



Information Technology Services Policy

Title: ITS Network Firewall Policy

Created: September 04, 2008

Author: E. Decker

Version: 1.0

Scope:

This policy defines the essential rules regarding the management, maintenance and operation of network firewalls at Loyola University Chicago and applies to all network firewalls procured through, operated or contracted by the University.

Purpose:

To establish a set policies and strategies in the deployment and configuration of all network firewalls that process University network traffic.

Policy:

Network Connections

All external and wireless connections to University networks must pass through a network firewall. In addition, all network connections entering a high security network must pass through a network firewall. Any change to an external connection or to the configuration of the firewall must be adequately tested and documented according to the [ITS Network Firewall Standard](#).

Dedicated Functionality

Network firewalls used to protect University networks must run on single-purpose devices.

- These devices may not serve other purposes, such as acting as web servers.
- Each network firewall must have a rule set specific to its purpose and location on the network, in accordance with the [ITS Network Firewall Standard](#).

Network Firewall Change Control

Network firewall configuration rules and permissible services rules must not be changed unless the permission of the Information Security Officer and Network Manager has first been obtained. Any change made to any network firewall needs to be documented using the [ITS Change Management System Procedures](#), and a justification for the change and the actual updated configuration or service rule needs to be documented in the [ITS Network Firewall Supporting Documentation](#).

Regular Auditing

An audit of network firewalls will be done on a quarterly basis. These audits must also include the regular execution of vulnerability scanning in accordance with the [ITS Vulnerability Assessment Policy](#). Audits must be performed by the Information Security Team.

Network Firewall Physical Security

All University network firewalls must be physically located in ITS data centers and accessible only to those whose roles and responsibilities permit them to access network firewalls as defined within the [ITS Access Control Policy](#).

These secure spaces must also have adequate physical security measures installed. All physical access to the secured spaces will be automatically logged. All visitor access to the secured space must abide by the [ITS Access Control Policy](#).

Exceptions:

Exceptions to this policy will be handled in accordance with the [ITS Security Policy](#).

Review:

This policy will be maintained in accordance with the [ITS Security Policy](#).

Emergencies:

In emergency cases, actions may be taken by the Incident Response Team in accordance with the procedures in the [ITS Incident Response Handbook](#). These actions may include rendering systems inaccessible.

Appendix

Documents Referenced

Change Management System Procedures
ITS Access Control Policy
ITS Network Firewall Supporting Documentation
ITS Network Firewall Standard
ITS Incident Response Handbook
ITS Security Policy