Firewall Policy

1.0 Purpose

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

2.0 Scope

This policy defines the essential rules regarding the management, maintenance and operation of all network firewalls owned, rented, leased, or otherwise controlled by Lawrence Technological University.

3.0 Policy Statement

All network firewalls at Lawrence Technological University must follow this policy. Departures from this policy will be permitted only if approved in advance and in writing by the Executive Director of Information Technology Services.

Network Connections

All external connections to University networks must pass through a network firewall.

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.

Change Control

Rules will be updated as new services are introduced and when existing services expire. Rules are reviewed against current best practices and current Lawrence Technology University needs. All changes to the University firewalls must go through the Change Control process.

Auditing

Because firewalls provide such an important barrier to unauthorized access to Lawrence Technological University networks, they must be audited on a periodic 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 should also include the regular execution of vulnerability identification software. These audits must be performed by technically proficient outside company rather than those responsible for the administration of the involved firewalls.

Physical Security

All University network firewalls must be physically located in EDCC data centers and accessible only to those whose roles and responsibilities permit them to access network firewalls. These secure spaces must also have adequate physical security measures installed.
Logs

All suspicious activity which might be an indication of unauthorized usage or an attempt to compromise security measures must also be logged. These logs must be reviewed periodically to ensure that the firewalls are operating in a secure manner.

Responsibility

The Edward Donley Computer Center (EDCC) staff of the Information Services department is responsible for installing, managing, monitoring and auditing of all firewalls connected to the Lawrence Technology University production network. Information Technology Services reserves the right to remove any firewall connected to the Lawrence Technological University production network that was not installed by the EDDC staff.