PRAIRIE VIEW A&M UNIVERSITY
UNIVERSITY ADMINISTRATIVE PROCEDURE

29.01.03.P0.13 Information Resources – Server Hardening
Approved May 26, 2009
Revised January 23, 2013
Revised August 14, 2017
Next Scheduled Review: August 2022

UAP Purpose

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 server hardening procedures is to describe the requirements for installing a new server in a secure fashion and maintaining the integrity of server and application software.

Definitions

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 Security Officer (ISO) - person responsible to the executive management for administering the information security function within the University. The ISO is the University's internal and external point of contact for all information security matters.

Confidential Information - information that is confidential pursuant to state or federal law. Such information may also be subject to state or federal breach notification requirements. See the Texas A&M University System Data Classification Standard for additional information.

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.

Information Resource Owner - an entity responsible for a business function and for determining controls and access to information resources supporting that business function.

System Administrator – any individual who operates and maintains a server.

Official Procedures and Responsibilities

1. CONTROLS AND RESPONSIBILITIES

1.1 System administrators must only install the operating system after they have verified the source is legitimate.

1.1.1 Only current, supported, and updateable operating systems are to be used. Out-of-support or sunset operating systems must have the approval of the Chief Information Officer and the Information Security Officer (ISO) before being used and appropriate security protocols agreed beforehand.

1.2 System administrators must ensure that vendor supplied patches are routinely acquired and installed promptly.

1.3 Upon completion of server installation, system administrators must remove unnecessary software, system services and drivers.

1.4 Upon completion of server installation, system administrators must set security parameters, file protections and enable audit logging.

1.5 Upon completion of server installation, system administrators must disable or change the password of default accounts.

1.6 Upon completion of server installation, system administrators must implement system identification and logon banners that include the following statements:

1.6.1 Unauthorized use is prohibited;

1.6.2 Usage may be subject to security testing and monitoring;

1.6.3 Misuse is subject to criminal prosecution; and,

1.6.4 No expectation of privacy except as otherwise provided by applicable privacy laws.

1.7 For Windows Servers, server administrator must run Microsoft Security Baseline Analyzer.

1.8 The ISO will monitor information technology servers (centralized & decentralized) for updates and patches periodically.

Related Statutes, Policies, Regulations and Rules

Tex. Admin. Code Ch. 202, Subch. C, Information Security Standards for Institutions of Higher Education

System Policy 29.01 Information Resources

System Regulation 29.01.03 Information Security

The Texas A&M University System Information Security Standards

Security Control Standards Catalog

Contact Office	
Office of Information Resources Management	936-261-9350