Local Administrative Privilege Standards

Background

Faculty and staff often have a legitimate need for administrative privilege on their computers. Administrative privileges may be required to install software and updates, perform computer management tasks, or run some software packages.

However, using administrative access for everyday tasks such as reading e-mail or browsing the web carries an increased risk. Malicious software can take advantage of administrative privileges to jeopardize the operational integrity of a computer system. Violated accounts with administrative privileges may allow intruders to disrupt computer or network operations; steal information; or allow unauthorized access to data residing on the system or attached devices. Improperly applied administrative privileges may directly impact the availability of both computing resources and IT professional support. For this reason it is prudent to restrict administrative access to those who truly need it for academic or business needs and to refrain from using administrative access for the most risky tasks.

Routine tasks that do not require administrative access, such as web browsing and reading of email, should be executed using unprivileged accounts. Administrative privileges should be granted under the IT concept of “least privilege”, meaning elevated privileges should only be granted to end-users who have a legitimate need. Tasks should be performed using the most appropriate privilege level.

University units must adopt a Local Administrative Privileges Standard that defines how users will be granted administrative privileges and that clearly defines the processes for requesting, granting/denying, appealing and revoking these privileges. These standards will be reviewed by the IT@UC Office of Information Security (OIS)for conformity to these requirements, and approved standards will be published. This approach will help ensure some measure of consistency, fairness and transparency to the processes used for managing local administrative privileges at UC.

Note: The definition of the term “unit” in this document is not meant to represent any particular organizational structure per se, the determination of which parts of an organization requires a local administrative privilege standard is left intentionally vague

to allow for differing organizational concerns within the various colleges and VP areas of the university.

The following document outlines the basic requirements to which all Local Administrative Privileges Standards must adhere and gives suggestions to help guide the development of these standards. A development checklist is included with this document (see Appendix A). The checklist will aid local units in assigning personnel and defining the appropriately empowered faculty and staff members to facilitate standard adoption.

Local Administrative Privileges Standard Requirements:

1. Every department must develop a local administrative privilege approval process or adopt the process developed by the OIS. In the absence of a locally developed submission the unit is assumed to have adopted the OIS developed process.

    a. The OIS sample process can be found in Appendix B.
    b. The process must support ed users, IT staff and unit administration.

Note: In the case of academic units, end-user representation must include faculty who will be affected by the standard. Faculty representative(s) must be involved in approving the drafted local standard. Once the standard is developed and adopted, faculty representatives must continue to be involved during the regular review of the standard.

A checklist to guide units through the creation of a local administrative privileges standard document is included in Appendix A.

2. The process for assigning administrative privileges must be expressly defined in the standard.

    a. The standard document must include the unit position on assigning local administrative privileges. The exception/appeal process handles any case not addressed by the normal user profiles. The standard document must outline the normal procedure a user must follow to request administrative privileges that are needed outside the “default” unit definition.
    e.g. “Only IT professionals will have administrative privileges” or “Mobile device (laptops, handheld, netbooks, etc.) users may be granted administrative privileges” but cases may exist where a “normal” user needs administrative privileges and these will be granted based on established exception criteria.
    Criteria for making the privilege approval decision must be clearly specified in the standard document.
    e.g. “End user privileges are granted based upon the following criteria:

- The end user(s) utilizes a program that will only function under an account with administrative privileges.
- The end user(s) regularly operates the computer in an area that does not offer IT professional support such as a location outside university property.
- The end user(s) regularly operates the computer at times when there is no IT professional support available, such as weekend nights.
- The user(s) does not rely upon IT professionals for daily support or is her/himself an IT professional."

b. Decisions about applications for administrative privileges must be made on a timely basis, consistent with the efficient operation of university units. The standard must state the interval within which the requests will be handled.

c. The document must state the length of time an approval is valid and the unit must establish a review process for all approved requests. The review frequency should not exceed an annual cycle.

d. If applications for administrative privileges are denied, end users must be notified in writing of the reason(s) for the decision. Responses must be returned in the same period of time the unit designates to address the initial request.

3. The standard document must include an exception/appeal process by which end users or IT staff can appeal an administrative rights decision (local appeal).

a. The exception/appeal process must be documented in the standard. The unit must designate the actions needed to request an exception to the normal approval process.

b. Appeal/Exception rulings must be documented and clearly explained to the user appealing the initial privilege decision. Responses must be communicated in a timely manner, but in no case should it exceed 10 business days.

c. Unresolved end user administrative privilege decisions may be referred to OIS or another local "court of last appeal"—such as a unit head or designate—for final arbitration. Whenever possible, units must clearly designate in the standard who is the final arbiter. The finality of the arbitration decision must be stated in the standard.

4. Units must include an educational component in their standard. The increased risk and responsibility inherent in operating with administrative privileges must be

adequately explained and users granted these rights must be properly educated regarding these factors.

a. Units may design their own local education materials. End users and IT professionals versed in security should work together to create these materials.

Locally developed materials should be reviewed/updated regularly for continued relevance.

b. A sample training curriculum/outline is available in Appendix C.

c. Users should demonstrate in some way that they understand the impact of operating using administrative privileges and the personal accountability this responsibility may bring (e.g. Signed statement of understanding or an evaluation).

5. The unit standard must state the conditions under which administrative privileges may be revoked.

a. The document must outline the process used to make revocation decisions (e.g. whether it can be made by one person or requires review by a committee)

b. The standard must define the notification process (e.g. notification to the user that access has been revoked, why it has been revoked, and how to request reinstatement).

c. OIS may get involved in "severe" cases (e.g. data breaches) and may request local units suspend administrative privileges from users involved in security incidents.

d. The reinstatement process should be the same as the appeals/ exception process and described within the standard document. This document should identify any additional considerations involved in reinstatement decisions. Reinstatement decisions must be documented and communicated to the end user in the time frame established for handling initial requests.

6. The Assistant Director, Information Security (or designee) must review and approve unit developed standard documents before adoption.

a. Units should submit draft privilege documents to the IT@UC Office of Information Security by sending them in e-mail to: infosec@uc.edu. OIS will respond to submitted drafts within 10 business days of receipt.

b. Approved standard documents must be posted to a staff and faculty accessible website. Members of a unit should have easy access to this document and the supporting educational or informational materials.

c. On approval, units must advertise the existence of the standard to local users.

7. Local standard documents and processes must be reviewed on a regular basis. The interval may be designed to best suit local resource requirements but should not exceed a biannual cycle.

a. Standards modified through local review must be resubmitted to the IT@UC Office of Information Security for approval.

8. The Office of Information Security must review this document and should update or modify the standard requirements as necessary on a biannual cycle.

Tools:

Appendix A - Local Administrative Privilege Standard Creation Checklist

Appendix B - Sample Process

Appendix C - Sample Training Curriculum/Outline

Contact Information

IT@UC Office of Information Security 513-558-ISEC (4732) infosec@uc.edu

History

Issued: 04/15/2015
Reviewed: 03/21/2017

Appendix A

Local Administrative Privilege Standard Creation Checklist

Step 1: Directive Creation	Met?	Comments
Review the standard document from the OIS		
Standard author(s) should evaluate current use of admin privileges on unit computer systems		
Classify overall roles of users inside unit: (common examples below)		
Research		
Software Development		
Teaching		
IT Operations		
Business Operations		
Mobile/Traveling Users		
Special/ Other roles		
Using the classifications, the author(s) should recommend and document the "default" administrative privilege level for users within unit roles		
Author(s) should determine the most common cases where users outside default roles can be granted administrative privileges		
Criteria for granting exceptions should be enumerated and determined for broadest examples. These broad factors should be documented in the standard		
Process for requesting admin privileges detailed and documented		
Appeal/exception process to grant privileges documented		
Step 2: Directive Review / Adoption		
Present standard to internal review committee		
Academic Units: Committee members must include at least 1 faculty representative		
Business Units: Committee may be comprised of any individuals assigned by unit management		
Hybrid Units: Committee must include at least 1 faculty representative (for example a Regional Campus)		
Committee reviews recommendations from standard author(s)		
Committee recommends adoption or requests revisions until it is prepared to adopt the standard		
Step 3: Final Approval		
Submit final directive statement to OIS for review/ recommendations		
Unit Committee responds to OIS review/recommendations modifies and resubmits or accepts comments and finalizes document		
Create form/e-mail or create help desk support process for privilege request		
Train support staff in request procedures		
Unit publishes final standard document		
Process goes into practice/requests are accepted.		
Approvals /denials documented		
Policy reviewed on regular basis for relevance		

Appendix B

Sample Local Administrative Privilege Standard Process

Note: The OIS sample document is written from the perspective of a hypothetical academic unit. Modifications may be necessary for units that do not follow the academic model.

Default Administrative Privilege Assignments:

Research – Administrative privilege assigned to head of research unit along with ability to delegate administrative responsibility to other members of the research unit on computers and equipment assigned to the research unit.

IT Staff – Administrative privileges are granted within the scope of the staff members area of responsibility. IT Staff members are granted administrative privileges only on those assets necessary for them to accomplish assigned job duties.

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

Exception Criteria:

Mobile/traveling user – The user often uses their assigned computer outside of the normal working hours or is not located in an area that the unit can support them.

User with specialized software – Software the user requires for the normal performance of their job does not allow non-administrative execution or is written in such a way as it requires the user to run as an administrator on the system.

Request Process

Users may request administrative privileges by contacting the IT support staff. The staff will respond to the request 10 business days. Urgent requests should be noted along with any information IT staff members may need to know prior to enabling the user's administrative access.

Users who do not fit the established roles which allow administrative privileges may request an exception by completing the attached form and sending it via email to the lead IT administrator for the unit. Requests will be considered within 5 business days of receipt and a ruling will be delivered to the requester within 5 additional business days.

Appeal Process:

Users whose request for administrative privileges is denied may appeal the decision to the unit Admin Privilege Committee. The committee may be reached by communicating the initial need and response from the IT administrator to the committee members (who are listed at xxx.xxx.xxx/xxx). The committee will respond to appeal requests in writing to the requester within 10 business days.

Users who wish to appeal a committee decision may opt to involve the Chief Information Officer (or representative) for a final arbitration. The ruling of the CIO or designate is considered binding and final.

Approval Duration:

Due to the evolving nature of technology and the changing roles of users at the university all requests for Administrative Privileges will be reviewed on an annual basis. This review will verify that the need stated in the request is still valid and/or that the employee still requires the approved access.

Education Requirements:

Users who are granted local administrative privileges must read the "Administrator Risks" pamphlet located at buckeyesecure.osu.edu/xxxx and must sign and agree to the Local Administrative Privileges Risk Agreement and submit it to the IT administrator.

Privilege Revocation:

User administrative privileges may be revoked for the following reasons:

- User no longer serves in a role that requires them.
- User no longer utilizes software that requires administrative privileges.
- User is involved in a data breach that is related directly to their having administrative privileges.
- User demonstrates unsafe practices while using administrative privileges.
- The unit determines that the user no longer needs administrative privileges to perform job tasks.
- User requires excessive support from unit IT staff as a result of having administrative privileges.

Decisions to revoke user administrative privileges will be made collaboratively by the IT administrator and the department head based on documentation of any of

the above conditions. Revocation of privileges by the unit will be communicated in writing to the user upon execution.

Users may request reinstatement of their previously granted administrative privileges using the exception/appeal process. The decision process may consider the documentation and decision that led to the revocation in the restoration decision.

Users whose administrative privileges are revoked may appeal the decision or request reinstatement at a later time with the unit Admin Privilege Committee. The committee may be reached by communicating the initial need and response from the IT administrator to the committee members (who are listed at www.uc.edu/xxx) The committee will respond to appeal requests in writing to the requester within 10 business days.

Document Posting and Review:

The approved Local Administrative Privileges document will be posted for staff and faculty at www.uc/xxx. The document has been reviewed and approved by the OIS and will be subject to local review and updates on a biannual basis based upon the date of last review.

Appendix C

Sample Training Curriculum/Outline

Local units are encouraged to develop an educational component to complement their locally developed administrative privilege standards. This training component should highlight the responsibility of being given administrative privileges, personal responsibility for ensuring the computers maintain compliance with the CCSS or any other security requirements as well as the dangers and threats associated with operating a computer using administrative privileges.

Units also should include clear direction for those granted these responsibilities with regards to any changes in internal support processes (i.e., if they need to follow a different process to get help from the unit IT staff). A rough outline of this suggested training component is listed below.

Units who wish to share their completed documents can submit them to Infosec@uc.eduand they will be added to this page as an example for other units to adapt/modify.

Outline:
I. Define administrative privilege and local policy on administrative privilege
II. University Policy education (i.e. Security Standards, Data Governance & Classification Policy, Vulnerable Electronic Systems Policy, Acceptable Use of University Information Technology Resources Policy and any local department policy)

a. What do you need to comply with
b. How do you comply
c. What to do if you can't comply
d. How to ensure you don't do something to remove compliance (I.e. remove the firewall, uninstall anti-malware software, etc.)

III. Common Risks

a. When you should and should not use administrative privileges
b. Applications that are dangerous to use while using admin privs.
    i. Internet Browsers
    ii. E-mail clients
c. Best Practice for various Operating systems
    i. Windows
    ii. Macintosh
    iii. Unix/Linux
d. Software update/installation considerations