Department of Biomedical Engineering
Local Administrative Privileges Document

Default Administrative Privilege Assignment

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.

Faculty, non-IT staff, and students – No administrative privileges are granted.

Exception Criteria

Mobile/travelling 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.

Research – Research groups may choose to administer their own computers with one or more designated administrators.

Responsibility

Users with administrative privileges share responsibility for understanding, following and enforcing all Departmental, College and University policies and standards.

Audit

All systems placed on the BME network are subject to audit by IT staff.

Request Process

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

Appeal Process

Users whose request for administrative privileges is denied may appeal to the Biomedical Engineering Computer Committee. The committee may be reached by communicating the initial need and the response from the IT manager to the committee members. The committee will respond to appeal request in writing within 20 business days. Final appeals may be made to the Biomedical Engineering Chair.

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 user still requires the approved access.

Education Requirements

Users who are granted local administrative privileges must:

- Read the "Administrator Risks" pamphlet located at http://buckeyesecure.osu.edu/notfinished
- Read the Minimum Computer Security Standard (MCSS) located at http://buckeyesecure.osu.edu/Policy/MCSS
- Read the Institutional Data Policy (IDP) located at http://cio.osu.edu/policies/institutional_data
- Take the IDP Training. Instructions are located at http://buckeyesecure.osu.edu/Policy/InstitutionalDataTraining
- Sign and agree to the Local Administrative Privileges Risk Agreement and submit it to BME IT manager

Privilege Revocation

Administrative privileges may be revoked for the following reasons:

- User no longer needs administrative privileges to perform job tasks
- User fails to comply with Departmental, College, and University IT policies or standards
- 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 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 Biomedical Engineering IT manager and the Biomedical Engineering Computer Committee based on documentation of any of the above conditions. Revocation of privileges will be communicated in email to the user upon execution.

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

Document Posting and Review

The approved Local Administrative Privileges Document will be posted at http://www.bme.ohio-state.edu/bmeweb3/bme_policies.html. The document will be reviewed by the Office of the Chief Information Officer and will be subject to local review and updates on a biannual basis based upon the date of last review.