Title: Firewall Access Policy

1.0 Overview
All computer systems connecting to Middle Georgia State University networks are subject to access rules imposed by the firewall. These access controls are established to protect Middle Georgia State University networks from the numerous threats emanating from the Internet while allowing network activities necessary in performance of the University mission.

2.0 Purpose
To establish guidelines for firewall configuration and access requests.

3.0 Scope
All computer systems connecting to the Middle Georgia State University computer network.

4.0 Policy

In-bound connections to internal networks and systems must be controlled using a firewall.

The default inbound access policy will be deny-all. Exceptions will be made, in accordance to established standards, to support the mission of the University.

Shared file systems between internal and external systems are prohibited.

Systems requiring unrestricted public access from the Internet must be located in the DMZ.

Virtual Private Network (VPN) access is available to faculty and staff who need unrestricted access from remote locations.

Standard

Blocked services
The following services are blocked at the screening router because they are inherently dangerous.

As recommended by NIST SP 800-10 Keeping Your Site Comfortably Secure: An Introduction to Internet Firewalls, the following services are blocked inbound and outbound at the screening router.

- TFTP, trivial FTP, UDP port 69, used for booting diskless workstations, terminal servers and routers, can also be used to read any file on the system if set up incorrectly.

- RPC, Remote Procedure Call, TCP/UDP port 111, services including NIS and NFS, which can be used to steal system information such as passwords and read and write to files.

- Rlogin, rsh, and rexec, TCP ports 513, 514, and 512, services that if improperly configured can permit unauthorized access to accounts and commands.

In addition, as recommended by CERT advisory CA-2003-23 http://www.cert.org/advisories/CA-2003-23.html the following ports are blocked inbound and outbound at the screening router.

- Epmap, TCP/UDP port 135, DCE endpoint resolution.
- Netbios-ns, UDP port 137, netbios name service.
- Netbios-dgm, UDP port 138, netbios datagram service.
- Netbios-ssn, TCP port 139, netbios session service.
- Microsoft-ds, TCP/UDP port 445.
- HTTP-rpc-map, TCP port 593, HTTP RPC Ep Map.

With the consent of the CIO, additional services may be added to this list as the need arises.

Default Firewall Configuration
The firewall configuration consists of three active interfaces or security zones with values of 0-100. The Middle Georgia State University LAN is attached to the internal interface with a value of 100. The Internet is connected to the outside interface with the value of 0. The DMZ is connected to the DMZ interface with the value of 10. By default all connection requests from a higher security zone to a lower security zone are permitted. Connection requests from a lower security zone to a higher security zone are denied. When connection requests from a lower security zone to a higher security zone are required to support the University mission, an access rule must be added to the firewall. All requests for adding access rules must be submitted to the Office of Network Administration with the following information:

Source IP address
Source organization name
Destination IP address
Destination protocol and port
Destination contact, name phone, email address
Reason required in support of the academic mission of the University.
Signature of authorizing department chair.

Source IP address and destination IP address and port must be as specific as possible so access rules will be least permissive.

Network IP addresses will be permitted as the source address, as long as the destination is specified by a specific IP address and port.

DMZ (Demilitarized Zone)
The DMZ network interface on the firewall is dedicated to servers hosting public services, such as public web servers and email front ends. Servers on the DMZ allow “public” access; therefore this network should be considered only “semi-protected.” It is the only interface on which a source address of “any” will be allowed in firewall rules.

This policy is intended to reduce exposure to threats associated with connecting to the Internet. The Chief Information Officer (CIO) must approve any waiver of these requirements

5.0 Enforcement
Firewall and router access rules will be used to enforce the requirements set forth in this document.

In the event of an emergency, additional configuration and procedural changes may be made in order to protect the Middle Georgia State University Network. Faculty and staff will be informed immediately if these changes are significant or disruptive. Workarounds will be provided for any disrupted services. In the event an acceptable workaround is unavailable, the CIO will determine the course of action.

5.0 Revision History
04/20/2006 - Original
01/28/2013 – Changed institution name to reflect consolidation
08/04/2015 - Changed institution name to reflect University status