Firewall Procedure

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. Connectivity defines which computer systems can exchange information. A service is sometimes called an application, and it refers to the way that information flows through a firewall. Firewalls establish a perimeter where access controls are enforced. Examples of services include FTP (file transfer protocol) and HTTP (web browsing).

Purpose
The purpose of this procedure 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 procedure applies to individuals that install, operate or maintain TAMUK Information Resources.

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

All firewalls at TAMUK must follow the following:

- **Inbound Traffic - Default To Deny All**
  - 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 reasons.

- **Outbound Traffic – Default to Allow All**
  - 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.

- **Firewall Dedicated Functionality**
  - Firewalls used to protect TAMUK’s internal data center networks must run on dedicated devices.

- **Firewall Change Control**
  - Firewall rule changes must comply with the University Change Management Procedure and require ISO 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.

- **Penetration Testing**
  - Firewalls provide an important barrier to unauthorized access to TAMUK networks and must be penetration tested on an annual basis. These tests must also include the regular execution of vulnerability identification software.

- **System Logs**
  - All changes to firewall configuration parameters, enabled services, and permitted connectivity must be logged. 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.

- **Firewall Physical Security**
  - All TAMUK firewalls must be located in secured areas accessible only to those who require physical access to perform the tasks assigned by management.

**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