Server Hardening Procedure

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 at Texas A&M University-Kingsville (TAMUK). 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.

Purpose
The purpose of this procedure 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.

Audience
This procedure applies to individuals that are responsible for the installation of new servers, the operations of existing servers, and individuals charged with server security at TAMUK.

Server Hardening Procedure
1. A server must not be connected to the University network until it is in an accredited secure state and the network connection is approved by iTech.
2. The Server Hardening Procedure provides the detailed information required to harden a server and must be performed for accreditation.
3. Some of the general steps included in the Server Hardening Procedure include:
   a. Installing the operating system from an iTech approved source
   b. Applying vendor supplied operating system, application patches and updates
   c. Removing or disabling of unnecessary system services or drivers
   d. Uninstalling of unnecessary software
   e. Setting security parameters, file protections and enabling audit logging
   f. Disabling or changing the password of default accounts
   g. Installing iTech approved anti-virus software
4. iTech will test security patches against iTech resources where practical.
5. iTech may make hardware resources available for testing security patches in the case of special applications.
6. Security patches must be implemented within the specified timeframe.
7. Vulnerability assessments will be performed in accordance with the Vulnerability Assessment Procedures.
8. Violations of this procedure must be reported to the Information Security Officer or Security Analyst.

Disciplinary Actions
Violation of this procedure 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 TAMUK Information Resources access privileges, civil, and criminal prosecution.
References

1. Copyright Act of 1976
2. Computer Fraud and Abuse Act of 1986
4. DIR Practices for Protecting Information Resources Assets
5. DIR Standards Review and Recommendations Publications
7. The Health Insurance Portability and Accountability Act of 1996 (HIPAA)
8. IRM Act, 2054.075(b)
9. The State of Texas Information Act
10. The State of Texas Penal Code, Chapters 33 and 33A
11. Texas Administrative Code, Chapter 202
12. Texas A&M University-Kingsville Procedure 29.01.03.K1.010
13. Texas A&M University-Kingsville Procedure 29.01.04.K1.010
14. Texas Government Code, Section 441