UMBC POLICY ON FIREWALLS
UMBC#X-1.00.04

I. POLICY STATEMENT

Firewalls are an essential component for insuring the security of critical services operating on the UMBC network This firewall policy outlines UMBC's responsibilities regarding the use and management of firewalls on the UMBC network.

II. PURPOSE FOR POLICY

The State of Maryland IT Security Policy requires all state agencies to have a firewall and develop a firewall policy that defines how the firewall rules may be adjusted. The UMBC Office of Information Technology is the entity responsible for securing the UMBC network environment. The purpose of this policy is to establish how firewall technology is installed in the campus network and to outline the firewall change management procedures.

III. ENTITIES AFFECTED BY THIS POLICY

All academic and administrative units of the UMBC community.

IV. WHO SHOULD READ THIS POLICY

A. Information Technology Support Staff
B. Faculty and staff that wish to bypass the firewall rules.

V. CONTACTS

Direct any general questions about this University Policy – UMBC Policy Formulation and Management first to your department's administrative office. If you have specific questions, call the following offices:

Subject	Contact	Telephone / Email
Policy Clarification	Office of Information Technology	(410) 455-3208
Standard Format Information	UMBC Policy Liaison/Provost's Office	(410) 455-2333

VI. DEFINITIONS

Firewall	A firewall is a hardware or software solution to enforce security policies. In the physical security analogy, a firewall is equivalent to a door lock on a perimeter door or on a door to a room inside of the building - it permits only authorized users such as those with a key or access card to enter. A firewall has built-in filters that can disallow unauthorized or potentially dangerous material from entering the system. It also logs attempted intrusions.
Firewall Ruleset	Each of the firewall rules contains a policy, which specifies what action has to be taken when a packet matches with the rule.
Requestor	Individual responsible for specific firewall rulesets associated with a particular host on the UMBC network. Requestors assume responsibility for the rules associated with the hosts (e.g. servers, desktops) they manage.

VII. FIREWALL OVERVIEW

A. UMBC's Firewall Layers

i. **Border Firewall Protection**
A border firewall layer is the location in the network that separates the Internet, Internet2, and other external network connections from the internal campus network.

ii. **Core Network Firewall Protection**
A core network firewall layer is the location in the network that separates the major areas of the campus network. Examples of major network areas are the campus residential network, the computer room networks, and the wireless network.

iii. **Building Network Firewall Protection**
A building network firewall layer is the location in the network that separates the networks between buildings and within buildings.

iv. **Network Device Firewall Protection**
A network device firewall layer is the location in the network that separates an individual network device from the campus network.

B. Firewall Change Management

i. See **"Firewall Procedures & Guidelines"**

Policy Number: X-1.00.04
Category: Miscellaneous - IT
Responsible Administrator: Michael Carlin
Responsible Office: Division of Information Technology
Originally Issued: *DRAFT Approved* July 20, 2007
Revision Date(s):

Firewall Procedures & Guidelines

A. Default Firewall Network Rules:

a. All inbound traffic from the outside of the campus is blocked at the Border Firewall layer. People with valid UMBC accounts can access the network through the UMBC VPN service (Default Deny).
b. The UMBC Residential Network is blocked at the Core Network Layer from sending connections, to other Core Network areas, on common Microsoft Windows ports (135, 137, 139, and 445).
c. No connections are allowed into the Wireless Network and Remote Access Network at the Core Network layer.
d. The common Microsoft Windows ports are blocked between the buildings in the academic building network.
e. All outbound traffic is allowed.

B. Firewall Rule Changes

a. **Faculty and Staff:** Full-time faculty and staff members may request additional blocks or exceptions as needed. These additional blocks or exceptions can be requested in two ways:
   1. UMBC Network Administration tool is available at http://my.umbc.edu under the Services tab.
   2. The OIT Helpdesk is available at either helpdesk@umbc.edu or x53838.

C. Firewall Rule Aging

Firewall rules can be removed in three ways:

a. **Deletion** – Full-time faculty and staff members can request to have firewall rules deleted through the UMBC Network Administration Tool or the OIT Helpdesk. When a deletion request is made, the Director or a Coordinator of the Networks and Security group will consult with the original requestor to determine if the deletion of the rule will create an unacceptable security risk.

b. **Rule Renewal** – Firewall rules must be renewed every academic year or OIT will assume they are no longer needed. Renewal notices will be sent out to the requestor, via email in May, prior to the annual August 15th renewal deadline. Any machine that has not been updated by the annual August 15th renewal deadline will be sent to OIT management for review. The decision to delete rules, not renewed by the August 15th renewal date, will be assessed on case-by-case basis by OIT management.

c. **Termination of the Requestor's Account** – If the UMBC account record for a firewall rule requestor is terminated, for any reason, all rules associated with that account will be temporarily left in place. OIT management will contact individual departments to determine if the

existing rules should be deleted or if the existing rules will be assigned to a new owner who will assume responsibility.

D. Firewall Rule Modification Review

a. All firewall rule requests will be reviewed by the Director of the Networks and Security group or designee. The Director and/or a designee will evaluate the potential security risk of each rule change request. Where the risks are acceptable, OIT will work with the department to make the changes.