1. **Introduction**

Firewalls are an essential component of Texas A&M University-Kingsville's information systems security infrastructure. 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).

2. **Scope**

This policy defines the essential rules regarding the management and maintenance of firewalls at Texas A&M University-Kingsville and it applies to all firewalls owned, rented, leased, or otherwise controlled by Texas A&M University-Kingsville.

3. **Policy Statement**

All firewalls at Texas A&M University-Kingsville must follow this policy.

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

In-bound connections to Texas A&M University-Kingsville 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 Information Security Officer (ISO) only when the paths are necessary for valid business reasons.

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

Outbound-bound connections from Texas A&M University-Kingsville 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.

3.3. **Firewall Dedicated Functionality**

Firewalls used to protect Texas A&M University-Kingsville’s internal data center networks must run on dedicated devices.

3.4. **Firewall Change Control**

Firewall rule changes must comply with the university change management policy 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.

3.5. **Penetration Testing**

Firewalls provide an important barrier to unauthorized access to Texas A&M University-Kingsville networks and must be penetration tested on an annual basis. These tests must also include the regular execution of vulnerability identification software.

3.6. **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.

3.7. **Firewall Physical Security**

All Texas A&M University-Kingsville firewalls must be located in secured areas accessible only to those who require physical access to perform the tasks assigned by management.

4. **Responsibilities**

The Information Security Officer is responsible for ensuring the implementation of the requirements of the Firewall policy.

5. **Disciplinary Actions**

Employees who violate this policy will be subject to disciplinary action up to and including termination of employment. Anyone who knows or has reason to believe that another person has violated this policy should report the matter promptly to his or her supervisor or the Information Security Officer. All reported matters
will be investigated, and, where appropriate, steps will be taken to remedy the situation. Where possible, every effort will be made to handle the reported matter confidentially. Any attempt to retaliate against a person for reporting a violation of this policy will itself be considered a violation of this policy that may result in disciplinary action up to and including termination of employment.