

**THE TEXAS A&M UNIVERSITY SYSTEM  
HEALTH SCIENCE CENTER RULES**

---

---

**24.99.99.Z1 Security of Electronic Information Resources**

*Approved October 24, 2003*

*Revised December 11, 2007*

Supplements System Policy 7.01 and System Policy 33.04

---

---

**1. GENERAL**

- 1.1 The Texas A&M Health Science Center's (HSC) electronic information resources are vital academic and administrative state assets that require appropriate safeguards. Information resources include all computer and telecommunications hardware, software, and networks owned, leased or operated by the HSC as well as the information stored therein.
- 1.2 The HSC will make every effort to protect all data and information technology resources in accordance with the Texas Department of Information Resources information security standards, and guidelines published in the Texas Administrative Code. The HSC is also bound by federal requirements such as the Federal Trade Commission rules regarding the safeguarding of customer information, as well as federal laws relating to privacy of student information and protection of employee and patient health records.

**2. USE OF INFORMATION RESOURCES**

- 2.1 The business or purpose of the HSC is defined by its missions, and information resources are to be used in support of those missions. All persons who have access to and use of HSC information resources, other than resources made available to the public in general, must comply with this Rule and with applicable laws and regulations relating to information resources of state agencies.
- 2.2 There are many issues associated with information resources, not all of which are addressed by this Rule. Additional information is available in the Texas A&M System Policy 7.01 on Ethics, and in System Policy 33.04 Use of System Property. Protocols related to technical standards are also available on the HSC's information technology website.

**3. RESPONSIBILITIES**

- 3.1 The Texas Administrative Code assigns ultimate responsibility for protection of informational resources to the President. For the purposes of this Rule, the procedural responsibilities for the HSC's compliance with the state and federal requirements

regarding information security standards has been delegated by the President to the Vice President for Information Technology and Chief Information Officer.

- 3.2 The Vice President for Information Technology and Chief Information Officer designates the Information Security Officer the responsibility for ensuring that an appropriate security program is in effect and that compliance with this Rule and the Texas Administrative Code standards is maintained for information systems owned and operationally supported by the HSC.
- 3.3 System Administrators who have been assigned custodial responsibility for the information resources utilized in carrying out their technical activities are also responsible for ensuring the security of those resources.
- 3.4 Confidential information maintained on an individual workstation or personal computer must be afforded the appropriate safeguards as stated in the Texas Administrative Code standards. It is the responsibility of the operator, or owner, and/or the departmental System Administrator of that workstation or personal computer to insure that adequate security measures are in place.

#### **4. INFORMATION SECURITY**

- 4.1 Based on risk assessment, performed with the ISAAC-S tool, newly implemented information systems are to be designed to prevent the disclosure of confidential or sensitive information to any unauthorized person and to prevent unauthorized changes to files. Systems are to be designed for ease of use and for quick recovery in the event of disaster.
- 4.2 Accounts that give users restricted access to information resources are to be used only by the persons to whom the accounts are assigned. Log-on IDs, passwords, telephone calling cards, and other means of access must not be shared with anyone. Similarly, users may only access resources for which they are authorized. Holders of means of access are responsible for unauthorized access to their account that results from their negligence in maintaining confidentiality of their means of access.
- 4.3 Users are required to agree by written or electronic signature to use a password identifier only for the purposes intended, not to disclose their password, and to immediately report any possible breach in security. Each employee's information access authority will be reviewed periodically including review at time of a transfer, promotion, or termination.
- 4.4 For various reasons users from outside the HSC community (such as vendors, visitors, consultants, etc.) may occasionally need to gain access to the HSC network. This access will be allowed only when it is 1) authorized, 2) created with a specific expiration date, and 3) removed when the specific project or defined need is complete. Temporary users are subject to the rules and policies of the HSC.

## **5. SECURITY AWARENESS AND TRAINING**

Personnel whose duties bring them into contact with confidential or sensitive information will be required to attend a training program at least annually, and will also receive periodic briefings from the Information Security Officer, or the appropriate designee, to increase their awareness of security issues.

**6. CONTACT:** Information Policy and System Administrator: 800-799-7HSC (800-799-7472)

## **OFFICE OF RESPONSIBILITY**

**Vice President for Information Technology and Chief Information Officer**