



TULANE UNIVERSITY FIREWALL POLICY

Department: Technology Services	Policy Description: Firewall
Approved: 01-01-2006	Revised:
Effective Date: 01-01-2006	Policy Number: TS-001

1.0. INTRODUCTION

Firewalls are an essential component of Tulane University's information systems security infrastructure. Firewalls are defined as security systems that control and restrict both Internet connectivity and Internet services. Firewalls establish a perimeter where access controls are enforced. Connectivity, as the word is used here, defines which computer systems can exchange information. A service, as the word is used here, is sometimes called an application, and it refers to the way for information to flow through a firewall. Examples of services include FTP (file transfer protocol) and HTTP (web browsing).

2.0. SCOPE

This policy defines the essential rules regarding the management and maintenance of firewalls at Tulane University and it applies to all firewalls owned, rented, leased, or otherwise controlled by Tulane University workers.

3.0. POLICY STATEMENT

All firewalls at Tulane University must follow this policy. Departures from this policy will be permitted only if approved in advance and in writing by both the Information Security Officer and the Director of Network Services.

3.1. Default To Deny All

Every Internet connectivity path and Internet service not specifically permitted by this policy (and supporting documents issued by the Technology Services Department) must be blocked by Tulane University firewalls. The list of currently approved services must be documented and distributed to all systems administrators with a need-to-know by the Technology Services Department. Likewise, every network connectivity path not specifically permitted by the Technology Services Department must be denied by firewalls. Prior to the deployment of every Tulane University firewall, a diagram of permissible paths with a justification for each must be submitted to the Technology Services Department. Permission to enable any paths will be granted by both the Information Security Officer and the Director of Network Services only when (1) the paths are necessary for important business reasons, and (2) sufficient security measures will be consistently employed.

3.2. External Connections

All in-bound real-time external connections to Tulane University internal data center networks must pass through a firewall before users can reach a log-in banner.

3.3. Firewall Dedicated Functionality

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

3.4. Firewall Change Control

Firewall configuration rules and permissible services rules have been reached after an extended evaluation of costs and benefits. These rules must not be changed unless the permission of both the Information Security Officer and the Director of Network Services have first been obtained.

3.5. Regular Auditing

Because firewalls provide such an important barrier to unauthorized access to Tulane 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 also include the regular execution of vulnerability identification software. These audits must be performed by technically proficient persons other than those responsible for the administration of the involved firewalls.

3.6. 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.

3.7. Firewall Physical Security

All Tulane 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. The placement of firewalls in the open area within a general purpose data processing center is prohibited, although placement within separately locked rooms or areas which themselves are within a general data processing center is acceptable. These rooms must have burglar alarms as well as an automated log of all who gain entry to the room.

4.0. RESPONSIBILITIES

The Information Security Officer is responsible for ensuring the implementation of the requirements of the Firewall policy.

Employees who violate this policy will be subject to disciplinary action up to and including termination of employment. Anyone who knows or has reason to believe that another person has violated this policy should report the matter promptly to his or her supervisor or the Information Security Officer. All reported matters will be investigated, and, where appropriate, steps will be taken to remedy the situation. Where possible, every effort will be made to handle the reported matter confidentially. Any attempt to retaliate against a person for reporting a violation of this policy will itself be considered a violation of this policy that may result in disciplinary action up to and including termination of employment.