

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

29.01.03.Z1.04 Administrative/Special 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 special access account privilege requirements compared to typical or everyday users. The fact that these administrative and special access accounts have a higher level of access means that granting, controlling and monitoring these accounts is extremely important to an overall security program.

1.2 Audience

The Texas A&M University System Health Science Center (HSC) Administrative/Special Access Policy applies equally to all individuals that have, or may require, special access privilege 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 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.
- **Office of Information Technology (OIT):** The name of the institution department responsible for computers, networking and data management.
- **Security Administrator:** The person charged with monitoring and implementing security controls and procedures for a system. Whereas each institution will have one Information Security Officer, technical management may designate a number of security administrators.
- **System Administrator:** Person responsible for the effective operation and maintenance of IR, including implementation of standard procedures and controls, to enforce an organization's security policy.
- **Abuse of Privilege:** When a user willfully performs an action prohibited by organizational policy or law, even if technical controls are insufficient to prevent the user from performing the action.

- **Vendor:** A person who supplies goods or a service to a governmental entity or another person directed by the entity. The term does not include a state agency or institution, except for Texas Correctional Industries. The term includes an officer or employee of a state agency or institution when acting in a private capacity to supply goods or a service.

2. ADMINISTRATIVE/SPECIAL ACCESS POLICY

- 2.1 HSC departments must submit to OIT a list of administrative contacts for their systems that are connected to the HSC network.
- 2.2 All users must sign the HSC Information Resources Security Acknowledgement and Nondisclosure Agreement before access is given to an account.
- 2.3 All users of administrative/special access accounts must have account management instructions, documentation, training, and authorization.
- 2.4 Each individual that uses administrative/special access accounts must refrain from abuse of privilege and must only initiate investigations under the direction of the ISO.
- 2.5 Each individual that uses administrative/special access accounts must use the account privilege most appropriate with work being performed (i.e., user account vs. administrator account).
- 2.6 Each account used for administrative/special access must meet the HSC Password Policy.
- 2.7 The password for a shared administrator/special access account must change when an individual with the password leaves the department or HSC, or upon a change in the vendor personnel assigned to the HSC contract.
- 2.8 In the case where a system has only one administrator there must be a password escrow procedure in place so that someone other than the administrator can gain access to the administrator account in an emergency situation.
- 2.9 When special access accounts are needed for Internal or External Audit, software development, software installation, or other defined need, they:
 - must be authorized,
 - must be created with a specific expiration date, and
 - must be removed when work is complete.

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