Firewall Operational Standards and Procedures

Area: Information Technology Services	Number:	
Subject: Firewall Management	Issued:	8/1/2012
Applies To: University	Revised:	
Sources:	Updated:	
	Reviewed:	
Responsible Party: Vice President for Information Technology	Page(s):	Page **1** of **3**

I. Purpose

This standard defines the essential rules regarding the management and maintenance of firewalls at Georgia Southern University and it applies to all firewalls owned, rented, leased, or otherwise controlled by Georgia Southern University employees.

II. Policy Statement

1.0. INTRODUCTION

Firewalls are an essential component of Georgia Southern University's information systems security infrastructure. Firewalls are defined as security systems that control and restrict both network connectivity and network services. Firewalls establish a perimeter where access controls are enforced and subsequently define how a network service is utilized. Examples of services include FTP (file transfer protocol) and HTTP (web browsing).

2.0. SCOPE

This standard defines the essential rules regarding the management and maintenance of firewalls at Georgia Southern University and it applies to all firewalls owned, rented, leased, or otherwise controlled by Georgia Southern University employees.

3.0. STANDARD STATEMENT

All firewalls at Georgia Southern University must follow the following standards. Departures from this standard will be permitted only if approved in advance and in writing by the CIO or his/her designee

3.1. Perimeter Firewalls

Perimeter Firewall(s) will allow access to the following for outbound and inbound network traffic:

3.1.1 Outbound: Allow ALL network traffic to hosts and services outside of the perimeter.

3.1.2 Inbound: Only secure applications and specific services which support the Georgia Southern University mission will be allowed access from the perimeter.

3.1.3 Any secure application or specific service will be restricted to a specific outside IP address (es) unless approved otherwise by IT services.

3.1.4 Every network connectivity path and network service not specifically permitted by this standard (and supporting documents issued by Information Technology Services (ITS)) must be blocked by University firewalls. Likewise, every network connectivity path not specifically permitted by the IT Services must be denied by firewalls. Prior to the deployment of any University firewall, permission to enable any firewall will be granted by the CIO or his/her designee only when (1) the device is necessary for important business reasons, and (2) sufficient security measures will be consistently employed.

3.2. Host Based Firewalls

For Microsoft Windows, Mac OS X, or Linux/Unix devices for which host-based firewall software is available, host-based firewall software must be running and configured to block all inbound traffic that is not explicitly required for the intended use of the device. Use of a network-based firewall does not obviate the need for host-based firewalls.

3.3. External Connections

All in-bound real-time external connections to University internal data center networks must pass through a firewall.

3.4. Firewall Dedicated Functionality

Firewalls used to protect the University's internal data center networks must run on dedicated devices. These devices may not serve other purposes, such as act as web servers.

3.5. Firewall Change Control

Firewall configuration rules and permissible services rules must not be changed unless the permission of the CIO or his/her designee has first been obtained.

3.6. Regular Auditing

Because firewalls provide such an important barrier to unauthorized access to Georgia Southern University networks, they must be audited on a regular basis. At a minimum, this audit process must include consideration of defined configuration parameters, enabled services, permitted connectivity, current administrative practices, and adequacy of the deployed security measures. These audits must be performed by technically proficient persons other than those responsible for the administration of the involved firewalls.

3.7. Logs

All changes to firewall configuration parameters, enabled services, and permitted connectivity must be logged. In addition, all suspicious activity which might be an indication of unauthorized usage or an attempt to compromise security measures must also be logged. The integrity of these logs must also be protected with checksums, digital signatures, encryption, or similar measures. These logs must be promptly removed from the recording

systems and stored in a physically protected container for at least six months after the time they were recorded. These logs must be reviewed periodically to ensure that the firewalls are operating in a secure manner.

3.8. Firewall Physical Security

All Georgia Southern University firewalls must be located in locked rooms accessible only to those who must have physical access to such firewalls to perform the tasks assigned by management. These rooms must have environmental alarms as well as an automated log of all who gain entry to the room.

4.0. RESPONSIBILITIES

The CIO or his/her designee is responsible for ensuring the implementation of the requirements of the Firewall standard. Employees who violate this standard will be subject to disciplinary action up to and including termination of employment.

5.0 ACCESS CONTROL

The following table shows the most common services for Internet communication. This list is not exhaustive.

Services	VPN (via Internet) to GSNet	Internet to GSNet Enabled	Notes
Email	Yes	Must be requested; must be approved by IT	Pop, SMTP, Imap / only authorized email servers
Web hosting	N/A	Must be requested; must be approved by IT	includes HTTP and HTTPS (SSL)
FTP	Yes	No	must use Secure FTP
Telnet	No	No	must use SSH
SSH	Yes	Must be requested; must be approved by IT	required use
Streaming media (Audio/Video)	Yes	Must be requested; must be approved by IT	Audio, video, H323, IP Video
Remote Management	Yes	No	PCAnywhere, Timbuktu, VNC, etc. are required to use university VPN
other access	Yes	Must be requested; must be approved by IT	these will be evaluated on a case by case basis