Texas A&M University System Standard – Server Hardening

Standard Statement

The purpose of the System Office (SO) server hardening standard 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. Refer to the System Regulation 29.01.03 and the related Data Classification Standard for more information.

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 SO or information resource owner to be essential to the continued performance of the mission of the SO. 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 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 Standards

1. GENERAL

   Computer servers are relied upon to deliver, store and secure 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 standard applies to all SO 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 standard 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 standard. All exclusions must be in accordance with standard *Exclusions from Required Risk Mitigation Measures*.

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

3. STANDARDS

3.1 System administrators will test security patches prior to implementation where practical. Systems administrators 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 and timely acquired, systematically tested, and installed promptly based on risk management decisions.

3.3 System Administrators shall remove unnecessary software, system services, and drivers or those that pose an elevated risk profile which makes a server a target or vulnerable to a breach.

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 standard for *Malicious Code*). Audit logging shall also be enabled and retained for a 12-month period. 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 standard for *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) based upon risk management decisions by management, owners of systems and recommendations from vendors of their products. System Administrators will be fully knowledgeable regarding server platforms and security at all times and keep current knowledge of security issues regarding servers, server platform systems and server platform management.

Related Statutes, Policies, or Requirements

Regulation 29.01.03

Contact Office

For interpretation or clarification, contact The Texas A&M University System Chief Information Officer.

OFFICE OF RESPONSIBILITY: The Texas A&M University System Chief Information Officer