The Division of Information Technology
University Information Security Standards

Information Security Standard – Intrusion Detection (Legacy TAC 202)
Approved: April 15, 2005
Last Revised: July 26, 2017
Next Scheduled Review: August 2018

1. General

Intrusion detection plays an important role in implementing and enforcing an organizational security policy. As information resources 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.

2. Applicability

This standard applies to University information resources that store, process, or transmit mission critical and/or confidential information.

The purpose 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 division, division/department heads, or deans will provide to further mitigate risks. The assessment of potential risks and the application of appropriate mitigation measures are to be determined by the department heads and their identified information security administrators. 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 is based on documented and approved information security risk management decisions and business functions. Such risk management decisions must be documented and approved by the designated Information Security Officer (ISO).

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

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: Any and all computer printouts, online display devices, magnetic storage media, and all computer-related activities involving any device capable of receiving email, browsing Web sites, or otherwise capable of receiving, storing, managing, or transmitting electronic data including, but not limited to, mainframes, servers, personal computers, notebook computers, hand-held computers, personal digital assistant (PDA), pagers, distributed processing systems, network attached and computer controlled medical and laboratory equipment (i.e. embedded technology), telecommunication resources, network environments, telephones, fax machines, printers and service bureaus. Additionally, it is the procedures, equipment, facilities, software, and data that are designed, built, operated, and maintained to create, collect, record, process, store, retrieve, display, and transmit information.

3.3 Information Resources Manager (IRM): Responsible to the State of Texas for management of the agency/university's information resources. The designation of an agency/university information resources manager is intended to establish clear accountability for setting policy for information resources management activities, provide for greater coordination of the state agency's information activities, and ensure greater visibility of such activities within and between state agencies. The IRM has been given the authority and the accountability by the State of Texas to implement Security Policies, Procedures, Practice Standards, and Guidelines to protect the Information Resources of the agency. If an agency does not designate an IRM, the title defaults to the agency's Executive Director, and the Executive Director is responsible for adhering to the duties and requirements of an IRM.

3.4 Information Security Officer (ISO): Responsible to the executive management for administering the information security function within the agency. The ISO is the university's internal and external point of contact for all information security matters.

3.5 User: An individual or automated application or process that is authorized to the resource by the owner, in accordance with the owner's procedures and rules.

3.6 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.

3.7 Owner of an Information Resource: an entity responsible:

(1) for a business function (Department Head); and,

(2) for determining controls and access to information resources

4. Procedures

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

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

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

4.4 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.

(1) Host based intrusion tools will be tested on a routine schedule.

(2) Reports shall be reviewed for indications of intrusive activity.

4.5 All suspected and/or confirmed instances of successful intrusions shall be immediately reported to the information security officer (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 helpdesk. System administrators shall keep abreast of industry best practices regarding current intrusion detection events and methods to detect intrusions. Intrusion detection methods shall be utilized as needed.

5. Response and Recovery

Based on the assessment of risk, appropriate action should be taken to protect West Texas A&M University's information resources.

OFFICE OF RESPONSIBILITY: Information Technology

CONTACT: Chief Information Officer