmental records retention schedules.

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