29.01.99.E1.20  Information Resources - Server Hardening

Supplements  TEES Rule 29.01.99.E1

Standard Administrative Procedure Statement
The scope of this procedure is to ensure the servers are installed and maintained in a manner that prevents unauthorized access, unauthorized use, and disruptions in service.

Reason for Standard Administrative Procedure
The purpose of the server hardening procedure is to describe the requirements for installing a new server in a secure fashion and maintaining the security integrity of the server and application software.

Procedures and Responsibilities

1. CONTROLS AND RESPONSIBILITIES
   
   1.1 Division information technology personnel will test security patches prior to implementation where practical. Division information technology personnel are encouraged to have hardware resources available for testing security patches in the case of special applications.
   
   1.2 System administrators ensure that vendor supplied patches are routinely acquired, systematically tested, and installed promptly based on risk management decisions.
   
   1.3 System administrators shall remove unnecessary software, system services, and drivers.
   
   1.4 System Administrators shall enable security features included in vendor supplied systems including, but not limited to, firewalls (unless this is part of a system inside a departmental hardware firewall), virus scanning and malicious code protections, and other file protections (see TEES SAP 29.01.99.E1.23, Malicious Code). Audit logging shall also be enabled. User privileges shall be set utilizing the least privileges concept of providing the minimum amount of access required to perform job functions. Privileges may be added as need is demonstrated by the user. The use of passwords shall be enabled in accordance with TEES SAP 29.01.99.E1.14, Password/Authentication.
1.5 System Administrators shall disable or change the password of default accounts before placing the resource (e.g., server) on the network.

1.6 Servers shall be tested by system administrators or their designee for known vulnerabilities periodically or when new vulnerabilities are announced.

1.7 System Administrators shall seek and implement best practices for securing their particular system platform(s).

Related Statutes, Policies, or Requirements
TAMU SAP 29.01.99.M1.20, Information Resources – Server Hardening

TEES Rule 29.01.99.E1, Security of Electronic Information Resources

TEES SAP 29.01.99.E1.14, Information Resources – Password/Authentication

TEES SAP 29.01.99.E1.23, Information Resources – Malicious Code

Contact Office
Information Technology Services
(979) 847-8585