The City College of New York

Office of Information Technology

VPN Access Request Form

Impact Statement

Virtual Private Network

Virtual Private Networks (VPN) provide easy access from the Internet to 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. A Chairperson, Dean or Vice President **must** sign the form for the request to be granted.

Unguarded computing habits can lead to malware infections potentially resulting in a multitude of detrimental effects, from the widespread exposure of sensitive information stored on the device, to compromising the performance and security of the entire City College network environment.

Following the precautionary policies, guidelines, recommendations and instructions outlined below will help minimize the security risks of using a VPN, and ensure that you conform with CCNY/CUNY's information security policies.

CUNY Information Security website: **http://security.cuny.edu**

CCNY Information Security website: **https://www.ccny.cuny.edu/it/security**

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 with the latest definition file and updates (ie. McAfee virus scan, Norton anti--virus, AVG, Avast etc).

1. All VPN requests should start with the Service Desk. A user gets a form (or a link to the form) and the instructions on how to complete it. The completed and signed form is then returned to the service desk, which scans it, creates a ticket and assigns the ticket to I.T. Security.

If the form is filled out correctly and signed by the correct supervisor we will continue to the next step. If not, the form must be done again.

2. When it is completed, we check the user's computer for virus and malware, after which we ensure that the computer is installed with the latest security updates for their operating system.

3. At this point we will instruct Networking to create the account. They will contact the requester and give them their login credentials.

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**.

The City College of New York

Office of Information Technology

VPN Access Request Form

JUSTIFICATION FOR VPN ACCESS:
☐ System Administration ☐ Research ☐ Other (Specify Below)

SYSTEM(S) YOU NEED TO ACCESS:			
IP Address	**Host Name**	**Operating System (Build)**	**Anti-malware**

WHAT APPLICATIONS AND RESOURCES WILL YOU ACCESS: (i.e. wordpress, ssh, mysql, etc...)

EMPLOYEE/SPONSOR INFORMATION:		
Last Name:	First Name:	
Phone:	Email:	
Department:	Building:	Room:
Duration of Access (end date): / /	Dept. System Admin:	
INFORMATION SECURITY STATEMENT:		
I hereby certify that the computer I or my contractor uses to connect to CCNY via VPN 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 Acceptable Use of Computer Resources (security.cuny.edu) will apply as if I were on campus.		
Employee/Sponsor Signature:		
Chair, Dean or VP's Last Name:	First Name:	
Chair, Dean or VP's Signature:	Date:	

NOTE: Supervisor approval needed for part-time employees

APPROVALS:	
Supervisor's Last Name:	First Name:
Supervisor's Signature:	Date:

NOTE: If you are requesting a VPN account for non-CCNY personnel complete section below.

NON-CCNY PERSONNEL INFORMATION:	
Last Name:	First Name:
Phone:	Company Email:
Company:	VPN Access end date (*one year limit*): / /