STANDARD ADMINISTRATIVE PROCEDURE

29.01.99. S1.33 Information Resources – Firewalls

Approved
Next scheduled review:

Standard Administrative Procedure Statement

A firewall is the first line of defense against unauthorized or malicious access to System Office (SO) information resources. It is of significant importance to ensure that firewalls protecting SO information resources are correctly configured. This Standard Administrative Procedure provides users information on where to find expert guidance for administering both host-based and departmental firewalls.

Definitions

Firewall - a software or hardware device or system that filters communications between networks that have different security domains based on a defined set of rules. A firewall may be configured to deny, permit, encrypt, decrypt, or serve as an intermediary (proxy) for network traffic.

Host-based firewall - software that functions on a single host (i.e., a single computer including laptop computers) that can permit or deny incoming or outgoing traffic to or from only that host (as opposed to a network-based firewall which protects one or more networks of hosts).

Official Procedure/ Responsibilities/ Process

1. APPLICABILITY

This Standard Administrative Procedure (SAP) applies to all firewalls owned, rented, leased, or otherwise needed by SO network users.

2. RESPONSIBILITIES

Users of the System Office system who operate firewall technology on System Office owned information resources are responsible for following the procedures described herein. System Office users shall operate firewall technology with instruction and guidance from security employees with University Network and Information Systems
(NIS). The NIS security team is authorized to disconnect users from the internet if these procedures are not followed.

Security team members assigned to NIS are responsible for providing specific guidance and direction in the following areas:

2.1 Virtual and physical architecture;

2.2 Protocols and applications that are permitted through the firewall, both inbound and outbound;

2.3 Traffic monitoring rule set;

2.4 Approval process for updating or changing rule sets; and,

2.5 Auditing and testing to verify a firewall’s configuration, rule set accuracy, and effectiveness.

3. GUIDELINES

For detailed guidelines refer to: Firewalls

______________________________________________________________

Related Statutes, Policies, or Requirements

1 Texas Administrative Code, Ch. 202, Subchapter C

Rule 29.01.99.S1 Security of Electronic Information Resources

______________________________________________________________

Contact Office

For interpretation and clarification contact The Texas A&M University System Chief Information Officer

OFFICE OF RESPONSIBILITY: The Texas A&M University System Chief Information Officer