29.01.03.H0.19 Security Monitoring

Approved: April, 2014
Next Scheduled Review: April, 2019

Procedure Statement

Security monitoring is a method used to confirm that 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
- user account logs
- application logs
- Help Desk logs
- firewall logs
- network scanning logs
- data backup recovery logs
- other log and error files

Reason for Procedure

The purpose of this procedure is to ensure that Information Resource security controls are in place, are effective, and are not being bypassed. One of the benefits of security monitoring is the early identification of wrongdoing or new security vulnerabilities. This early identification can help to block the wrongdoing or vulnerability before harm can be done, or at least to minimize the potential impact. Other benefits include audit compliance, service level monitoring, performance measuring, limiting liability, and capacity planning. This procedure applies to all IT custodians and IT owners of department or information technology resources (including, but not limited to, any networking devices, network monitoring devices, computers acting as network monitoring devices, intrusion detection systems, other packet sniffing devices, logs of other devices such as firewalls and flow detectors monitoring network activity) operating on the Texas A&M University-Texarkana (TAMUT) network.

Definitions

Information Resources (IR): Any computer printouts, online display devices, magnetic storage media, and all computer-related activities involving any device capable of receiving email, browsing websites, 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, tablets, distributed processing systems, network attached and computer controlled medical and laboratory equipment (i.e. embedded technology), smartphones, telecommunication resources, network environments, telephones, fax machines, printers and service bureaus. Additionally, it includes 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): Person responsible to the State of Texas for management of the agency's information resources. The designation of an agency information

resources manager is intended to establish clear accountability for setting policy for information resources management activities, provide for greater coordination of the agency'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 agency. At TAMUT, the IRM is the CIO.

Information Security Officer (ISO): Person responsible to the executive management for administering the information security functions within the University. The ISO is TAMUT'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.

Procedures and Responsibilities

1. SECURITY MONITORING

1.1 All TAMUT computers and network activity are subject to ongoing and unannounced security audits. The inappropriate use of the systems and/or networks which violate TAMUT policies or local, state and federal laws will be investigated (i.e. copyright violations, pornography). The CIO will authorize these investigations, and the appropriate authorities will be notified. The ISO will be responsible for conducting these audits as necessary.

1.2 TAMUT has the right to disclose the contents of electronic files, as required by law, System Internal Audit, or System Office of General Counsel.

1.3 The ISO will be the contact for resolution of security-related anomalies or other suspicious activity.

1.4 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:

1.4.1 Internet traffic

1.4.2 Electronic mail traffic

1.4.3 LAN traffic, protocols, and device inventory

1.4.4 Operating system security parameters

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

1.5.1 Automated intrusion detection system logs

1.5.2 Firewall logs

1.5.3 User account logs

1.5.4 Network scanning logs

1.5.5 System error logs

1.5.6 Application logs

1.5.7 Data backup and recovery logs

1.5.8 Help Desk trouble tickets

1.5.9 Telephone activity – call detail reports

1.5.10 Network printer and fax logs

1.6 The following checks will be performed at least annually

1.6.1 Password strength

1.6.2 Unauthorized network devices

1.6.3 Unauthorized personal web servers

1.6.4 Unsecured sharing of devices

1.6.5 Unauthorized modem use

1.6.6 Operating system and software licenses

1.7 Any discovery of security issues will be reported to the ISO for follow-up investigation.

Related Statutes, Policies, or Requirements

Texas Administrative Code, Title 1, Part 10, Chapter 202, Subchapter C, Rule § 202.75, Information Resources Security Safeguards

References

Copyright Act of 1976
Foreign Corrupt Practices Act of 1977
Computer Fraud and Abuse Act of 1986

Computer Security Act of 1987
The Health Insurance Portability and Accountability Act of 1996 (HIPAA)
The State of Texas Information Act
Texas Government Code, Section 441
Texas Administrative Code, Chapter 202
IRM Act, 2054.075(b)
The State of Texas Penal Code, Chapters 33 and 33A
DIR Practices for Protecting Information Resources Assets
DIR Standards Review and Recommendations Publications

Contact Office

Information Security Officer
903-886-5425