Procedure Statement

Firewalls not only prevent unauthorized access to or from a private network, but are a fundamental element of the University’s information systems security infrastructure. Firewalls regulate and control network connectivity and necessary Internet services such as web browsing, mail services, and file transfers. Firewalls establish a perimeter where access controls are enforced.

Reason for Procedure

This Procedure applies to all users of Texas A&M University-San Antonio (A&M-San Antonio) information resources.

The purpose of the implementation of this Procedure is to provide a set of measures that will mitigate information security risks associated with firewall management. There may be other or additional measures that division or department heads will provide to further mitigate risks. In accordance with Texas Administrative Code 202 - Information Security Standards, each department and/or resource owner may elect not to implement some or all of the risk mitigation measures provided in this Procedure based on documented and approved information security risk management decisions and business functions. Such risk management decisions must be documented and approved by the designated Information Security Officer (ISO).

Official Responsibilities and Procedure

1. All A&M-San Antonio Internet access will be consolidated and provided through a perimeter firewall and a centralized information technology infrastructure. Individual divisions, departments, and/or colleges should not establish independent Internet connectivity outside of the centralized information technology infrastructure. All requests for independent Internet connectivity will be directed to Information Technology Services (ITS) and must be approved by the Information Resources Manager (IRM).
2. The ISO will be responsible for providing guidance and direction for A&M-San Antonio firewall architecture, inbound/outbound protocols, traffic monitoring, and approval of any updates or changes to firewall rules. Enforcement of firewall and DMZ rules is the responsibility of the ISO.

3. ITS is responsible for monitoring and configuration of all firewall rule sets. The A&M-San Antonio ISO is responsible for enforcing all applicable firewall policies. The ISO shall coordinate with the State of Texas Department of Information Resources (DIR) or approved vendor to conduct annual controlled penetration testing and web server application vulnerability assessments. Formal reports generated from these tests will be delivered to the IRM. All corrections and enforcement of changes will be coordinated by the ISO.

4. All A&M-San Antonio perimeter firewalls shall be hardware appliances that provide a separate layer of architecture between the internal and external network. Perimeter firewalls shall be redundant and configured in an active/failover topology.

5. All A&M-San Antonio firewalls must be located in a secure location with controlled and monitored access.

6. The A&M-San Antonio perimeter firewall permits all outbound (egress) and inbound (ingress) traffic to Internet services with the exception of network traffic that violates A&M-San Antonio policy, state, and/or federal laws. Network traffic that contains unauthorized services, viruses, worms, or other malware may be blocked at any time to protect the integrity and reputation of A&M-San Antonio.

7. Alarm and alert functions as well as audit logging of any and all firewalls and/or other network perimeter access control systems shall be enabled.

8. All firewall activity shall be monitored and logged to ensure compliance with University policy, state, and/or federal laws. Additional logging devices and/or other third party inspection appliances may be used to provide further analysis and monitoring.

---

**Non-Compliance**

Violation of this Procedure may result in disciplinary action, which may include termination of employment for full-time and part-time employees; a termination of the employment relationship in the case of contractors or consultants; dismissal for interns and volunteers; or in the case of students suspension or expulsion administered based on the Code of Student Conduct. Additionally, individuals are subject to loss of access and privileges to the University information resources, civil, and/or criminal prosecution.
Related Rules

**DIR Practices for Protecting Information Resources Assets**

**Family Educational Rights and Privacy Act** (FERPA)

**Gramm Leach Bliley Act** (GLB Act)

**Health Insurance Portability and Accountability Act** (HIPAA)

**TAMU System Policy 29.01 Information Resources**

**Texas Administrative Code (TAC) 202** as amended or supplemented

**Texas Administrative Code (TAC) 202.75 Security Standards for Institutions of Higher Education**

**A&M-San Antonio Procedure 29.0103.O1.06 Backup Recovery**

**A&M-San Antonio Procedure 29.01.03.O0.01 Electronic Information Services Access and Security**

Definitions

**Accounts** - Information Resource users are typically assigned access to an information resource using logon credentials, which include, at the minimum, a unique user name and password.

**Change** – Any implementation of new functionality, any interruption of service, any repair of existing functionality, and/or any removal of existing functionality.

**Change Management** – The process of controlling modifications to hardware, software, firmware, and documentation to ensure that Information Resources are protected against improper modification before, during and after system implementation.

**Confidential Information** - Information that is excluded from disclosure requirements under the provisions of applicable state or federal law, (e.g. the Texas Public Information Act and other constitutional, statutory, judicial, and legal agreements).

**Custodian** - Guardian or caretaker (the holder of data). The agent charged with implementing the controls specified by the owner. The custodian is responsible for the processing and storage of information.
DMZ (Demilitarized Zone) - An area, a physical or logical sub-network where external facing services reside and are accessible to an untrusted network such as the Internet. Also known as a perimeter network.

Incident Report – A formal reporting of a known information technology related incident. This is performed by completing the associated ITS form.

Information Resources (IR) - The procedures, equipment, and software that are designed, employed, operated, and maintained to collect, record, process, store, retrieve, display, and transmit information or data.

Information Resources Manager (IRM) - The Information Resources Manager (IRM) oversees the acquisition and use of information technology within a state agency or university. The IRM ensures that all information resources are acquired appropriately, implemented effectively, and comply with regulations and agency policies.

Information Security Officer (ISO) - Responsible to the executive management for administering the information security functions within the agency. The ISO is the internal and external point of contact for all information security matters.

Information Technology Services (ITS) – The designated name for the central information technology department for the University.

Logon ID - A unique account name that is required as the first step in logging into a secure information resource. A logon ID typically must be associated with a user password to obtain access to the information resource.

Mission Critical Information - Information that is defined by A&M-San Antonio or information resource owner to be essential to the continued performance of the mission of A&M-San Antonio or department. Unavailability of such information would result in more than an inconvenience. An event causing the unavailability of mission critical information would result in consequences such as significant financial loss, institutional embarrassment, failure to comply with regulations or legal obligations, or closure of A&M-San Antonio or department.

Owner - The manager or agent responsible for the function which is supported by the resource; the individual upon whom responsibility rests for carrying out the appropriate use and safeguards for the resource. Where appropriate, ownership may be shared by managers of different departments.

User - An individual or automated application or process that is authorized to the resource by the owner, in accordance with the owner’s procedures and rules.

Vulnerability - A weakness or flaw in system security design, implementation, procedures or controls that can cause a violation of the system’s security policy or a security breach if exploited by an attacker.
Contact Office

Finance and Administration, Information Technology Services (210) 784-4357 (HELP)