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

Firewall Policy: IT-21

PURPOSE:

SHSU operates external firewalls or gateways between the Internet and the SHSU network to establish a secure environment for the university's information technology resources. Internal firewalls are in place to establish secure communications between different segments of the University's network where different levels of security are warranted.

SHSU's firewalls are key components of the university's network security architecture. The Firewall Policy governs how the firewalls will filter traffic to mitigate the risks and losses associated with security threats to SHSU's information technology resources. This policy will attempt to balance risks incurred against the need for access.

The purpose of this policy is to protect SHSU's information technology resources from hacking and virus attacks by restricting access to information technology resources on the University campus. It is designed to minimize the potential exposure of SHSU to the loss of sensitive confidential data, intellectual property, and damage to public image which may follow from unauthorized use of SHSU's information technology resources.

SCOPE:

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

POLICY STATEMENT:

Perimeter Firewalls:

The perimeter firewall permits the following outbound and inbound Internet traffic:

- *Outbound* - All Internet traffic to hosts and services outside SHSU's networks except those specifically identified and blocked as malicious sites.
- *Inbound* - Allow Internet traffic that supports the mission of the institution and is in accordance with defined system, application and service procedures.
- *Outbound/Inbound* – All internet traffic detected as malicious by the university's intrusion prevention system (IPS) and/or all traffic violating SHSU firewall policies is dropped.

Reason for filtering ports:

- Protecting SHSU Internet Users - Certain ports are filtered to protect SHSU information technology resources. The perimeter firewall protects against certain common worms and from dangerous services on SHSU information technology resources that could allow intruders access.

- Protecting our outbound bandwidth - If SHSU Internet users overuse their outbound bandwidth by running high-traffic servers or by becoming infected with a worm or virus, it can degrade the service of other SHSU systems.
- Protecting the rest of the Internet - Some filters prevent users from both knowingly or unknowingly attacking other computers on the Internet. In addition to being in SHSU's interests for protecting our bandwidth, it is the institutions' responsibility to prevent abuse of its network.

Roles and Responsibilities:

The Information Security Office is responsible for implementing, configuring and maintaining SHSU's firewalls and for activities relating to this policy.

1) At a minimum, firewalls must be annually tested and reviewed.
2) When there are major changes to the network requirements, firewall security policies will be reviewed and may warrant changes.
3) Firewalls must have alert capabilities and supporting procedures.
4) Auditing must be active to permit analysis of firewall activity.

Related Policies, References and Attachments:

An index of approved IT@Sam policies can be found on the SHSU Information Technology Services Policies website at http://www.shsu.edu/intranet/policies/information_technology_policies/index.html. Reference materials, legal compliance guidelines, and policy enforcement are available in the IT-00 Policy Compliance Document. The SHSU Information Security Program and SHSU Information Security User Guide are also available on the Information Technology Services Policies website.

Reviewed by: Mark C. Adams, Associate VP for Information Technology, January 19, 2012
Approved by: President's Cabinet, February 6, 2012
Next Review: November 1, 2015