Texas A&M Health Science Center Guidelines

29.01.99.Z1.01 Guideline: Acceptable Use of Information Resources

Approved November 6, 2003
Revised October 7, 2009
Revised September 1, 2010
Revised February 13, 2013

Supplements System Regulation 29.01 and TAMU SAP 29.01.03.M1.02

Reason for the Guidelines

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 guideline 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 and to educate individuals who may use information resources with respect to their responsibilities associated with such use. The Texas A&M University System Health Science Center’s (HSC) Acceptable Use of Information Resources guideline applies equally to all individuals granted access privileges to any HSC information resources.

1. Responsibility for Use of Information Resources

1.1 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.

1.2 Users must not attempt to access any data or programs contained on HSC systems for which they do not have authorization or explicit consent.

1.3 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.

1.4 Users must not make unauthorized copies of copyrighted software.

1.5 Users must not use non-standard shareware or freeware software without HSC Information Resources Manager (IRM) approval.
1.6 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.

1.7 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.

1.8 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).

1.9 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.

1.10 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.

2. 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.
3. 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