

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

---

---

**29.01.99.Z1.01 Acceptable Use of Information Resources**

*Approved November 6, 2003*

*Revised October 7, 2009*

*Revised September 1, 2010*

**Supplements System Policy 29.01**

---

---

**1. GENERAL**

1.1 Introduction

Under the provisions of the 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 information resources.
- To educate individuals who may use information resources with respect to their responsibilities associated with such use.

1.2 Audience

The Texas A&M University System Health Science Center's (HSC) Acceptable Use of Information Resources policy applies equally to all individuals granted access privileges to any HSC information resources.

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, Title 1, Chapter 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 assistant (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 or automated application or process that is authorized access to the resource by the owner, in accordance with the owner's procedures and rules.

## **2. RESPONSIBILITY FOR USE OF INFORMATION RESOURCES**

- 2.1 Users must report any weaknesses in HSC computer security, any incidents of possible misuse or violation of this agreement to the proper authorities by contacting the appropriate management.
- 2.2 Users must not attempt to access any data or programs contained on HSC systems for which they do not have authorization or explicit consent.
- 2.3 Users must not divulge Dialup or Dial-back modem phone numbers to anyone.
- 2.4 Users must not share their HSC account(s), passwords, Personal Identification Numbers (PIN), Security Tokens (i.e. Smartcard), or similar information or devices used for identification and authorization purposes.
- 2.5 Users must not make unauthorized copies of copyrighted software.
- 2.6 Users must not use non-standard shareware or freeware software without HSC IRM approval unless it is on the HSC standard software list.
- 2.7 Users must not purposely engage in activity that may: harass, threaten or abuse others; degrade the performance of information resources; deprive an authorized HSC user access to a HSC resource; obtain extra resources beyond those allocated; circumvent HSC computer security measures.
- 2.8 Users must not download, install or run security programs or utilities that reveal or exploit weaknesses in the security of a system. HSC information resources must not be used for personal benefit.
- 2.9 Users must not intentionally access, create, store or transmit material which the HSC may deem to be offensive, indecent or obscene (other than in the course of academic research where this aspect of the research has the explicit approval of the HSC official processes for dealing with academic ethical issues).
- 2.10 Access to the Internet from a HSC owned, home based, computer must adhere to all the same policies that apply to use from within HSC facilities. Employees must not allow family members or other non-employees to access HSC computer systems.
- 2.11 Users must not otherwise engage in acts against the aims and purposes of the HSC as specified in its governing documents or in rules, regulations and procedures adopted from time to time.

### **3. INCIDENTAL USE**

As a convenience to the HSC user community, incidental use of information resources is permitted. The following restrictions apply:

- 3.1 Incidental personal use of electronic mail, Internet access, fax machines, printers, copiers, and so on, is restricted to HSC approved users; it does not extend to family members or other acquaintances.
- 3.2 Incidental use must not result in direct costs to the HSC.
- 3.3 Incidental use must not interfere with the normal performance of an employee's work duties.
- 3.4 No files or documents may be sent or received that may cause legal action against, or embarrassment to, the HSC.
- 3.5 Storage of personal email messages, voice messages, files and documents within the HSC's information resources must be nominal.
- 3.6 All messages, files and documents – including personal messages, files and documents – located on HSC information resources are owned by HSC, may be subject to open records requests, and may be accessed in accordance with this policy.

### **4. 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**