29.01.99.K1.180 Server Hardening Standards

Effective: April 1st, 2004
Revised: April 25th, 2013
Revised: April 2019
Next Scheduled Review: April 2024

Introduction

Servers are depended upon to deliver applications and 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 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.

Audience

This standard 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 Standard

1. A server must not be connected to the University network until it is in a secure state approved by iTech.
2. The Server Hardening Standard provides the detailed information required to harden a server and must be performed for iTech approval. Some of the general steps included in the Server Hardening Standard include:
    a. Installing the operating system from an iTech approved source which includes proper licenses.
    b. Applying vendor supplied operating system and 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
h. Setting up encrypted remote access if needed

3. Vulnerability assessments will be performed in accordance with the Vulnerability Assessment Procedures.
    a. Network/operating system vulnerabilities identified as high or medium risk must be corrected within the specified timeframe.
4. Violations of this standard must be reported to the Information Security Officer.

Disciplinary Actions

Violation of this standard may result in disciplinary action up to and including termination for employees and temporaries; a termination of contract 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. Computer Fraud and Abuse Act of 1986
2. Computer Security Act of 1987
3. DIR Standards Review and Recommendations Publications
4. DIR Practices for Protecting Information Resource Assets
5. IRM Act, 2054.075(b)
6. The State of Texas Information Act
7. The State of Texas Penal Code, Chapters 33 and 33A
8. Texas Administrative Code, Chapter 202
9. Texas A&M University-Kingsville Acceptable Use Procedure 29.01.99.K1.010
10. Texas Government Code, Section 441

Contact Office

For More Information, Contact: iTech
MSC 185, 700 University Blvd., Kingsville, TX 78363-8202
Contact Phone: 361-593-2404