Texas A&M Health Science Center Guidelines

29.01.03.Z1.21 Guideline: Firewall

Approved February 13, 2013

Supplements System Regulation 29.01 and TAMU SAP 29.01.03.M1.33

Reason for the Guidelines

Firewalls not only prevent unauthorized access to or from a private network, but are a fundamental element of the Texas A&M University Health Science Center (HSC) information systems security infrastructure. Firewalls regulate and control Internet connectivity and necessary Internet services such as web browsing, mail services, and file transfers. Firewalls establish a perimeter where access controls are enforced. The HSC Firewall guideline applies equally to all individuals with access to any HSC information resource.

1. Firewall

1.1 Internet access at university locations will be consolidated and provided through the Office of Information Technology (OIT). Individual divisions, departments, and/or colleges will not be permitted to establish independent Internet connectivity outside of the HSC. All requests for Internet access will be directed to OIT.

1.2 The network services manager is primarily responsible for the monitoring and configuration of all firewall rule sets. The Information Security Officer (ISO) is responsible for enforcing all applicable firewall policies. The ISO shall also coordinate regular controlled penetration testing and web application vulnerability assessments.

1.3 All university perimeter firewalls shall be independent hardware appliances.

1.4 All HSC firewalls must be located in a locked room accessible only to those who must have physical access to such firewalls to perform the tasks associated with firewall management. The placement of firewalls in open and unsecured areas is strictly prohibited. All physical security policies shall be enforced in regards to firewalls.

1.5 The university perimeter firewall permits all inbound and outbound Internet traffic to access Internet services outside of the university, with the exception of network traffic that violates university policy, state, and/or federal laws.
1.6 All updates and/or changes to firewall configuration parameters and services must be approved by the network services manager, ISO, or the Information Resources Manager (IRM).

1.7 All external facing servers must be on the HSC Demilitarized Zone (DMZ) for security purposes. If the server cannot be moved to the DMZ, then that server must be accessed through a security proxy.

2. Violations

Violations of this policy may result in disciplinary action, which may include termination for employees and temporary workers; a termination of employment relations in the case of contractors or consultants; dismissal for interns and volunteers; or suspension or expulsion in the case of a student. Additionally, individuals are subject to loss of HSC information resources access privileges, civil, and criminal prosecution.

OFFICE OF RESPONSIBILITY:

Vice President for Finance and Administration