Information Technology Services
Security Monitoring Standard

Approved: February 11, 2020

Standard 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: user account logs, application logs, data backup and recovery logs, automated intrusion detection system logs, etc.

Reason for Standard

This standard applies to all university-managed information resources containing mission critical information, confidential information, and other information resources as may be managed by Tarleton State University.

The purpose of the security monitoring policy is to ensure that information resource security controls are in place, are effective, and are not being bypassed. In addition, this standard provides 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. In accordance with Texas Administrative Code 202 - Information Security Standards, each department and/or resource owner may elect not to implement some or all of the risk mitigation measures provided in this standard based on information security risk management decisions and business functions. Such risk management decisions must be documented and reported to the designated information security officer (ISO).

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

Standards and Responsibilities

1. Automated tools will provide real-time notification and appropriate response as necessary of detected wrongdoing and vulnerability exploitation. Where possible, a security baseline will be developed and the tools will report exceptions.

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

Definitions

Confidential Information: information that is expected from disclosure requirements under the provisions of applicable state or federal law (e.g., the Texas Public Information Act).

Information Resources (IR): the standards, 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 university or information resource owner to be essential to the continued performance of the mission of the university or department. 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 university or 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.

Contact Office

Information Technology Services
CIO of Information Technology Services
254.968.9395