THE OHIO STATE UNIVERSITY

JOHN GLENN COLLEGE OF PUBLIC AFFAIRS

Local Administrative Privileges Standard

A. Purpose

The purpose of the Local Administrative Privileges Standard is to define how users will be granted administrative privileges and to enumerate the processes for requesting, granting/denying, appealing, and revoking those privileges.

B. Audience

1. Information Resource System Owners
2. Information Resource System stewards, custodians, and users
3. All John Glenn College of Public Affairs (JGCPA) administrators, faculty, staff, students, and visitors

C. Local Administrative Privileges Standard

1. Default Administrative Privilege Assignments:

i. IT Staff – IT Staff members are granted administrative privileges only on those assets necessary for them to accomplish assigned job duties.

ii. Faculty and Non-IT staff – No administrative privileges are granted.

2. Exception Criteria:

i. Computers where the majority of usage occurs off site – The computer is not located in an area where IT staff can easily access or support it. This might include a desktop system located in another part of campus or off campus, or it might be a laptop or tablet that is rarely used in College buildings.

ii. Users with specialized software – That is, essential software which does not allow non-administrative execution or is written in such a way that it requires the user to run, update, or patch as an administrator on the system. This exception will not apply if alternate non-administrative software, a modified software configuration, or other reasonable alternatives exist. IT staff and the user will work together to investigate other alternatives before this exception is granted.

3. Restrictions on Approved Exceptions:

i. IT staff will retain the exclusive use of the built-in Administrator account. Under no circumstances will the user be permitted to logon to, possess or change the password of, or access the files stored under this account.

ii. IT staff will create an administrator-level account for the approved user in addition to their normal non-administrative account. Under no circumstances will the approved user allow others to access this administrator-level account or share its password.
iii. The user must log in with their non-administrative account and may elevate privileges only as necessary for completing work-related tasks that require administrative rights.
iv. All administrative accounts will be time-limited according to the approved proposal and exception granted.
v. Purchases of software and/or licenses with University funds (including grant, research, and Individual Spending Accounts) must be completed by or with the approval of the Glenn College IT staff.
vi. Under no circumstances will the user remove or disable any software that has been installed by IT staff. The user also agrees not to modify the configuration of the operating system, including file and folder access control lists and encryption. Anything to the contrary must first be coordinated with and approved by IT staff.
vii. During the exception period, the affected computer must be made available to the IT staff upon request to review the system logs.

4. Request Process:

i. Users may request administrative privileges by submitting a written proposal to the IT Manager.
ii. This proposal must include the business purpose and duration of administrative access as well as the specific device(s) to which the user is requesting local administrative rights.
iii. The exception proposal will be evaluated by the Glenn College IT staff and faculty member(s) as selected by the Dean.
iv. The user will be contacted as soon as possible with any follow-up questions, points for clarification, or to discuss alternative options. Staff will make every attempt to respond with a determination within ten business days. Urgent or time sensitive requests should be noted along with all information needed to make a determination regarding access.

5. Appeal Process:

i. A determination to deny administrative access may be appealed to the Director of Administration.

6. Education Requirements

i. Users who are granted an exception and local administrative privileges must read, understand, and agree to abide by the following documents:
    1. LAPS Training (https://ocio.osu.edu/kb04088)
    2. Institutional Data Policy (https://ocio.osu.edu/sites/default/files/assets/Policies/InstitutionalData.pdf)
    3. Responsible Use of University Computing and Network Resources (https://ocio.osu.edu/sites/default/files/assets/Policies/Responsible-Use-of-University-Computing-and-Network-Resources-Policy.pdf)

ii. Users who are granted administrative rights must fill out and submit a Local Administrative Privileges Agreement form found at http://glenn.osu.edu/policies.
iii. Users who are granted local administrative privileges must also have completed the *Protecting Institutional Data* course in BuckeyeLearn prior to the issuance of an exception. This training must have been completed at some point within the previous calendar year.

7. Privilege Revocation:

i. User administrative privileges may be revoked for the following reasons:
    1. The term of the approved exception has expired
    2. User no longer serves in a role that requires administrative privileges
    3. User no longer utilizes software that requires administrative privileges
    4. User is involved in a data breach that is related directly to their having administrative privileges
    5. User demonstrates unsafe, illegal, or unethical practices while using administrative privileges
    6. The unit determines that the user no longer needs administrative privileges to perform job tasks.
    7. User requires excessive support from unit IT staff as a result of having administrative privileges.
ii. A decision to revoke user administrative privileges will be made by the IT Manager based on documentation of any of the above conditions and will be communicated to the user and the Glenn College Dean in writing prior to implementing the revocation.
iii. Users may request reinstatement of their previously-granted administrative privileges using the Appeal Process above. Such reviews will include consideration of the documentation and decision that led to the revocation.

8. Document Posting and Review

i. The approved Local Administrative Privileges document will be posted for staff and faculty at http://glenn.osu.edu/policies. The document has been reviewed and approved by the Office of the Chief Information Officer and will be subject to local review and updates on an annual basis based upon the date of last review.