29.01.99.K1.165 Firewall Standard

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

Introduction

Firewalls are an essential component of information systems security infrastructure at Texas A&M University-Kingsville (TAMUK). Firewalls are defined as security systems that control and restrict both Internet connectivity and Internet services. Firewalls establish a perimeter where access controls are enforced.

Purpose

The purpose of this standard is to define the essential rules regarding the management and maintenance of firewalls at TAMUK and it applies to all firewalls owned, rented, leased, or otherwise controlled by TAMUK.

Audience

This standard applies to individuals that install, operate or maintain TAMUK Information Resources.

Firewall Standard

1. The Information Security Officer (ISO) is responsible for ensuring the implementation of the requirements of the Firewall Standard.

2. All firewalls at TAMUK must follow the following:
    a. Inbound Traffic - Default To Deny All
        i. In-bound connections to TAMUK internal networks must pass through a firewall before allowing any type of connection. Any incoming service not specifically allowed in the firewall rule set will be automatically denied. Permission to enable any other paths or services will be granted by the ISO only when the paths are necessary for valid business or academic reasons.

b. Outbound Traffic – Default to Allow All
    i. Outbound-bound connections from TAMUK internal networks must pass through a firewall before being routed to any external network or the Internet. By default, all outbound traffic will be allowed except in cases where the protocols or services involved are deemed to be a threat to the Internet community or does not conform to generally accepted best practices.

c. Firewall Change Control
    i. Firewall rule changes must comply with the University Change Management Procedure and require ISO or designee approval. Additionally, all rule sets must be reevaluated on a biennial basis in conjunction with the campus risk assessment in order to determine if a particular rule is still needed.
    ii. All changes to firewall configuration parameters, enabled services, and permitted connectivity must be logged.
d. Firewall Physical Security
    i. All TAMUK firewalls must be located in secured areas accessible only to those who require physical access to perform the tasks assigned by management.

3. Penetration Testing
    a. Penetration testing must be performed on an annual basis on all outward facing firewalls.
4. System Logs
    a. All suspicious activity which might be an indication of unauthorized usage or an attempt to compromise security measures must be logged. These logs must be reviewed periodically to ensure that the firewalls are operating in a secure manner.

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 Practices for Protecting Information Resources Assets
4. DIR Standards Review and Recommendations Publications
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 29.01.03.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