Procedure Statement

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. Additionally, desktop computing systems must be secured and maintained to prevent similar unauthorized use and access.

Reason for Procedure

This Procedure applies to all Texas A&M University-San Antonio (A&M-San Antonio) information resources that store or process mission critical and/or confidential information.

The purpose of the implementation of this Procedure is to provide a set of measures that will mitigate information security risks associated with server hardening. There may also be other or additional measures that division or department heads will provide to further mitigate risks. The assessment of potential risks and the application of appropriate mitigation measures are to be determined by the department heads and their identified information security administrators. In accordance with Texas Administrative Code 202 - Information Security Standards, each department and/or resource owner may elect not to implement some or all of the risk mitigation measures provided in this Procedure based on documented and approved information security risk management decisions and business functions. Such risk management decisions must be documented and approved by the designated Information Security Officer (ISO).

The intended audience for this Procedure includes, but is not limited to, system managers and administrators, who manage A&M-San Antonio information resources that store or process mission critical and/or confidential information.
Official Responsibilities and Procedure

1. PROCEDURES FOR ALL SERVERS

1.1. Systems administrators will test security patches prior to implementation when practical. Systems administrators are encouraged to have hardware resources available for testing security patches in the case of special applications.

1.2. A server must not be connected to the A&M-San Antonio network until it is in an accredited secure state and the network connection is approved by network services personnel.

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

1.4. System Administrators shall remove unused software, system services, and drivers as needed.

1.5. 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.

1.6. System Administrators shall enable audit logging, preferable to a central logging server, and shall review logs based on risk management decisions.

1.7. User privileges shall be set utilizing the least privileges concept of providing the minimum account of access required to perform job functions. Privileges may be added as need is demonstrated by the user and appropriate division/department head. The use of passwords shall be enabled in accordance with 29.01.03.O0.25 Password Authentication.

1.8. System Administrators shall disable or change the password of default accounts before placing the resource onto the network. The System Administrator will assign a “strong” password based on strong password standards on all default and/or administrative accounts.

1.9. Servers shall be tested for known vulnerabilities when new vulnerabilities are announced, and shall seek and implement industry security practices for securing their particular system platform(s). Upon notice of vulnerability, servers will be tested within 30 days.
2. WINDOWS SERVERS

2.1. Microsoft Windows Server Update Services shall be utilized to provide automatic hotfixes, patches, service packs, and device drivers from a centralized IT server. In instances where automated update pools are unable to be utilized, manual updates will be performed as soon as reasonably possible based on risk management decisions.

Non-Compliance

Violation of this Procedure may result in disciplinary action, which may include termination of employment for full-time and part-time employees; a termination of the employment relationship in the case of contractors or consultants; dismissal for interns and volunteers; or in the case of students suspension or expulsion administered based on the Code of Student Conduct. Additionally, individuals are subject to loss of access and privileges to the University information resources, civil, and/or criminal prosecution.

Related Statutes, Policies, or Requirements

- DIR Practices for Protecting Information Resources Assets
- Family Educational Rights and Privacy Act (FERPA)
- Gramm Leach Bliley Act (GLB Act)
- Health Insurance Portability and Accountability Act (HIPAA)
- Texas Administrative Code (TAC) 202 as amended or supplemented
- Texas Administrative Code (TAC) 202.75 Security Standards for Institutions of Higher Education
- TAMU System Policy 29.01 Information Resources

Definitions

- **Accounts** - Information resource users are typically assigned access to an information resource using logon credentials, which include, at the minimum, a unique user name and password.

- **Change** – Any implementation of new functionality, any interruption of service, any repair of existing functionality, and/or any removal of existing functionality.
**Change Management** – The process of controlling modifications to hardware, software, firmware, and documentation to ensure that information resources are protected against improper modification before, during and after system implementation.

**Confidential Information** - Information that is excluded from disclosure requirements under the provisions of applicable state or federal law, (e.g. the Texas Public Information Act and other constitutional, statutory, judicial, and legal agreements).

**Custodian** - Guardian or caretaker (the holder of data). The agent charged with implementing the controls specified by the owner. The custodian is responsible for the processing and storage of information.

**Emergency Change** – When an immediate response to imminent critical system failure is needed to prevent widespread service disruption.

**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.

**Information Resources Manager (IRM)** - The Information Resources Manager (IRM) oversees the acquisition and use of information technology within a state agency or university. The IRM ensures that all information resources are acquired appropriately, implemented effectively, and comply with regulations and agency policies.

**Information Security Officer (ISO)** - Responsible to the executive management for administering the information security functions within the agency. The ISO is the internal and external point of contact for all information security matters.

**Information Technology Services (ITS)** – The designated name for the central Information Technology department for the University.

**Mission Critical Information** - Information that is defined by A&M-San Antonio or information resource owner to be essential to the continued performance of the mission of A&M-San Antonio 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 A&M-San Antonio or department.

**Owner** - The manager or agent responsible for the function which is supported by the resource; the individual upon whom responsibility rests for carrying out the appropriate use and safeguards for the resource. Where appropriate, ownership may be shared by managers of different departments.

**Production System** - The hardware, software, physical, procedural and organizational issues that need to be considered when addressing the security of an application, group of applications, organizations, or group of organizations.
**Scheduled Change** – A system modification accompanied by a formal notification received, reviewed, and approved by the review process in advance of the change being made.

**Security Patch** - A fix or repair to a program that eliminates a known system vulnerability.

**System Custodian** – Guardian or caretaker of the operating system and physical hardware; the person(s) charged with implementing the controls specified by the owner of the system. This custodian is responsible for operating system updates and assisting the Application Custodian with any testing or major changes to the system.

**Unscheduled Change** – A system modification that fails to present notification to the formal process in advance of the change being made.

**User** - An individual or automated application or process that is authorized to the resource by the owner, in accordance with the owner’s rules and procedures.

**Vulnerability** - A weakness or flaw in system security design, implementation, procedures or controls that can cause a violation of the system’s security policy or a security breach if exploited by an attacker.

**Contact Office**

Finance and Administration, Information Technology Services (210) 784-4357 (HELP)