

# STANDARD ADMINISTRATIVE PROCEDURE

## 29.01.99.M1.20 Information Resources – Server Hardening

*Approved July 18, 2005*

*Revised February 24, 2009*

*Next Scheduled Review: February 24, 2012*

---

### Standard Administrative Procedure Statement

---

The purpose of the TAMU server hardening procedures 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.

---

### Definitions

---

**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.

**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.

**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.

**Security Patch** - a fix to a program that eliminates a vulnerability exploited by malicious hackers.

**Information Resource Owner** - an entity responsible for:

- a business function; and,
- determining controls and access to information resources supporting that business function.

---

## Responsibility and Procedures

---

### 1. GENERAL

Servers are relied upon to deliver data in a secure, reliable fashion. There must be assurance that data integrity, confidentiality and availability are maintained. One of the required steps to attain this assurance is to ensure that the servers are installed and maintained in a manner that prevents unauthorized access, unauthorized use, and disruptions in service.

The purpose of the TAMU server hardening procedures 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.

### 2. APPLICABILITY

This Standard Administrative Procedure (SAP) applies to all University information resources that store or process mission critical and/or confidential information.

The information resource owner, or designee, is responsible for ensuring that the risk mitigation measures described in this SAP are implemented. Based on risk management considerations and business functions, the resource owner may determine that it would be appropriate to exclude certain risk mitigation measures provided in this SAP. All exclusions must be in accordance with SAP 29.01.99.M1.27 Exclusions from Required Risk Mitigation Measures.

The intended audience includes, but is not limited to, computing system managers and administrators who manage University information resources that store or process mission critical and/or confidential information.

### 3. PROCEDURES

3.1 Departmental information technology personnel will test security patches prior to implementation where practical. Departmental information technology personnel are encouraged to have hardware resources available for testing security patches in the case of special applications.

3.2 System Administrators shall ensure that vendor supplied patches are routinely acquired, systematically tested, and installed promptly based on risk management decisions.

- 3.3 System Administrators shall remove unnecessary software, system services, and drivers.
- 3.4 System Administrators shall enable security features included in vendor supplied systems including, but not limited to, firewalls, virus scanning and malicious code protections, and other file protections (see [SAP 29.01.99.M1.23, 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 [SAP 29.01.99.M1.14, Password/Authentication](#).
- 3.5 System Administrators shall disable or change the password of default accounts before placing the resource (e.g., server) on the network.
- 3.6 Servers, especially, shall be tested by system administrators or their designee for known vulnerabilities periodically or when new vulnerabilities are announced.
- 3.7 System Administrators shall seek and implement best practices for securing their particular system platform(s).

---

### **Related Statutes, Policies, or Requirements**

---

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

---

### **Contact Office**

---

Contact [Information Technology Issues Management](#) for SAP interpretation or clarification.

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