

**Procedure 29.01.03.T1.14 (Effective 5/4/2006)**  
( Supplements [Rule 29.01.03.T1](#))

## **Information Resources – Security Monitoring**

### 1. GENERAL

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.

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. One of the benefits of security monitoring is the early identification of wrongdoing or new security vulnerabilities.

### 2. APPLICABILITY

This Standard Administrative Procedure (SAP) 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 implementation of this SAP 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. 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 SAP 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 that are responsible for the installation of new information resources, the operations of existing information resources, and individuals charged with information resources security.

### 3. DEFINITIONS

3.1 **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.

3.2 **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.

3.3 **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, failure to comply with regulations or legal obligations, or closure of the university or department.

3.5 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

#### 4. PROCEDURES

4.1 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. These tools will be deployed to monitor:

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

4.2 The following files shall be checked, as appropriate, for signs of wrongdoing and vulnerability exploitation at a frequency determined by risk:

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

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

- o Password strength
- o Unauthorized network devices
- o Unauthorized personal web servers
- o Unsecured sharing of devices
- o Unauthorized modem use

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

**OFFICE OF RESPONSIBILITY:** Department of Information Resources

**CONTACT:** Executive Director of Information Resources