

# STANDARD ADMINISTRATIVE PROCEDURE

## **29.01.99.M1.11 Information Resources – Intrusion Detection**

*Approved July 18, 2005*

*Next Scheduled Review: Currently Under Review*

*Supplements [University Rule 29.01.99.M1](#)*

### 1. GENERAL

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:

- 1.1 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.
- 1.2 A trigger is a mechanism that determines when to activate planned responses to an intrusion incident.

### 2. APPLICABILITY

This Standard Administrative Procedure (SAP) applies to 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 in the annual ISAAC report (See [University Rule 29.01.99.M1](#)).

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 (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.
- 3.4 Owner of an Information Resource: an entity responsible for:
  - 3.4.1 a business function; and,
  - 3.4.2 determining controls and access to information resources supporting that business function.

### 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.
  - 4.4.1 Host based intrusion tools will be tested on a routine schedule.

4.4.2 Reports shall be reviewed for indications of intrusive activity.

- 4.5 All suspected and/or confirmed instances of successful intrusions shall be immediately reported according to incident management procedures (see [SAP 29.01.99.M1.09, Incident Management](#)).

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 CIS Help Desk.

- 4.6 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.

CONTACT: [Information Technology Issues Management of CIS](#)

OFFICE OF RESPONSIBILITY: [Vice President and Associate Provost for Information Technology](#)