CFAES Local Administrative Privileges Standard

Version 1.0 -January 25, 2013

Overview

Regular use of computers employing the enhanced privileges granted to administrative users may seem like the best way to reduce the impact of constant program changes and software updates while providing the flexibility to install software easily without disruption. Unfortunately, this practice exposes computers and users to risks that do not exist when running with normal user privileges.

The ability to make changes to a computer's operating system core components - a necessary privilege for system administration - can lead to inadvertent changes being made by users or the unexpected installation of malicious software by malware and websites.

The purpose of the CFAES Local Administrative Privileges Standard (LAPS) is to establish a college policy for the assignment and management of administrative privileges. The university requires that each college adopt a LAPS with the express purpose of limiting the use of administrative privileges to reduce business risk.

Described in the following sections are the procedures for the assignment of administrative privileges for faculty and staff, how employees may request administrative privileges, and how administrative privileges will be managed.

Administrative Privilege Assignment:

Faculty and Non-IT Staff – Administrative privileges are assigned to individual faculty and non-IT staff by the Chair, Director, or unit leader of the department, school, institute, or service unit. The Chair, Director, or unit leader will consult with their respective IT staff to determine an appropriate default assignment for their employees with the understanding that the use of administrative privileges should be limited.

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

Request Process:

Faculty and staff members may request administrative privileges by contacting their department, school, institute, or service unit's IT staff. IT staff will work in a collaborative manner with the requester to determine if administrative privileges should be granted and will make a recommendation to the requester's department/unit leader. The decision to grant or reject the request is the responsibility of the department/unit leader. The IT staff will provide the relevant Chair, Director, or unit leader with the request and the leader will provide direction to the IT staff as to how to respond to the request within 10 business days. Urgent requests should be noted along with any information IT staff members may need to know prior to enabling the requester's administrative access.

Appeal Process:

Faculty and staff members whose requests for administrative privileges are denied may appeal the decision to the CFAES IT Advisory Council. The council may be reached by communicating the initial need and response from the department/unit leader to the CFAES CIO via e-mail. The council will respond to appeal requests in writing to the requester within 10 business days.

Faculty and staff members who wish to appeal a CFAES IT Advisory Council recommendation may opt to involve the university's Chief Information Officer (or designee) for a final arbitration. The ruling of the university CIO or designee is considered binding and final.

Approval Duration:

Due to the evolving nature of technology and the changing roles of faculty and staff members 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:

Faculty and staff members who are granted administrative privileges must read the Administrative Privilege Risks Overview (located at http://itac.cfaes.ohio-state.edu/home), must sign and agree to the Local Administrative Privileges Risk Agreement, and submit the signed agreement to the relevant department/unit IT and human resources staff for inclusion in the personnel file of the employee.

Privilege Revocation:

A faculty or staff member's administrative privileges may be revoked for the following reasons:

- User no longer serves in a role that requires administrative privileges
- 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
- User configures administrative privileges for another user without following the procedures outlined in this document
- The department/unit leader determines that the user no longer needs administrative privileges to perform job tasks
- User requires excessive support from department/unit IT staff as a result of having administrative privileges.

Decisions to revoke a faculty or staff member's administrative privileges will be made by the relevant department/unit leader based on documentation of any of the above conditions. Revocation of privileges by the department/unit leader will be communicated in writing to the employee upon execution.

Faculty and staff members may request reinstatement of their previously granted administrative privileges using the exception/appeal process. The process may consider the documentation and decision that led to the revocation in the restoration decision. Employees whose administrative privileges are revoked may appeal the decision or request reinstatement at a later time by petitioning the CFAES IT Advisory Council. The Council may be reached by communicating the initial need and response from the relevant department/unit leader to the CFAES CIO via e-mail. The Council will respond to appeal requests in writing to the requester within 10 business days.

Document Posting and Review:

The approved Local Administrative Privileges Standard document, and supporting documents, will be posted at http://itac.cfaes.ohio-state.edu/home. The document will be subject to review and update on an annual basis.

Supporting Documents:

Administrative Privilege Risk Overview
Local Administrative Privileges Risk Agreement