The City College of New York

Office of Information Technology

Firewall Exception Request Form

Impact Statement

Guidelines

Network firewalls filter network traffic based on attributes such as the 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, 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 these openings to 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 the widespread exposure of sensitive information stored on your personal device to compromising the performance and security of the entire college's network environment.

Following the precautionary policies, guidelines, recommendations and instructions outlined below will help minimize the security risks of accessing a firewall port, while ensuring that you are conforming 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. These can be downloaded at **http://update.microsoft.com** for windows OS or **http://www.apple.com/support/downloads/** for MAC OS. In addition, anti-malware software MUST be installed (ie. McAfee virus scan, Norton anti-virus, AVG, Avast etc).

To make a firewall request, users gets a form or a link to the form and the guidelines from the CCNY website at https://support.ccny.cuny.edu/pdf/Firewall_Exception_Request_Form.pdf. Return the completed and signed form to the Service Desk so they scan it, create a ticket and assign the ticket to I.T. Security.

The form must be filled out fully and signed by the department Chair, Dean or VP, before we can continue to the next step. Not filling out the form correctly will result in unnecessary delays.

We will then notify Networking to create the exception and they will contact the user.

Firewall Exception Request Form

JUSTIFICATION FOR FIREWALL EXCEPTION:

☐ HTTP   ☐ SSH   ☐ SFTP   ☐ OTHER (Specify below)

NETWORK FIREWALL REQUEST CHANGES (Place check mark under add or remove)

Add	Remove	Source I.P.	Destination I.P.	Service/Port

EMPLOYEE/SPONSOR INFORMATION:

Last Name:	First Name:	
Phone:	Email:	
Department:	Building:	Room:
Duration of access: (end date) / /	Department System Admin:	

INFORMATION SECURITY STATEMENT

I hereby certify that my or my contractors server has the most recent operating system updates, has been checked for malware, and has a regularly updated anti-malware package installed and I will continue to ensure these are maintained. I understand that The City University of New York Policy on Acceptible Use of Computer Resources (security.cuny.edu) will apply.

Employee/Sponsor's Signature: Date:

APPROVALS:

Chair, Dean or VP Last Name:	First Name:
Chair, Dean or VP Signature:	Date:

NON-CCNY PERSONNEL INFORMATION:

Last Name:	First Name:
Phone:	Company Email:
Company:	Firewall Access end date (one year limit): / /