Texas A&M University System Standard – Security Monitoring

Standard Statement

Security Monitoring is a process 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: user account logs, application logs, data backup and recovery logs, automated intrusion detection system logs, etc.

Reason for Standard

The purpose of the security monitoring standard 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.

Definitions

Confidential Information: Information that is excepted from disclosure requirements under the provisions of applicable state or federal law, e.g., the Texas Public Information Act. Refer to System Regulation 29.01.03 and the related Data Classification standard.

Information Resources (IR): The procedures, equipment, and software that are designed, employed, operated, and maintained to collect, record, process, store, retrieve, display, and transmit information or data.

Mission Critical Information: Information that is defined by the System Office or information resource owner to be essential to the continued performance of the mission of the System Offices. Unavailability of such information would result in more than an inconvenience. An event causing the unavailability of mission critical information would result in consequences such as significant financial loss, institutional embarrassment, and failure to comply with regulations or legal obligations, or closure of the department.

Owner of Information Resources: an entity responsible for:

(1) A business function; and

(2) Determining controls and access to information resources supporting that business function.

1. APPLICABILITY

This Standard applies to all System Office managed information resources containing mission critical information, confidential information, and other information resources as may be managed by System Office.

The purpose of the implementation of this standard is to provide a set of measures that will mitigate information security risks associated with security monitoring. There may also be other or additional measures that will provide appropriate mitigation of the risks. The assessment of potential risks and the application of appropriate mitigation measures are to be determined by the information resource owner or their designee.

The information resource owner or designee (e.g., custodian, user), is responsible for ensuring that the risk mitigation measures described in this standard are implemented. Based on risk management considerations and business functions, the resource owner may determine that it would be appropriate to exclude certain risk mitigation measures provided in this standard. All exclusions must be in accordance with standard *Exclusions from Required Risk Mitigation Measures*.

The intended audience is *all individuals that are responsible for the installation of new information resources*, the operations of existing information resources, and individuals charged with information resources security.

2. STANDARDS

2.1 Security monitoring of information resources shall be implemented based on risk management decisions by the resource information owner.

2.1.1 Mission critical or confidential information resource systems shall, at a minimum, be enabled. Automated tools shall be used where deemed beneficial by the resource owner.

2.1.2 Non-mission critical and non-confidential information resource systems monitoring may be enabled as well as other security monitoring features.

2.1.3 Network security monitoring will be conducted by the Security Operations Center (SOC) or other authorized independent parties. Any other monitoring shall be coordinated with System Office ISO, or the Information Resource Manager (IRM), or the System CISO (SCISO).

2.1.4 Logs and other data generated by security monitoring shall be reviewed periodically based on risk management decisions by the system

administrator and will be kept for a period sufficient to enable forensic examination if needed.

2.2 Where feasible, a security baseline information shall be developed and automated detection tools shall report exceptions for mission critical and/or confidential information and kept for a period sufficient to enable forensic examination if needed.

2.3 Any significant security issues discovered and all signs of unauthorized activity shall be reported according to the standard *Incident Management* and in-line with the Regulation 29.01.03 and the process for reporting a breach, hack or incident.

Related Statutes, Policies, or Requirements

Supplements SO standard for *Privacy*

Contact Office

For interpretation or clarification, contact The Texas A&M University System Chief Information Officer.

OFFICE OF RESPONSIBILITY: The Texas A&M University System Chief Information Officer