Texas A&M Health Science Center Guidelines

29.01.03.Z1.15 Guideline: Security Monitoring

Approved September 1, 2010
Revised February 13, 2013

Supplements System Regulation 29.01.03 and TAMU SAP 29.01.03.M1.18

Reason for the Guidelines

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. The Texas A&M System Health Science Center (HSC) Security Monitoring SAP 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. Security Monitoring

1.1 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,
- Local Area Network (LAN) traffic, protocols, and device inventory, and
- Operating system security parameters.

1.2 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.
1.3 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.

1.4 Any security issues discovered will be reported to the Information Security Officer (ISO) for follow-up investigation.

2. Violations

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 Finance and Administration