EMORY UNIVERSITY SCHOOL OF MEDICINE | Department of Medicine

Administrative Privileges Policy

Responsible Official: Department of Medicine IT Manager
Administering Division/Department: Department of Medicine (DOM)
Effective Date: 10/10/2017 **Last Revision:** 10/10/2017

I. Overview[1]

Administrative privileges (also referred to as root privileges) allow a user to install software, change system configurations and other settings and modify users on computers. As a general practice, users are given non-administrative privileges to protect the integrity and security of the University computing environment. The following risks are associated with the use of administrative privileges:

- Ability to install software that interferes with normal operating system or application behavior.
- Intentional or unintentional changes made to the system that causes it to fail or operate in an unexpected manner.
- Malicious software that takes advantage of administrative privileges to infect the system.

II. Applicability

This policy applies to all desktop and laptop computers financed and supported by the Department of Medicine, even if they reside in space owned by an entity other than Emory University. This policy does not apply to personal devices, those financed and supported by Emory Healthcare, the Veterans' Health Administration, or Grady Health System.

III. Policy Details

1. DOM IT staff will have administrative privileges appropriate for the scope of their responsibilities.
2. All other members of the Department of Medicine are by default not granted administrative privileges.
3. The installation of standard DOM software and repair of computer systems is the primary responsibility of the DOM IT staff.
4. Only DOM IT staff may be granted administrative privileges to a computer that does not have a permanent or temporary connection to the Emory network for essential security updates.
5. Compliance regulations preclude DOM users from having administrative access to machines that host sensitive data governed by the VA or that manage or store data covered by federal contracts.
6. A user may apply for administrative privileges (Section IV) for the following reasons:
    a) The sole use of the system is to operate equipment used for research purposes.
    b) The user requires administrative privileges to fulfill his/her job responsibilities.
    c) The system runs software that is not provided by the University or Healthcare Software Distribution Centers and is not supported by DOM IT.

[1] Adapted from the Emory College Administrative Privileges Policy

IV. Process to Obtain Administrative Privileges

1. To receive administrative privileges, users must submit a “Request for Administrative Privileges" to DOM IT which will retain copies of all requests. A request can be submitted via an online form or by email using an interactive PDF (both can be found on the DOM IT website: http://medicine.emory.edu/faculty-staffresources/it-resources.html).
2. Each case will be reviewed by DOM IT for appropriateness; not all cases may be approved.
3. Administrative privileges will be granted through the procedure most appropriate for the operating system platform.
    a) Windows XP – Administrative rights will be granted through creation of a second local administrative account. **no longer a supported operating system**
    b) Windows Vista – Administrative rights will be granted by giving administrative privileges to the user's domain account. **no longer a supported operating system**
    c) Windows 7, 8, and 10 – Administrative rights will be granted by giving administrative privileges to the user's domain account.
    d) Mac OS X – Administrative rights will be granted by giving administrative privileges to the user's domain account.
    e) Linux – Administrative rights will be granted by adding the user's account to the "sudoers" file.
4. The Principal Investigator of a research group may request administrative privileges for a limited number of users. A justification must accompany the request. The PI is responsible for ensuring full compliance with this policy by all members of his/her lab or research group.
5. No user will be granted administrative privileges on a laptop computer unless encryption software is installed by DOM IT.

V. User Responsibilities

If granted administrative privileges, the user agrees to the following:

1. Any changes made to the computer or software/hardware downloads will be for the sole purpose of fulfilling job responsibilities.
2. The user will retain copies of non-standard software licensing for the purpose of accounting during annual DOM audits.
3. The user will abide by SOM/DOM IT policies.
4. The user is responsible for re-installing any data or software lost if it becomes necessary for the DOM IT staff to reformat the machine due to issues caused by the user having administrative privileges.
5. The user will reset his/her administrative privileges password once every six months to prevent security breaches. The same password should not be reused two consecutive periods.
6. The user will never share his/her password with another user.
7. The user will immediately report any technical failures or security breaches to DOM IT.
8. The user will not block, disable, or revise any services that may prevent routine updates.
9. The user will read and abide by security updates distributed to all users with administrative privileges and will certify that they have read and understand these updates.

VI. Revocation of Privileges

The Department of Medicine IT Manager reserves the right to revoke administrative privileges and will communicate in writing to the user prior to revocation. Administrative privileges may be revoked for the following reasons:

1. The user is involved in a data security breach that is related to his or her having administrative privileges.
2. The user demonstrates unsafe or unlawful computing practices such as the intentional downloading of malicious software, software piracy, or the downloading of copyrighted content.
3. The user does not comply with SOM/DOM IT policies and procedures.
4. Administrative privileges are no longer needed to perform job duties.
5. The user requires excessive support from DOM IT staff as a result of having administrative privileges.
6. The user does not abide by the responsibilities outlined in Section V *(User Responsibilities)* of this document.
7. Any resulting revocation of privileges will be discussed with the DOM IT Steering Committee by DOM IT Manager, who will review all cases for severity and intent.
8. Any other reason identified by the DOM IT Steering Committee or the DOM IT Manager as necessary and confirmed by the DOM IT Steering Committee.

The Department of Medicine IT Manager will keep records of requests related to administrative privileges and will present these to the DOM IT Steering Committee and the DOM IT Faculty and Staff Advisory Committee on a quarterly basis.

VII. Appeal Process

A user whose administrative privilege request has been denied or revoked may file an appeal in writing to the Chair of the Department of Medicine.

VIII. Approval Duration

The DOM IT team will review long-term requests annually or upon reimaging or renewal of a system to ensure that the reason for each request is still valid. It is the responsibility of the DOM IT Manager to schedule these reviews.

IX. Department of Medicine Responsibilities

- All Department of Medicine personnel must comply with this policy. Managers and supervisors should ensure compliance.
- DOM IT staff will respond in a timely manner to requests and contact the user prior to arriving in person to ensure the user is available. Whenever possible, DOM IT staff will use remote access to fulfill requests.
- If the user feels he/she is not receiving proper customer service, he/she should contact the DOM IT Manager.
- The DOM IT Steering Committee and the DOM IT Faculty and Staff Advisory Committee will maintain and update this policy as necessary.

X. Related Links

- Current version of this policy
- Emory IT policies
- Contact Department of Medicine IT

XI. Contact Information

For clarifications on this policy, please contact the DOM IT Manager.