Network Firewall Policy

Policy Title:
Network Firewall Policy

Responsible Executive(s):
Jim Pardonek, Director and Chief Information Security Officer

Responsible Office(s):
University Information Security Office

Contact(s):
If you have questions about this policy, please contact the University Information Security Office.

I. Policy Statement

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. In addition, please note that this policy covers all IoT devices.

II. Definitions

Not applicable.

III. 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 an additional 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 Chief Information Security Officer and Network Manager has first been obtained. Any change to rules and permissible services made to any network firewall needs to be documented using the ITS Change Management Policy, 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. Changes made to Intrusion Prevention functions of the Internet facing firewalls (See Allowable Changes) are an exception and do not require a change management request.

Allowable Changes (External Facing Firewalls Only)

The following list of changes do not require a change management request:

- Security Profiles (Antivirus, Anti-Spyware, Vulnerability Protection, URL Filtering, File Blocking, Wildfire Analysis, Data Filtering, and DoS protection)
- Zone Protection
- Log Forwarding
- VPN

Regular Auditing

An audit of network firewalls will be done on a biannual 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 and Network Services.

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.

IV. Related Documents and Forms

Not applicable.

V. Roles and Responsibilities

Jim Pardonek, Director and Chief Information Security Officer	Enforcing the Network Firewall Policy at the University by setting the necessary requirements

VI. Related Policies

Please see below for additional related policies:

- Security Policy
- ITS Access Control Policy
- ITS Network Firewall Standard
- Incident Response Plan
- ITS Security Policy

Approval Authority:	ITESC	**Approval Date:**	August 11th, 2017
Review Authority:	Jim Pardonek	**Review Date:**	June 14th, 2024
Responsible Office:	UISO	**Contact:**	datasecurity@luc.edu