

NETWORK FIREWALL POLICY

The Internet firewall at Eastern Mennonite University enhances security of computer and network resources to ensure a more reliable network and reduce illegal and malicious activities. The firewall policy attempts to balance risks incurred against the need for access.

A firewall is one element of security for the campus network. It reduces the threat of outsiders either damaging EMU's systems or using the systems as a jumping off point for illegal entry into other systems. A firewall does not prevent malicious or illegal activities from inside the firewall.

This firewall policy statement assumes that Security Standards for EMU Computer Network Users, Acceptable Use Policy for EMU's Campus Computer Network, and other Information Systems policy statements regulating use of computing and network resources at Eastern Mennonite University are in force.

The general firewall policy is stated as follows:

1. The intent of the firewall is NOT to restrict access to external resources from those inside the firewall. Some restrictions may be put in place in order to protect the functionality of the entire EMU network and will be done so with oversight provided by the Information Systems Planning Committee.
2. Access to internal resources by those outside the network is limited by the firewall. Access is provided only in the following instances:
 - a. Information Systems will provide access through the firewall to the campus web servers and campus email.
 - b. Certain mission-critical functions require vendors and other entities to have limited access to system resources from outside the firewall. Where feasible, functions/entities that require open access from the outside world will be located outside the firewall (the Ariel document delivery system used by the library is an example). Functions/entities that require open access that cannot be located outside the firewall will be restricted to mission-critical administrative functions (such as access to and by Jenzabar, the administrative systems vendor, and SIRSI, the library automation systems vendor). Where feasible, such outside access will be limited to specific times that connections are needed.
 - c. Faculty, staff, and students may request additional access from the external world to resources inside the firewall. These requests must be in writing and must include a rationale for the request. Requests for access to file servers and web servers will generally be granted. Information Systems staff will evaluate the risk of opening the firewall to accommodate other requests. Where the risk is acceptable, granting of requests will be dependent on network infrastructure limitations and the availability staff resources (primarily time) available to implement the request. If there is disagreement between the requestor and IS staff about the feasibility of the request, the request may be appealed to the Information Systems Planning Committee.

Reviewed by ISPC
April 17, 2008

Approved by Cabinet
July 3, 2000