

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

29.01.03.Z1.12 Physical Access

Approved September 1, 2010

Supplements System Regulation 29.01.03

1. GENERAL

1.1 Introduction

Technical support staff, security administrators, system administrators, and others may have information resource physical facility access requirements as part of their function. The granting, controlling, and monitoring of the physical access to information resources facilities is extremely important to an overall security program.

1.2 Audience

The Texas A&M University System Health Science Center (HSC) Physical Access Policy applies to all individuals within the HSC that are responsible for the installation and support of information resources, individuals charged with information resources security, and data owners.

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.

2. PHYSICAL ACCESS POLICY

- 2.1 All physical security systems must comply with all applicable regulations such as, but not limited to, building codes and fire prevention codes.
- 2.2 Physical access to all IR restricted facilities must be documented and managed.
- 2.3 All IR facilities must be physically protected in proportion to the criticality or importance of their function at HSC.
- 2.4 Access to IR facilities must be granted only to HSC support personnel, and contractors, whose job responsibilities require access to that facility.
- 2.5 The process for granting card and/or key access to IR facilities must include the approval of the person responsible for the facility.
- 2.6 Each individual that is granted access rights to an IR facility must receive emergency procedures training for the facility and must sign the appropriate access and non-disclosure agreements.
- 2.7 Requests for access must come from the applicable HSC data/system owner.
- 2.8 Access cards and/or keys must not be shared or loaned to others.
- 2.9 Access cards and/or keys that are no longer required must be returned to the person responsible for the IR facility. Cards must not be reallocated to another individual bypassing the return process.

- 2.10 Lost or stolen access cards and/or keys must be reported to the person responsible for the IR facility.
- 2.11 Cards and/or keys must not have identifying information other than a return mail address.
- 2.12 All IR facilities that allow access to visitors will track visitor access with a sign in/out log.
- 2.13 A service charge may be assessed for access cards and/or keys that are lost, stolen or not returned.
- 2.14 Card access records and visitor logs for IR facilities must be kept for routine review based upon the criticality of the IR being protected.
- 2.15 The person responsible for the IR facility must remove the card and/or key access rights of individuals that change roles within HSC or are separated from their relationship with HSC.
- 2.16 Visitors must be escorted in card access controlled areas of IR facilities.
- 2.17 The person responsible for the IR facility must review access records and visitor logs for the facility on a periodic basis and investigate any unusual access.
- 2.18 The person responsible for the IR facility must review card and/or key access rights for the facility on a periodic basis and remove access for individuals that no longer require access.
- 2.19 Signage for restricted access rooms and locations must be practical, yet minimal discernible evidence of the importance of the location should be displayed.

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