Sam Houston State University
A Member of The Texas State University System
Information Technology (IT)

Firewall Policy: IT-21

PURPOSE:

The purpose of this policy is to protect Sam Houston State University's (SHSU) information resources by implementing boundary protections to restrict network access to and from these resources. It is designed to prevent the loss of sensitive confidential data, intellectual property, and damage to public image which may follow from unauthorized use of SHSU's information resources. SHSU operates external firewalls or gateways between the Internet and the SHSU network to establish a secure environment for the University's information resources.

SHSU's firewalls are key components of the university's network security architecture. The Firewall Policy governs how the firewalls filter traffic to mitigate security threats to SHSU's information resources.

SCOPE:

The Firewall Policy applies to all firewall devices owned and/or operated by SHSU.

POLICY STATEMENT:

1. Perimeter firewalls must deny inbound and outbound traffic by default except for that traffic which is explicitly permitted in the following cases:

    a. *Outbound* - Any Internet traffic to hosts and services outside SHSU's networks except those specifically identified and blocked as malicious sites.
    b. *Inbound* - Appropriate Internet traffic that supports the mission of the institution and is in accordance with defined system, application, and service procedures.

2. Firewall filters may also be put in place to:

    a. protect outbound bandwidth to ensure network service for all SHSU information resources; and
    b. prevent users from both knowingly or unknowingly attacking other information systems.

3. Internal firewalls shall be put in place to establish secure communications between different segments of the University's network where different levels of security are warranted.

4. Information system owners and custodians responsible for implementing,

configuring, and maintaining firewalls on SHSU information resources are responsible for the following activities:

a. Firewalls must be tested and reviewed at least once per year.
b. When there are major changes to the network requirements, firewall security policies will be reviewed and changed as appropriate.
c. Firewalls must have alert capabilities and supporting procedures.
d. Auditing must be active to permit analysis of firewall activity.

REFERENCE:

There are many individual laws, regulations, and policies that establish our information security requirements. While it is not possible to list all potentially applicable laws and regulations, the most relevant are listed in the Texas State University System (TSUS) Rules and Regulations, Rule III Paragraph 19 and associated TSUS IT Policies.

Version 1.02
Approved by: President's Cabinet, February 6, 2012
Reviewed by: Heather Thielemann, Information Resources Manager, May, 2023
Next Review: May, 2024