29.01.99.E1.18 Information Resources - Security Monitoring

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
The scope of this procedure is to monitor information resources.

Reason for Standard Administrative Procedure
The purpose of the security monitoring procedure is to ensure that information resource security controls are in place, are effective, and are not being bypassed.

Procedures and Responsibilities

1. CONTROLS AND RESPONSIBILITIES

   1.1 Security monitoring of information resources shall be implemented based on risk management decisions by the resource information owner.

      1.1.1 Mission critical or confidential information resource systems shall, at a minimum, enable operating system logging features. Automated tools shall be used where deemed beneficial by the resource owner.

      1.1.2 Non-mission critical and non-confidential information resource systems may enable operating system logging features and other security monitoring features.

      1.1.3 Network security monitoring will be conducted by TAMU Computing and Information Services (CIS). Any other monitoring shall be coordinated with CIS and TEES CIO. They can be contacted through CIS Network Group or Help Desk Central at (979) 845-8300.

      1.1.4 Logs and other data generated by security monitoring shall be reviewed periodically based on risk management decisions by the system administrator.
1.2 Where feasible, a security baseline shall be developed and automated detection tools shall report exceptions for mission critical and/or confidential information.

1.3 Where possible, the following checks will be performed at least annually by the information resource owner and documented in the annual ISAAC process:

1.3.1 Password policy implementation verification;

1.3.2 Absence of unauthorized servers (e.g., web, ftp, file); and,

1.3.3 Integrity and appropriateness of access controls.

1.4 Any significant security issues discovered and all signs of unauthorized activity shall be reported according to TEES SAP 29.01.99.E1.09, Incident Management.

Related Statutes, Policies, or Requirements
TAMU SAP 29.01.99.M1.18, Information Resources – Security Monitoring

TEES Rule 29.01.99.E1, Security of Electronic Information Resources

TEES SAP 29.01.99.E1.09, Information Resources – Incident Management

Contact Office
Information Technology Services
(979) 847-8585