IUPUI
SCHOOL OF SCIENCE

Computer Administrative Rights Policy

Reason for Policy:

This policy is intended to support the goal of insuring the highest level of stability and usability for computers. This is based on the premise that computers are a productivity tool where stability and usability are most important. In such an environment, limiting administrative privileges is an IU "best-practice" and requirement of IU IT policy 12. One of the most effective ways to shield yourself from viruses and spyware is to not log on to your computer as an administrator. Administrative rights are typically reserved for IT personnel who are responsible for providing administrative services such as system maintenance and user support.

On Windows and Macintosh computers, a user may require administrative privileges to:

- install software
- install hardware
- modify system settings

On Linux, a subset of administrative permissions can be granted via sudo to provide the functionality listed above. IT personnel will work closely with you to make ensure the sudo configuration to best meet your needs.

These tasks are restricted by default since they can have a profound impact on the stability and usability of a computer. The associated risks with use of administrator access include, but are not limited to:

- Users intentionally or unintentionally installing malicious code or software from unreliable sources potentially increasing the risk of exposure to viruses, worms, spy-ware, keystroke loggers, phishing software and Trojan horses on campus computers, servers, and on the network.
- Users intentionally or unintentionally making changes to the security configuration of the system making the system more vulnerable to attack.
- Users intentionally or unintentionally installing unlicensed software or copyrighted material
- Users intentionally or unintentionally installing unapproved software or patches that could compromise the stability and performance of the system.

The School provides trained and experienced support staff to perform these functions. Due to the inherent dangers of inappropriate, uninformed, or unintentional use of logins with administrative rights, **the School of Science policy is to restrict the use of administrative rights.**

In unique instances, it may be necessary for administrative rights to be issued to faculty or staff on either a temporary or ongoing basis to perform tasks within the scope of their research or employment. This policy provides a procedure to authorize users for administrative rights and regulate the granting of administrative rights.

Authorized users must have the knowledge to configure and manage their workstations and possess an understanding of the responsibility of following appropriate security practices. It is not necessary (and a violation of IU IT policy 12) for users to always be logged in as an administrator. Authorized users will be provided a secondary account with administrative access rights to their local computer. Use of this account will enable the authorized user to install software, and manipulate the required system settings on their workstations when necessary. As a rule, students will not be granted administrative access except in cases where the course work or research requires it (primarily computer science). In this case alternative departmental forms may be required.

School of Science
Computer Administrative Access Request Form

Users requesting administrative access must complete this form and submit it to the IT group. The access will be for a specific computer and the access will expire when the computer is retired or admin access is no longer required. A form must be submitted and will be kept on file with the IT group for each computer for which administrative access is required.

Date:

User Information
First Name__________________________
Last Name__________________________
Department_________________________
Username___________________________
Phone______________________________

System Information
Manufacturer_________________________
Model ______________________________
Operating System_____________________
Computer Name______________________
Serial Number/Service Tag______________
Location Bldg.______ Room_____________

Reason Administrative access is required

Authorized users are required to log in using their primary account (without administrative rights) for routine computer use and only utilize the administrative access account when system administration (e.g., software installation, reconfiguration) is required.

Authorized users must not:

- install or use software that are considered insecure
- download software that is malicious to the network
- download unlicensed/illegal software
- download copyrighted material without permission
- download software containing viruses or Trojans
- access data or profiles belonging to other users (IU policy IT 7)

I agree to the points above and understand the caution required when using administrative access. I understand that any data lost as a result of this decision may not be recoverable.

Signature ____

Received by ____