

29.01.99.E1.11 Information Resources – Intrusion Detection

Approved January 20, 2004
Revised November 21, 2006
Revised September 15, 2009
Revised June 5, 2013
Next Scheduled Review: June 5, 2016

Supplements TEES Rule 29.01.99.E1

Standard Administrative Procedure Statement
Intrusion detection plays an important role in implementing and enforcing an organizational security policy.

Reason for Standard Administrative Procedure
The purpose of the intrusion detection procedure is to provide a set of measures that will mitigate information security risks associated with intrusion detection.

Procedures and Responsibilities

1. CONTROLS AND RESPONSIBILITIES

   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 TEES personnel.

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

      1.4.2 Reports shall be reviewed for indications of intrusive activity.

   1.5 All suspected and/or confirmed instances of successful intrusions shall be immediately reported according to incident management procedures (see TEES SAP 29.01.99.E1.09, Incident Management). Information resource users are encouraged to report any anomalies in system performance and/or
signs of unusual behavior or activity to their division system administrator or the TAMU Computing and Information Services (CIS) Help Desk.

1.6 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**

TAMU SAP 29.01.99.M1.11, Information Resources – Intrusion Detection

TEES Rule 29.01.99.E1, Security of Electronic Information Resources

TEES SAP 29.01.99.E1.09, Information Resources – Intrusion Detection

**Contact Office**

Information Technology Services
(979) 847-8585