Purpose:
The purpose of this document is to provide guidelines for using and maintaining a firewall to protect University computers from unauthorized access. Fordham IT recommends that all users protect the computers and communication equipment for which they are responsible. Fordham IT recommends that all users familiarize themselves with the documentation for the firewall software they have installed.

Scope:
This IT Policy, and any other policy referenced herein, shall apply to all members of the University community including, but not limited to, faculty, students, administrative officials, staff, and independent contractors (hereinafter the “User(s)” or “you”) who uses, accesses, or otherwise employs, locally or remotely, the University’s IT Resources, whether individually controlled, shared, stand-alone, or networked.

- Background
  - Firewalls are used to prevent unauthorized access by Internet users to private network resources. Firewalls can be implemented using hardware, software, or a combination of both. The University Firewalls provide “perimeter” protection against outside attacks. All traffic entering or leaving the Fordham University network passes through a firewall, which examines each message and blocks those that do not meet specified security criteria. Attacks from inside the campus network do not pass through the perimeter firewalls and may pose greater threats than outside attacks.
  - Host-based firewalls may be used to provide an additional level of security to individual computer systems. Host-based firewalls are typically software, which is installed on a single computer, which can provide customized protection for that computer.

- Windows Operating System
  - Symantec Client Firewall
    - To protect our computing environment, Fordham IT provides firewall software at no cost to all faculty, staff, and students for use on University as well as personal computers. The University standard software of choice is Symantec Client Firewall (part of the Symantec Client Security product suite).
    - To obtain a copy of this firewall software or to update this software, call IT Customer Care at 718-817-3999 (internal extension 3999) or e-mail HelpIT@fordham.edu.
  - Windows Firewall
Windows Firewall is available for Microsoft Windows XP and later releases. For those computers on which Windows XP Service Pack 2 (SP2) has been installed, Windows Firewall is turned on by default at the time of installation. However, since some computer manufacturers and network administrators may have turned Windows Firewall off Fordham IT strongly recommends that all users determine that their Windows Firewall is turned on and set to provide the correct level of protection. For assistance in determining whether the Windows Firewall software is correctly configured for maximal protection, call IT Customer Care at 718-817-3999 (internal extension 3999). Instruction on how to manually configure Windows Firewall is available at: http://technet.microsoft.com/en-us/library/bb456986(TechNet.10).aspx

- Other firewall products
  - If you install your own firewall software, you are responsible for the maintenance and upkeep of the software. IT Customer Care and User Support does not provide support for these products.

- Mac OS X 10.5 and higher
  - Application Firewall
    - Like Windows, Apple has provided Application Firewall in MAC OS X 10.5 and higher.
    - Instructions on how to configure Application Firewall is available at: http://support.apple.com/kb/HT1810
  - Other firewall products
    - If you install your own firewall software, you are responsible for the maintenance and upkeep of the software. IT Customer Care and User Support does not provide support for these products.

- Other Operating Systems
  - Please refer to vendor documentation for specific firewall configuration.
  - If you install your own firewall software, you are responsible for the maintenance and upkeep of the software. IT Customer Care and User Support does not provide support for these products.

  - Other firewall products
    - If you install your own firewall software, you are responsible for the maintenance and upkeep of the software. The Help Desk and User Support will be unable to provide guidance to these products.