Impact Statement

Virtual Private Network
Virtual Private Networks (VPN) provide easy access from the Internet into a private network and its internal resources. VPN security is only as strong as the methods used to authenticate the users (and the devices) at the remote end of the VPN connection.

Network Firewall Exceptions
Network firewalls filter network traffic based on attributes such as IP address and port. Network firewall exceptions or opening a port allow certain traffic to be sent to or from your computer through that firewall. Allowing all network traffic from a specific IP address or port through a firewall is like opening a tiny door in the firewall.

Each time you create an exception or open a port for a program to communicate through a firewall, the computers being protected by that firewall become a bit less secure. The more exceptions or open ports your firewall has, the more opportunities there are for hackers or malicious software to use one of those openings to spread a worm, access your files, or use your computer to spread malicious software to others.

Unguarded computing habits can lead to malware infections that can cause detrimental effects ranging from widespread exposure of sensitive information stored on the device to compromising the performance and security of the college’s network environment.

Following the precautionary policies, guidelines, recommendations and instructions outlined below will not only minimize the security risks of using a VPN or firewall exceptions, but will also allow you to conform with CCNY/CUNY’s information security policies.

CUNY Information Security website: http://security.cuny.edu
CCNY Information Security website: http://ccny.cuny.edu/it/security.cfm

It is critical that your computer has the most recent security patches for your operating systems. (Visit http://update.microsoft.com for windows OS or http://www.apple.com/support/downloads/ for MAC OS. Anti-virus software MUST be installed and with the latest definition file and updates (ie. McAfee virus scan, Norton anti-virus, AVG, Avast etc.

If you need help ensuring that your computer meets these requirements – Please contact the Service Desk in NAC 1/301, call (212) 650---7878 or email servicedesk@ccny.cuny.edu.
VPN Request

Please justify your need for VPN access:

List the application(s) and/or servers (including ip address) you need access to:

What resources will you use it to access, what functions will be performed, etc.:

Network Firewall Requested Changes

<table>
<thead>
<tr>
<th>Add</th>
<th>Remove</th>
<th>Source</th>
<th>Destination</th>
<th>Service</th>
<th>Accept/Block</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

I hereby certify that the computer I use to connect to the CCNY network has the most recent operating system updates, has been checked for spyware, and has a regularly updated anti-virus package installed and I will continue to keep these maintained. I understand that the same Acceptable Use of Computer Resources policies will apply the same as if I was on campus.

First Name  Last Name

Department   Building   Room

Phone Number  Cell Number  Email

Requestor’s Signature  Date

Supervisor’s Name  Supervisor’s Signature  Date

To Be Filled in By OIT Staff:

CIT #  Manufacturer  Model #  Serial#

IP Address  Host Name  MAC Address

Duration Of Access  Computer Type (server, desktop, laptop)  OS (e.g. Windows, Mac, Linux)

Contact Person  Department SysAdmin (if applicable)