

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

29.01.03.Z1.15 Security Monitoring

Approved September 1, 2010

Supplements System Regulation 29.01.03

1. GENERAL

1.1.Introduction

Security monitoring is a method used to confirm the security practices and controls in place are being adhered to and are effective. Monitoring consists of activities such as the review of:

- Automated intrusion detection system logs,
- Firewall logs,
- User account logs,
- Network scanning logs,
- Application logs,
- Data backup recovery logs,
- Help desk logs, and
- Other log and error files.

1.2.Audience

The Texas A&M University System Health Science Center (HSC) Security Monitoring Policy applies to all individuals that are responsible for the installation of new information resources, the operations of existing information resources, and individuals charged with information resource security.

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.
- **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 executive management for administering the information security functions within the institution. The ISO is the institution's internal and external point of contact for all information security matters.
- **Local Area Network (LAN):** A data communications network spanning a limited geographical area, a few miles at most. It provides communication between computers and peripherals at relatively high data rates and relatively low error rates.

2. SECURITY MONITORING POLICY

2.1. Automated tools will provide real time notification of detected wrongdoing and vulnerability exploitation. Where possible a security baseline will be developed and the tools will report exceptions. These tools will be deployed to monitor:

- Internet traffic,
- Electronic mail traffic,
- LAN traffic, protocols, and device inventory, and
- Operating system security parameters.

2.2. The following files will be checked for signs of wrongdoing and vulnerability exploitation at a frequency determined by risk:

- Automated intrusion detection system logs,
- Firewall logs,
- User account logs,
- Network scanning logs,
- System error logs,
- Application logs,
- Data backup and recovery logs,
- Help desk trouble tickets,
- Telephone activity – Call Detail Reports, and
- Network printer and fax logs.

2.3. The following checks will be performed at least annually by assigned individuals:

- Password strength,
- Unauthorized network devices,
- Unauthorized personal web servers,
- Unsecured sharing of devices, and
- Operating System and Software Licenses.

2.4. Any security issues discovered will be reported to the ISO for follow-up investigation.

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