

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

---

---

**29.01.03.Z1.16 Security Training**

*Approved September 1, 2010*

**Supplements System Regulation 29.01.03**

---

---

**1. GENERAL**

1.1 Introduction

Understanding the importance of computer security and individual responsibilities and accountability for computer security are paramount to achieving organization security goals. This can be accomplished with a combination of general computer security awareness training and targeted, product specific training. The philosophy of protection and specific security instructions needs to be taught to, and re-enforced with, computer users. The security awareness and training information needs to be continuously upgraded and reinforced.

1.2 Audience

The Texas A&M University System Health Science Center (HSC) Security Training Policy applies equally to all individuals that use 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 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.
- **Office of Information Technology (OIT):** The name of the institution department responsible for computers, networking and data management.
- **User:** An individual that is authorized access to the resource by the owner, in accordance with the owner's procedures and rules. This may include employees, consultants, contractors, temporary workers, or others.

## 2. SECURITY TRAINING POLICY

- 2.1 All new users must take an approved Security Awareness training course prior to, or within 30 days of, being granted access to any HSC information resources.
- 2.2 All users must sign an acknowledgement stating they have read and understand HSC requirements regarding computer security policies and procedures.
- 2.3 All users must be provided with sufficient training and supporting reference materials to allow them to properly protect HSC information resources.
- 2.4 OIT must prepare, maintain, and distribute one or more information security manuals that concisely describe HSC information security policies and procedures.
- 2.5 All users must take an annual computer security compliance training course and pass the associated examination.
- 2.6 OIT must develop and maintain a process to be able to communicate new computer security program information, security bulletin information, and security items of interest.

### **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**