Purpose and Background:

This policy defines rules regarding the granting and use of local administrative privileges. “Local Administrative Privileges” means the granting of “Administrator” or equivalent rights on a particular University device, such as a Microsoft Windows desktop computer.

Routinely, users are assigned a user-level account for their CUNY work that provides access to common services and applications, such as web browsers, email, office productivity software, file storage and shared printer access. Users with user-level accounts cannot generally install new applications nor upgrade software components (e.g., on their computer workstation).

Some users, by the nature of their work, require additional software that is not included in the standard software suite available on managed devices. In most cases, technical support personnel can install additional licensed software on behalf of the user upon request. In other cases, local administrative privileges may be required to support a user’s needs.

An important security practice in this regard is the “principle of least privilege.” The principle advocates that users should use an account that is granted only the minimum access permissions necessary to complete a task and nothing more.

Scope:

This issuance of the policy applies to University-owned devices within the Central Office.*

* Campuses are encouraged to adopt this policy locally and/or as a best practice (with a suitably adapted request and approval process) pending consideration of university-wide adoption by the IT Steering Committee.
Local Administrative Privileges

Procedure(s):

Use of local administrative privileges is limited to the following circumstances:

- The nature of the user’s work requires the frequent ability to install or upgrade non-standard software on the device. “Frequent” is defined as anticipated to average more than once per month. Typically such users are software developers and system and application administrators but can include others utilizing specialized software.
- When required software will not operate without local administrative privileges.
- When local administrative privileges is the only mode available within a device (e.g., mobile devices such as iOS®- and Android®-based smartphones and tablets). (No approval required.)
- When required by IT technical support in the normal course of system administration. (No approval required.)

Users granted local administrative privileges must comply with the following:

- User is responsible on an ongoing basis to keep abreast of any security updates relevant to additional installed software as released by its publisher(s) and perform timely installation of such updates.
- Software that captures, displays or manipulates network traffic in a “promiscuous” or other mode may not be installed unless such is required in the normal course of assigned work responsibilities.
- Software that interferes, inhibits, disables or bypasses installed anti-malware software may not be used. Anti-malware software may be temporarily disabled when necessary to prevent issues during software installation only.
- Third-party remote access software (e.g., LogMeIn®, GotoMyPC®, TeamViewer®) may not be installed or used to enable remote desktop access to a University device. Where available, approved remote desktop access service can be requested through the Service Desk.
- Additional local accounts (with or without administrative privileges) may not be created unless they are a documented by the vendor as a requirement of software to be installed.
- Automatic Updates may not be disabled (where it may be configured for the operating system and other standard applications).
- Existing local accounts and services may not be disabled.
- IT’s ability to support the University-owned system may not be impeded.
- Only software in compliance with its copyright and licensing may be installed. See “Software Licensing & Copyright Laws” below.
- Only software applications and tools required for a user’s work in support of the University can be installed.
Local Administrative Privileges

Risks

The assumption of local administrative privileges on a University device carries certain inherent responsibilities and increased risks. These include the potential loss of data, compliance with copyright laws and increased threat of compromise.

- **Data Security**—Local administrative privileges increases susceptibility to spyware, malware and potentially damaging security breaches due to the elevated level of rights and permissions associated with administrative privileges.

- **Data Loss**—Safeguards intended to prevent inadvertent, irreversible actions can be inhibited by local administrative privileges. Users are solely responsible for any data that is stored locally and as such must exercise due diligence in providing a backup mechanism to ensure against the potential loss of any important data. Failure to implement a backup mechanism can result in permanent loss of such data.

- **Software Licensing & Copyright Laws**—Adherence to copyrights and licensing agreements is mandatory for all installed software. Users do not have the authorization to agree to software terms and conditions (End User License Agreements) on behalf of the University. Contact the Procurement and/or Office of General Counsel departments for more information.

Requesting Local Administrative Privileges

By default users are granted User access level on their devices. Local administrator access is granted on an as-requested basis for a particular device based on a justification of the need.

To request local administrative privileges:

1. Review these procedures.
2. Fill out the form below fully, signed by yourself and your supervisor.
3. Submit the form by email as a scanned PDF attachment and send it to security@cuny.edu
4. The submission will be reviewed, and, if approved, a signed copy will be sent back to you by return email.
5. Open a ticket with the CIS Service Desk requesting local administrative privileges and attach the signed form to the ticket.

Responsibility:

CUNY users, including faculty, students, staff and affiliates of CUNY.
Local Administrative Privileges

Related Information:

Acceptable Use of Computer Resources
IT Security Procedures
(Found at security.cuny.edu)

Effective Date:

Effective upon issuance.
CUNY CIS Request for Local Administrative Privileges

Name: ____________________________________________

Building: ___________________________ Room/Cubicle: ___________________________

Workstation / PC System / Device Name (optional): ___________________________________

Justification/Need: _______________________________________________________________
______________________________________________________________________________
______________________________________________________________________________
______________________________________________________________________________
______________________________________________________________________________

I have read, understand and agree to comply with these Procedures and assume the responsibility of Local Administrative Privileges.

Signature: ____________________________________________
Date: ________________________________________________________________________

Supervisor/Manager: I confirm that my subordinate named above requires Local Administrative Privileges to perform work as described and I approve the granting of such access.

Name of Supervisor/Manager: ____________________________________________ (printed)

Signature: ____________________________________________
Date: ________________________________________________________________________

All Signatures Are Required

Please submit for approval as a scanned PDF attachment by email to security@cuny.edu

CIO, Deputy CIO, CISO or designee Approval

Name: ____________________________________________ (printed)

Signature: ____________________________________________
Date: ________________________________________________________________________