Policy IT030: Administrative Rights

Recommended for Approval by: Fawn L. Petrosky

Fawn L. Petrosky, Vice President for Finance and Administration

Approved by: R. Lorraine Bernotsky

Dr. R. Lorraine Bernotsky, Interim President

Effective Date: 01/31/2024
Amended Date:

A. Intent

Administrative rights refer to the level of access and control granted to individuals within the University's IT systems and networks. These rights enable users to make significant changes to computer systems, including the installation and removal of software, configuration adjustments, and access to sensitive data. While administrative rights can be essential for certain tasks, their indiscriminate distribution poses substantial security risks.

The purpose of this policy is to establish guidelines for the responsible management of administrative rights within the University's IT environment. This policy aims to:

- Enhance cybersecurity by minimizing the potential for unauthorized changes, malicious activities, ransomware, export control violations, licensing, compliance issues, data loss, and data breaches.
- In accordance with the Principle of Least Privilege, ensure that administrative rights are only granted when necessary. Exceptions must be approved by Institution Leadership and only for specific roles and purposes.
- Promote efficient IT operations by streamlining administrative access to those who require it for legitimate purposes.

Scope

This policy applies to local Administrator rights for University-owned Desktop and Laptop systems.

B. Definition(s)

Principle of Least Privilege - refers to the practice of granting individuals or systems the minimum level of access, permissions, or privileges necessary to perform their specific tasks or functions, and no more. In essence, it limits users and processes to only the resources and permissions they need, thereby minimizing potential security risks and limiting the potential for misuse or abuse of privileges.

C. Policy

At PennWest University, we prioritize the security and integrity of our campus IT environment. To this end, we strictly adhere to the Principle of Least Privilege, which dictates that administrative rights are granted only to individuals when administrative rights are essential to fulfilling that individual's specific job responsibilities. This approach ensures that users are granted the minimum level of access required to carry out their duties, thereby mitigating potential security risks and minimizing the potential for misuse of privileges. Based on this principle, administrative rights will only be granted by request to those who meet specific criteria for having administrative rights.

For routine and one-off software installations, our IT Support teams are readily available to provide assistance and support. They possess the necessary permissions and expertise to perform these tasks efficiently while adhering to established security protocols. This practice not only streamlines the process for software installations but also reduces the risk associated with widespread administrative access.

Administrative rights will only be granted for specific exceptions and under carefully controlled circumstances. Such exceptions must be thoroughly justified and documented, and approval will be subject to review by the University's IT security team. These exceptions are granted sparingly and exclusively when there is a clear and compelling need.

Valid Reasons for Granting Administrative Rights

Administrative rights should only be granted when individuals have a legitimate need for them to perform their job responsibilities timely and effectively. Valid reasons for granting administrative rights include:

- **Laboratory Management**: Faculty or staff who manage University laboratories that require frequent software installations, updates, and configuration changes.
- **Teaching Demonstrations** – Routine use of laptop/desktop to perform demonstrations of teaching content that are restricted from functioning without administrative rights.
- **Specialized Software/Hardware**: Faculty or staff members who require administrative rights to install, maintain, and operate specialized software and/or hardware that would require frequent use of administrative rights critical for their academic or research activities.
- **IT Staff –** IT Staff will be assigned administrative rights to perform their job duties based upon the principles outlined in this document and based upon the duties required of their job roles at management's discretion.
- **Exceptional Circumstances**: In exceptional circumstances, administrative rights may be granted on a case-by-case basis with approval from the University's IT security team and Institution Leadership. Such cases should be rare and well-documented.

Administrative Rights Restrictions

Users receiving administrative rights will agree to the following restrictions:

- Users will receive a separate Administrative Account.
- Administrative accounts will last for 1 year and then must be re-requested/re-evaluated.
- Administrative accounts will not be used for general day-to-day activities such as logging into your computer or e-mail and web access.
- Administrative accounts will only be used to perform tasks requiring administrative privileges.
- Administrative accounts will not be used to remove or modify any hardware or software without Information Technology Services (ITS) permission.

- Administrative accounts will not be used to remove or modify antivirus/security software.
- Administrative accounts will not be used to disable or reconfigure the remote management services used by ITS.
- Administrative accounts will not be used to create additional user accounts, give any other accounts administrative rights or otherwise tamper with the administrative account.
- Administrative accounts will not be used to install any software that has not been purchased by the University through appropriate procurement processes, or that has a licensing agreement allowing for free use at a University. (Even free software has "click through" acceptance of terms that must be reviewed by University personnel. Even if software is free, it cannot be used if its terms and conditions are impermissible.)
- Administrative accounts will not be used to install applications that may establish network share protocols which result in an increase in bandwidth utilization as this may cause network congestion and degradation of network performance across wide areas of the campus. Examples include peer-to-peer (P2P) applications such as BitTorrent, Gnutella, etc.
- Administrative account users will allow for the removal of any software that adversely affects system efficiency or introduces a significant risk to system security as determined by ITS.
- Administrative account holder will be responsible for patching software that they install.

Additional Warnings

- The use of cloud services (Microsoft, Google, Apple, AWS, DropBox, etc.) for University business requires a contract that has been approved by University System Legal Counsel. The only approved cloud storage for both PennWest and PASSHE is Microsoft OneDrive/Teams/SharePoint. Adobe Creative Cloud is also approved. If you use cloud services that are not approved, then you are responsible for any and all implications that result and you may not be represented or indemnified by the University.
- Individuals are responsible for notifying the University of any software or modifications made to laptop configurations that might violate Export Control Laws when doing international travel.
- When travelling internationally IT must be notified and an Export Control Form must be filled out to ensure legal compliance. Users with administrative rights are responsible for verifying that software that they install is in compliance with Export Control Laws in the countries they are travelling to.
- Non-standard software will be removed as part of a normal repair process if necessary to restore system functionality.
- Administrative accounts that are not used or deemed a security risk may be revoked at the discretion of the IT Security Team.
- Systems may be placed in special protected networks to reduce risk at IT's discretion.
- Users with Administrative accounts on shared systems must consider the consequences of their actions on other users of those systems. For instance, users may unintentionally or intentionally modify system settings, which can disrupt network connectivity, cause software conflicts, or reduce the overall stability of the system by performing certain actions.

D. Procedure(s)

Requesting Administrative Rights

To request administrative rights, faculty and staff should follow a formal process that includes:

- Submitting a Helpdesk Ticket explaining the specific reasons and justifications for needing administrative rights.
- Review and approval:
    - By Department Chair, Dean of College, and the University's IT security team for Faculty.

    - By Director, Vice President, and the University's IT security team for Staff.
- Complete all IT Security Awareness Training and a special computer administrator training provided by IT.
- Provision of administrative rights for a limited and defined duration, with periodic reviews and audits.

Revocation of Administrative Rights

Administrative rights may be revoked under the following circumstances:

- The individual no longer requires administrative rights for their job responsibilities.
- No usage of Administrative Account for 6 months.
- Violation of University IT policies or security practices.
- A change in job responsibilities that no longer justifies administrative rights.
- Non-Compliance with IT Security Awareness Training

Non-Compliance and Sanctions

Persons in violation of this directive are subject to the full range of sanctions, including without limitation the loss of access privileges to resources, disciplinary action, dismissal from the University, and legal action. Some violations may constitute criminal offenses, as outlined by federal, Pennsylvania and all other applicable laws; the University will carry out its responsibility to report such violations to the appropriate personnel.

E. Related policies

IT001: Acceptable Use Policy
IT008: Cloud Application Policy
IT006: Information Security Policy
IT015: Export Control Policy
AAC053: Confidentiality of Student Records

F. Contact Information

Office/Name	Location	Phone Number
Information Technology Services	California, PA	724-938-4030

G. Policy Review Schedule

All policies will be reviewed every two years or on an as needed basis if a change in BOG, PASSHE or Pennsylvania law would create the need for an immediate change.