Elevated Privilege Rights Policy

Type of Policy: Administrative
Policy No: UP-05-001
Effective Date: TBD
Last Reviewed Date:
Next Review Date: TBD
Administrative Officer: James Pete, VP/CIO
Policy Owner: Information Technology Services
Contact Name: Dawn Krieger
Contact Title: Director Cybersecurity Compliance
Contact Email: dawnkrieger@clayton.edu

Reason for Policy:
Controlling access to information systems, products/services, and managing end user accounts are critical business processes that support effective use of information resources. This policy refers to the process by which an individual's access and permissions are activated (provisioned), reviewed, and deactivated (deprovisioned) consistent with the individual's roles and responsibilities as an employee. Account management must be addressed to lower the risks and threats facing users, hosts, networks, and business operations.

Policy Statement:
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 management of elevated rights within the University's Information Technology (IT) environment through Endpoint Privilege Manager (EPM).

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," that dictates that users should only be granted the minimum level of access for them to carry out their job functions and ensure that elevated rights are only granted when necessary.
    - Exceptions must be approved in writing by the unit head Vice President or Executive Director and ITS VP/CIO for specific roles and purposes.

- Promote efficient IT operations by streamlining elevated access to those who require it for legitimate business operational purposes.

Policy Scope:
This policy applies to local Administrator rights for University-owned or controlled devices, such as but not limited to desktops and laptops.

The affected stakeholders listed below indicate all entities and people within the enterprise that are affected by this policy.

- Vice Presidents, Deans, Directors, and Department heads
- All members of the university community (faculty, staff, and student employees)
- Vendors/Contractors
- All individuals using enterprise technology resources

Policy:
Clayton State University prioritizes the security and integrity of the university IT environment by strictly adhering to the Principle of Least Privilege. This dictates that elevated privileges (*formally administrative rights*) are granted only to individuals when elevated privileges 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, elevated privileges will only be granted by request to those who meet specific criteria.

For routine and one-off approved software installations, all stakeholders will use the HUB which is readily available to help and support. They possess the necessary permissions and expertise to perform these tasks efficiently while adhering to established security protocols. Using the HUB not only streamlines the process for approved software installations but also reduces the risk associated with widespread administrative access.

Elevated Privileges 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 ITS Vice President/CIO. Exceptional circumstances may be granted when there is a clear and compelling need.

Valid Reasons for Granting Elevated Privileges
Elevated Privileges will only be granted when individuals have a legitimate business need for them to perform their job responsibilities timely and effectively. Valid reasons for granting elevated privileges include:

- **University Laboratory Environment**: 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 will not function without elevated rights.

- **Approved Specialized Software/Hardware**: Faculty or staff members who require elevated rights to install, maintain, and operate approved specialized software and/or hardware that require frequent use of elevated privileges critical for their academic or research activities.
- **Information Technology Services (ITS)** – ITS 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 supervisor's discretion.
- **Exceptional Circumstances**: In exceptional circumstances, elevated privileges may be granted on a case-by-case basis with approval from the ITS VP/CIO and Institutional Leadership from the requested division/unit. Such cases should be rare and well-documented.

Elevated Privileges Restrictions

Users receiving elevated privileges through Endpoint Privilege Manager (EPM) (formally administrative rights) will agree to the following restrictions:

- Users will receive elevated privileges through EPM
- Elevated Privileges will last for up to 12 months for staff and per teaching semester for faculty and then must be re-requested/re-evaluated.
- Elevated Privileges will not be granted for general day-to-day activities such as logging in to a computer to bypass login policies or e-mail, web access, etc.
- Elevated Privileges will only be used to perform specific tasks requiring elevated privileges.
- Elevated Privileges will not be granted to remove or modify any hardware or software without Information Technology Services (ITS) permission.
- Elevated Privileges will not be used to remove or modify antivirus/security software.
- Elevated Privileges will not be granted to disable or reconfigure the remote management services used by ITS.
- Elevated Privileges will not be used to install any software that has not been purchased and approved by the ITS VP/CIO. This includes free software; even free software has "click through" acceptance of terms that must be reviewed by university personnel. Even if the software is free, it cannot be used if its terms and conditions are impermissible.
- Elevated Privileges will not be granted to install applications that may establish network share protocols which result in an increase in bandwidth utilization or 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.
- Elevated Privilege users understand that ITS maintains the unilateral right to remove any software that adversely affects system efficiency or introduces a significant risk to system security as determined by ITS. The user of the software will be informed of the removal within two business days if not sooner.
- Elevated Privilege users will be responsible for patching/updating software that they install.

Key Notifications

- The use of cloud services (Microsoft, Google, Apple, AWS, Dropbox, etc.) for University business requires a license granted by a contract that has been approved by the University. ***The only approved cloud storage for Clayton State University 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 all implications that result, you may not be represented or indemnified by the University.

- Individuals are responsible for notifying the HUB when planning to travel outside of the United States, if they will connect to CLSU IT services or conduct any business on behalf of the University while traveling.
- Non-standard approved software will be removed as part of a normal repair process if necessary to restore system functionality.
- Elevated Privileges that are not used or deemed a security risk may be revoked at the discretion of the ITS.
- Systems may be placed in special protected networks to reduce risk at ITS's sole discretion.
- Users with Elevated Privileges 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. Such actions should be avoided and can lead to revocation of privileges and disciplinary action.

Procedures:

Requesting Elevated Privileges

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

- Submit a request for Elevated Privileges (link form) explaining the specific reasons and justifications for needing elevated rights.
- Review and approval:
    - By Department Chair, Dean of College, and the ITS VP/CIO for Faculty.
    - By Director, Vice President, and the ITS VP/CIO for Staff.
- Complete all mandatory Security Awareness Training and other training as assigned.
- Provision of elevated privileges for a limited and defined duration, with periodic reviews and audits.

Revocation of Elevated Privileges

Elevated Privileges may be revoked under the following circumstances:

- The individual no longer requires elevated privileges for their job responsibilities.
- No usage of Elevated Privileges for 3 months.
- Violation of University ITS policies or security practices.
- A change in job responsibilities that no longer justifies elevated privileges.
- Non-Compliance with mandatory Security Awareness Training or failure to complete or adhere to any training and its requirements.

Non-Compliance and Sanctions

Violations of this Policy could result in loss of access privileges to the University resources, and/or disciplinary action, up to and including termination. Additionally, if applicable, certain violations may be referred to by the appropriate legal authorities for criminal prosecution.

Definition(s):
Administrative Rights – refers to the level of access and control granted to individuals to make significant changes to computer systems, including the installation and removal of software, configuration adjustments, and access to sensitive data.

Elevated Privilege - ensures that users are granted the minimum level of access to perform essential functions while mitigating potential security risks and minimizing the potential for misuse of privileges.

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.

References/Sources:

- USG IT Handbook (*Section 3.1.1*)
- Acceptable Use Policy
- Data Access Policy
- Identity and Access Management

Policy History:

Revision Date	Author	Description
TBD	Cybersecurity	Policy document created