

CFAES Local Administrative Privileges Standard

Draft v0.3 -May 04, 2010

Default Administrative Privilege Assignments

Tenured and Tenure-Track Faculty – No administrative privileges are granted. Administrative privileges may be provided to individual faculty by the department/unit head within the scope of the faculty members' area of responsibility based on need, and must be shared with appropriate IT staff. Employees requesting administrative privileges must complete educational requirements as defined below. Within departments, the right to grant administrative privileges may be delegated by the department/unit head to another member of the unit where appropriate.

Non-Tenured Faculty – No administrative privileges are granted. Administrative privileges may be provided to individual employees by the college department or Extension IT administrator within the scope of the employee's area of responsibility based on need, and must be shared with appropriate IT staff. Employees requesting administrative privileges must complete educational requirements as defined below.

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

Non-IT Staff – No administrative privileges are granted.

Exception Criteria:

1. Mobile/remote employee – The staff member often uses their assigned computer outside of normal working hours or is not located in an area where IT staff have the ability to provide support.
2. Employee with specialized duties or software – The staff member is required to perform duties that necessitate having administrative privileges, or the staff member must use software in the normal performance of their job that does not allow non-administrative execution or is written in such a way as to require the staff member to maintain administrator privileges on the system.

Request Process

Employees may request administrative privileges by contacting the appropriate IT administrator or the CFAES CIO. The IT administrator will respond to such a request within established service levels, but no later than 5 (five) business days after receiving notice. Urgent requests should be noted along with any information the IT administrator may need to know prior to enabling the employee's administrative access.

Appeal Process

An employee whose request for administrative privileges is denied may appeal the decision to the CFAES CIO or to the CFAES LAPS 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 determine web site location). The committee will respond to appeal requests in writing to the requester within 10 business days.

Employees who wish to appeal a decision by the CFAES CIO or the CFAES LAPS Privilege Committee may involve the university's Chief Information Officer (or his/her 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 employees at the university, all requests for administrative privileges will be reviewed on no more than a biannual 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

Employees who are granted local administrative privileges must read the "Administrative Privilege Risks" pamphlet located at <http://buckeyesecure.osu.edu/pmwiki/uploads/Policy/LAPS-Training.pdf>, must sign and agree to the CFAES Local Administrative Privileges Risk Agreement, and submit the signed agreement to the appropriate IT administrator.

Privilege Revocation and Reinstatement

An employee's administrative privileges may be revoked for the following reasons:

- Employee no longer serves in a role that requires administrative privileges
- Employee no longer utilizes software that requires administrative privileges
- Employee is involved in a data breach that is related directly to their having administrative privileges
- Employee demonstrates unsafe practices while using administrative privileges
- The college determines that the employee no longer needs administrative privileges to perform job tasks.

Decisions to revoke employee administrative privileges will be made collaboratively by the IT administrator and the appropriate department/unit head based on documentation of any of the above conditions. Revocation of privileges by the college will be communicated in writing to the employee upon execution.

Employees may request reinstatement of their previously granted administrative privileges using an exception/appeal process. The exception/appeal 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 contacting the CFAES CIO or the CFAES Administrative 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 determine web site location). The committee will respond to appeal requests in writing to the requester within 10 business days.

Document Posting and Review

The approved CFAES Local Administrative Privileges Standard document will be posted for staff and faculty at (determine web site location). Approval requires review and acceptance by the university's Office of the Chief Information Officer. The document will be subject to CFAES review and updates on no less than a biannual basis based upon the date of last review.

Supporting Documents (Under Development)

CFAES Administrative Privilege Exception Request Form

CFAES Local Administrative Privileges Risk Agreement