Texas A&M University System Standard – Intrusion Detection

Standard 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:

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

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 the Data Classification Standard under Regulation 29.01.03 for more information.

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 Office 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 System Office or department.

Owner of an Information Resource: an entity responsible for:

- A business function; and,
- Determining controls and access to information resources supporting that business function.

Official Standard

1. APPLICABILITY

This Standard (standard) applies to System Office information resources that store, process, or transmit mission critical and/or confidential information.

The purpose of the implementation of this standard 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.

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 the standard *Exclusions from Required Risk Mitigation Measures*.

The intended audience for this standard includes, but is not limited to, all information resources management personnel, owners, and system administrators.

2. STANDARDS

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

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

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

2.4 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 System Office personnel.

2.4.1 Host based intrusion tools will be tested on a routine schedule.

2.4.2 Reports shall be reviewed for indications of intrusive activity.

2.5 All suspected and/or confirmed instances of successful intrusions shall be immediately reported according to incident management procedures (see the standard *Incident Management*).

Information resource users are encouraged to report any anomalies in system performance and/or signs of unusual behavior or activity to the System Office Security Officer or to the System Chief Information Security Officer.

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

Related Statutes, Policies, or Requirements

Report a breach, incident or hack

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.