SAP 29.01.03.T0.06 Information Technology Services – Intrusion Detection

Approved:	May 4, 2006
Revised:	February 28, 2012
Revised:	May 21, 2014
Next Scheduled Review:	May 21, 2019

Procedure Statement

Intrusion detection plays an important role in implementing and enforcing an organizational security policy. As information systems grow in complexity, effective security systems must evolve. With the proliferation of the number of vulnerability points introduced by the use of distributed systems, some type of assurance is needed that the systems and network are secure. Intrusion detection systems can provide part of that assurance. Intrusion detection provides two important functions in protecting information resources:

1. Feedback is information that addresses the effectiveness of other components of a security system. If a robust and effective intrusion detection system is in place, the lack of detected intrusions is an indication that other defenses are working.

2. A trigger is a mechanism that determines when to activate planned responses to an intrusion incident.

Reason for Procedure

This Standard Administrative Procedure (SAP) applies to Tarleton State University information resources that store, process, or transmit mission critical and/or confidential information.

The purpose of the implementation of this SAP is to provide a set of measures that will mitigate information security risks associated with intrusion detection. 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 for this SAP includes, but is not limited to, all information resources management personnel, owners, and system administrators.

Procedures and Responsibilities

1. PREVENTION AND DETECTION

    1.1 Operating system, user accounting, and application software audit logging processes shall be enabled on all host and server systems where resources permit.

    1.2 Alarm and alert functions, as well as audit logging of any firewalls and other network perimeter access control systems, shall be enabled.

    1.3 Audit logs from the network perimeter access control systems shall be monitored/reviewed as risk management decisions warrant.

    1.4 Audit logs for servers and hosts on the internal, protected network shall be reviewed as warranted based on risk management decisions. The system administrator will furnish any audit logs as requested by appropriate university personnel.
    - Host-based intrusion tools will be tested on a routine schedule.
    - Reports shall be reviewed for indications of intrusive activity.

    1.5 All suspected and/or confirmed instances of successful intrusions shall be immediately reported to the ISO. Information resource users are encouraged to report any anomalies in system performance and/or signs of unusual behavior or activity to their departmental system administrator or the Information Resources Help Desk.

    1.6 System administrators shall keep abreast of industry best practices regarding current intrusion events and methods to detect intrusions. Intrusion detection methods shall be utilized as needed.

2. RESPONSE AND RECOVERY

    2.1 Based on the assessment of risk, appropriate action should be taken to protect Tarleton State University's information resources.

Related Statutes, Policies, or Requirements

Supplements *SAP 29.01.03.T0.19 Security of Electronic Information Resources*

Definitions

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.

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. **Information Security Officer (ISO):** responsible for administering the information security functions within Tarleton and reports to the information resources manager (IRM).

4. **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 a department or the university.

5. **Owner of an Information Resource**: an entity responsible for a business function and determining controls and access to information resources supporting that business function.

Contact Office

Information Technology Services
Executive Director and CIO of Information Technology Services
254.968-9395