The Division of Information Technology
University Information Security Standards

Information Security Standard – Server Hardening (Legacy TAC 202)
Approved: April 15, 2005
Last Revised: July 26, 2017
Next Scheduled Review: August 2018

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 information security standard applies to all University information resources that store or process mission critical and/or confidential information.

The purpose of this information security standard 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 department heads or deans will provide to further mitigate risks. The assessment of potential risks and the application of appropriate mitigation measures is 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 is based on documented 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 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

3.1 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.

3.2 Information Resources: Any and all computer printouts, online display devices, magnetic storage media, and all computer-related activities involving any device capable of receiving email, browsing Web sites, or otherwise capable of receiving, storing, managing, or transmitting electronic data including, but not limited to, mainframes, servers, personal computers, notebook computers, hand-held computers, personal digital assistant (PDA), pagers, distributed processing systems, network attached and computer controlled medical and laboratory equipment (i.e. embedded technology), telecommunication resources, network environments, telephones, fax machines, printers and service bureaus. Additionally, it is the procedures, equipment, facilities, software, and data that are designed, built, operated, and maintained to create, collect, record, process, store, retrieve, display, and transmit information.

3.2 Information Resources Manager (IRM): Responsible to the State of Texas for management of the agency/university's information resources. The designation of an agency/university information resources manager is intended to establish clear accountability for setting policy for information resources management activities, provide for greater coordination of the state agency's information activities, and ensure greater visibility of such activities within and between state agencies. The IRM has been given the authority and the accountability by the State of Texas to implement Security Policies, Procedures, Practice Standards, and Guidelines to protect the Information Resources of the agency. If an agency does not designate an IRM, the title defaults to the agency's Executive Director, and the Executive Director is responsible for adhering to the duties and requirements of an IRM.

3.3 Information Security Officer (ISO): Responsible to the executive management for administering the information security function within the agency. The ISO is the university's internal and external point of contact for all information security matters.

3.3 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.

4. Procedures

4.1 Systems administrators will test security patches prior to implementation, when applicable.

4.2 A server must not be connected to the West Texas A&M University network until it is in a West Texas A&M University accredited secure state and the network connection is approved by West Texas A&M University information technology – network services personnel.

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

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

4.5 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. Audit logging shall also be enabled. 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 this standard for password authentication.

4.6 System Administrators shall disable or change the password of default accounts.

4.7 Servers, especially, shall be tested periodically by system administrators (or their designee) for known vulnerabilities.

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

OFFICE OF RESPONSIBILITY: Information Technology

CONTACT: Chief Information Officer