Server Hardening Policy

Introduction
Servers are depended 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.

1. Purpose
The purpose of the Texas A&M University-Kingsville Server Hardening Policy document 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.

2. Audience
The Texas A&M University-Kingsville Server Hardening Policy applies to all individuals that are responsible for the installation of new Information Resources, the operations of existing Information Resources, and individuals charged with Information Resource security.

3. Server Hardening Policy
3.1. A server must not be connected to the Texas A&M University-Kingsville network until it is in a TAMUK CIS accredited secure state and the network connection is approved by TAMUK CIS.
3.2. The Server Hardening Procedure provides the detailed information required to harden a server and must be implemented for Texas A&M University-Kingsville CIS accreditation. Some of the general steps included in the Server Hardening Procedure include:
   • Installing the operating system from an CIS approved source
   • Applying vendor supplied operating system, application patches and updates
   • Removing or disabling of unnecessary system services or drivers
   • Uninstalling of unnecessary software
   • Setting security parameters, file protections and enabling audit logging
   • Disabling or changing the password of default accounts
   • Installing CIS approved anti-virus software
3.3. Texas A&M University-Kingsville CIS will monitor security issues, both internal and external to Texas A&M University-Kingsville, and will manage the release of security bulletins on behalf of Texas A&M University-Kingsville.
3.4. Texas A&M University-Kingsville CIS will test security patches against CIS resources where practical.
3.5. Texas A&M University-Kingsville CIS may make hardware resources available for testing security patches in the case of special applications.
3.6. Security patches must be implemented within the specified timeframe of notification from Texas A&M University-Kingsville CIS.
3.7. Violations of this policy must be reported to the ISO or Security Analyst.

Disciplinary Actions
Violation of this policy may result in disciplinary action up to and including termination for employees and temporaries; a termination of employment relations in the case of contractors or consultants; dismissal for interns and volunteers; or suspension or expulsion in the case of a student. Additionally, individuals are subject to loss of Texas A&M University-Kingsville Information Resources access privileges, civil, and criminal prosecution.