Network Firewall Standard

Applies To:	All	Policy Number:	ITS-0039
Issued By:	AVP for IT	Policy Version Number:	1.0
Date Issued:	July 1, 2016	Last Review Date:	July 1, 2016
		Last Revised Date:	July 1, 2016

Scope
These standards cover the configuration of University's network firewalls.

Purpose
To establish a uniform set of standards for implementing and maintaining established network firewall policies. Including, but not limited to, defining network security zones within the University's network and the type and nature of traffic which will be allowed or denied access to those zones. Also, to maintain the stability of the network and increase the security for identified resources.

Standard
Ownership and Responsibility
All equipment and applications within this scope will be administered by Network Services.

Network Security Zones
A set of clearly defined network zones, with different levels of security requirements, built to provide the proper secure levels of networking access to the University community.

- *Detroit Mercy DMZ*
  A semi-restrictive network, or group of networks, whose purpose is to publish content for public and/or Internet consumption. This zone contains a mix of ITS and Academic resources.
- *Detroit Mercy Campus*
  A semi-restrictive network, or group of networks, which contain the majority of the University's network traffic whose purpose is to provide internal and external connectivity to network and system resources as well as the Internet.
- *Management Network*
  A restricted network that contains ITS network devices, such as network firewalls, routers, switches and managing servers, used in providing and controlling access to University's network.
- *Backup Network*
  A restricted network that contains ITS network devices exclusively configured to support connectivity to the University's backup systems.
- *High Security DMZ*

A restricted access network, or group of networks, whose purpose is to publish high security content for public and/or Internet consumption. This zone will contain ITS resources that serve as an interface for the protected, mission critical systems. Only traffic that has previously been justified will be allowed to enter and leave this security zone.

- *High Security Internal*
  A highly restricted network, or group of networks, whose purpose is to protect the University's mission critical resources. This security zone will store, transmit or process University Protected and Sensitive data (see Data Classification section of the Acceptable Use & Security Policy). Only traffic that has previously been justified will be allowed to enter and leave this security zone.

Firewall Ruleset

Each network security zone shall have a different set of access restrictions applied to them, ranging from least restrictive to most restrictive. The ruleset for each network security zone is located in the ITS Network Firewall Supporting Documentation.

All ports opened within either of the High Security DMZ, High Security Internal and the Management Network zone must have accompanying justification, documented within ITS Network Firewall Supporting Documentation.

Administrative Access

All administrative access to the University network firewalls will be governed by the following rules:

- All administrative users must authenticate via RADIUS. A backup administrator account shall be used only for console access.
- All administrative access shall be encrypted, at a minimum, via the following methods: SSHv2, AES 128 bit or 3DES 128 bit.
- All administrative access shall be restricted to networks and hosts as identified in the ITS Network Firewall Supporting Documentation.
- Each network firewall will present the following login banner when a user logs in to the device:
- "UNAUTHORIZED ACCESS TO THIS NETWORK DEVICE IS PROHIBITED. You must have explicit permission to access or configure this device. All activities performed on this device may be logged, and violations of this policy may result in disciplinary action in accordance with the appropriate handbook, and may be reported to law enforcement. There is no right to privacy on this device."

Logging

All network firewalls will be configured to use the syslog protocol for system log transport, and abide by the audit and logging strategy based on the ITS Log Management Standard.

Addressing

No private address, as defined in RFC 1918, shall ever be routed to the Internet. Port Address Translation (PAT) or Network Address Translation (NAT) will be used to shield all internal address from being reveled externally.

History and Updates

July 1, 2016: Initial Policy