



Home | Calendar | Academic Affairs | Student Affairs | President's Office | Directory | JOBS | Giving to PVAMU

Business Affairs

- ▶ Our Mission
- ▶ Contact Information
- ▶ Organization Chart
- ▶ Staff Directory
- ▶ Forms Library
- ▶ Policy Library
- ▶ Reports Library
- ▶ Training Library
- ▶ Business Affairs Online Services
- ▶ Professional Development
- ▶ Business Affairs Calendar
- ▶ Office of VPBA Presentations
- ▶ Send us your comments

Business Affairs Services

- ▶ Administrative Memoranda
- ▶ Compensation Pay Plan
- ▶ Financial Aid Policies & Procedures
- ▶ Human Resources Policies
- ▶ **Information Security Standards**
 - Acceptable Use
 - Authorized Software
 - Email Usage
 - Internet/Intranet Usage
 - Malicious Code
 - Network Access
 - Portable Computing
 - Privacy
 - Security Training
 - Network Configuration
 - Account Management
 - Administrator/Special Access
 - Backup/Recovery
 - Change Management
 - Incident Management
 - Intrusion Detection
 - Physical Access
 - Security Monitoring
 - **Server Hardening**
 - Vendor Access
 - System Development
- ▶ Parking Rules & Regulations
- ▶ PVAMU Administrative Procedures
- ▶ PVAMU Rules
- ▶ Travel Policies

Information Technology Services

Home Student Portal Panther Email Printable Version

Home » Forms, Policies & Reports » Policy Library » Information Security Standards » Server Hardening

Server Hardening

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.

2. Applicability

This procedure applies to all University information resources that store or process mission critical and/or confidential information. The purpose of this procedure is to provide a set of measures that will mitigate information security risks associated with server hardening. The intended audience includes, but is not limited to, system managers and administrators, who manage University information resources that store or process mission critical and/or confidential information.

3. 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, and failure to comply with regulations or legal obligations, or closure of the University or department.

4. Procedures

1. Systems administrators will test security patches prior to implementation.
2. System administrators shall ensure that vendor supplied patches are routinely acquired, systematically tested, and installed promptly (Usually within 2 weeks of its release).
3. System administrators shall remove unnecessary software, system services, and drivers.
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 Malicious Code procedure). 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. The use of passwords shall be enabled in accordance with the University Password Policy.
5. System administrators shall disable or change the password of default accounts.
6. Servers shall be tested for known vulnerabilities when new vulnerabilities are announced, and shall seek and implement best practices for securing their particular system platform(s).

Contact PVAMU | ADA Resources | Compact with Texans | Homeland Security | Legal Notices
Open Records | Privacy | Risk & Misconduct Hotline | TRAIL | State of Texas | Webmaster

2003 PRAIRIE VIEW A&M UNIVERSITY - ALL RIGHTS RESERVED
P.O. Box 519 - Prairie View, Texas - 77446-0519
FM 1098 Rd & University Dr, Prairie View, TX 77446

University Operator: (936) 261-3311
Best viewed with Netscape 6 or Internet Explorer 6