29.01.99.K1.175 New Server Standard Administrative Procedure

Effective: April 1st, 2004
Revised: April 25th, 2013
Revised: July 8th, 2019
Next Scheduled Review: July 2024

Introduction

Servers at Texas A&M University-Kingsville (TAMUK) are depended upon to deliver data in a secure, reliable fashion. There must be assurance that data confidentiality, integrity and availability are maintained. One of the required steps to attain this assurance is to ensure that the servers are in compliance with 1_180_Server Hardening Procedure to prevent unauthorized access, unauthorized use, and disruptions in service.

Servers at TAMUK play an important role in the delivery of critical data to students, faculty, staff, and the public. To this end, controls must be in place to protect the confidentiality, integrity, and availability of the data housed on these servers. Technical, Managerial, and Operational controls work together to assure that new servers are installed and configured in such a manner to emphasize security and minimize service disruptions.

Purpose

The purpose of this procedure is to outline and collectively define the University's required server base configuration.

Audience

This procedure applies to individuals that are responsible for the installation of new servers at TAMUK.

New Server Procedure

1. All servers connected to the TAMUK network must meet the server hardening requirements outlined in the 1_180 Server Hardening Procedure.

2. Servers which process, transmit, or store confidential or sensitive data may have additional requirements.
3. All server purchases must be approved by iTech.
4. Once a new server has been configured to meet the university required hardening standards, the information resource owner will submit a Helpdesk ticket to request a static IP.
5. Prior to a new server entering production status, a security scan of the system must be completed by iTech. Identified risks will be communicated to the system administrator and must be corrected or justified.

Disciplinary Actions

Violation of this procedure 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. Copyright Act of 1976
2. Computer Fraud and Abuse Act of 1986
3. Computer Security Act of 1987
4. DIR Practices for Protecting Information Resources Assets
5. DIR Standards Review and Recommendations Publications
6. Foreign Corrupt Practices Act of 1977
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 Acceptable Use Procedure 29.01.99.K1.010
14. 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