The City College of New York

Office of Information Technology

Admin Access Request Form

Impact Statement

Administrative privileges on modern desktop Operating Systems grant users complete control over most functions and features of the Operating System and Applications. 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 not only help minimize the security risks of administrative privileges, but will also allow you to conform to 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

Conditions (requirements to acquire an administrative account)

Integrity of User Files

○ Aside from software provided by the College, the user bears responsibility for any loss or corruption of files due to his or her use of the privileges available through the administrative account.

○ The Office of Information Technology will not view, tamper or inspect users' files without the request or approval of the user.

Use of Non-Public University Information (NPUI)

○ NPUI includes many forms of information which must always be treated as highly confidential, including:

- Social Security numbers
- Drivers Licenses or other government-issued identification
- Credit/debit card numbers and pins
- Usernames with passwords
- Student records (GPAs, transcripts, grades, test results)
- Health records
- Confidential research data

○ These forms of information must not be stored, transported, or taken home on portable devices (e.g., laptops, flash drives) of any type without the express approval of the user's immediate supervisor, as well as the department's executive Vice President and the Office of Information Security.

○ Where approval is granted, additional password protection and encryption of data are required. No exceptions.

Admin Access Request Form

Software Installation Requirements

- All software installed on college-owned computers must be properly licensed.

- All users, including those with administrative privileges, must adhere to all federal and state laws, and University regulations, paying particular attention to copyright.

- Peer-to-peer applications, which open the user's machine to other computers on the Internet allowing outsiders access to the CCNY Network, are known to pose risks to the user's computer and the network; hence such software should not be used except for research purposes

- The Office of Information Technology will not offer technical support for any user-installed, specialized software. Network Access

- All users will continue to have access to the network services provided by the college, such as email, Internet access, etc.

- Elevated user privileges on the local machine(s) do not apply to network devices or services. Passwords and User Accounts

- The Office of Information Technology will maintain an administrative account on each machine.

- The user will not create any unauthorized administrator or user account on the machine.

- The user will not delete any user accounts initiated by OIT on the machine.

- The user will not make any password change that results in restricting the Office of Information Technology from administering the machine. Local Machine

- The detection of a malware activity, or any other disruptive element affecting the CCNY network, will automatically result in the disconnection of the affected machine from the CCNY network and revocation of administrative privileges.

- The user will be responsible for installing software updates on the local machine, unless and until such time as a College-wide automated procedure is implemented.

- Hardware configurations cannot be modified in such a way as to void the manufacturer's warranty.

- Peripherals (e.g., printers, scanners, external drives, etc.) can be added by the user

- The user will not permanently uninstall, disable or modify any software designed to protect the system that has been installed by the Office of Information Technology, without prior permission.

- The Office of Information Technology will schedule the resolution of any technical problems created as a result of an administrative account according to the normal technical support procedures

Admin Access Request Form

General Guidelines and Loss of Privileges

○ The Office of Information Technology in consultation with the College administrators reserves the right to suspend the administrative account if any condition is violated.

○ Users acknowledge that compromised operating systems might require re-installation, potentially resulting in partial or total loss of files.

○ The user agrees to make a good faith effort not to disrupt any network services for other researchers, other faculty, staff and students. User Rights

User Rights

○ OIT will maintain the same level of service as provided to all users. This includes installation and re-installation of site licensed software. It also includes trouble-shooting problems not unique to user-installed software

Important

○ Only use the administrative account for administrative purposes (downloading, installing, and upgrading software and hardware applications and performing basic maintenance).

○ Never use the administrative account for day-to-day computer tasks (browsing websites, using social media, checking email, working with documents, spreadsheets, and database, which are vectors for transmitting malware. Contracting malware with administrative account, grants administrative control over the computer resources to the malware

○ Schedule a meeting with Client Service technicians in the Office of Information Technology for advice and assistance maintaining the local desktop in an administrative environment.

○ The user is encouraged to perform daily tasks using the generic user account; the administrative account should be reserved exclusively for tasks that require elevated privileges (software installation, updates, upgrades, troubleshooting, etc.).

○ OIT will provide a list of “best practices” to help users properly utilize their administrative privileges. Acceptance of Agreement In order to perform my job duties and fulfill my responsibilities to CCNY, I am requesting administrative privileges on my CCNY-issued computer. CCNY/CUNY has issued this device to me and I am the primary user and custodian. I understand that this access allows me to install and update software and I must confirm the authenticity of all software before installing. By signing this application, I acknowledge that I have read the CCNY Administrative Account Request Form, and agree to abide by the rules and regulations that apply.

The City College of New York

Office of Information Technology

Admin Access Request Form

JUSTIFICATION FOR ADMIN ACCESS:			
☐ System Administration	☐ Software Installation	☐ Application Requirement	☐ Other (Specify Below)

EMPLOYEE INFORMATION:		
Last Name:	First Name:	
Phone:	Email:	
Building:	Department	Room:

SYSTEM INFORMATION:	
Host Name:	IP Address:
Operating System:	Anti-Malware Software:
Manufacturer:	Model:
Serial Number:	CIT Number:

INFORMATION SECURITY STATEMENT	
In order to perform my job duties and fulfill my responsibilities to CCNY, I am requesting administrative privileges on my CCNY-issued computer. CCNY/CUNY has issued this device to me and I am the primary user and custodian. I understand that this access allows me to install and update software and I must confirm the authenticity of all software before installing. By signing this application, I acknowledge that I have read the CCNY Administrative Account Request Form and agree to abide by the rules and regulations that apply. I hereby certify that this computer has the most recent operating system updates, has been checked for malware, has a regularly updated anti--malware package installed and that I will continue to keep these maintained. I understand that The City University of New York Policy on Acceptable Use of Computer Resources (security.cuny.edu) will apply.	
Requestor's Signature:	Date:

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

Notes: