



CEHS Office of Technology Services Local Administrative Rights Procedures

A local administrator is a person who has access to manage her or his own computer. The responsibilities of a local administrator involve operating system, hardware installations and configurations, application installations, and upgrades. Generally, it is against University and College policy for users to have administrative rights for a computer. In fact the MSU Office of Information Technology (OIT) will not provide technical support to users with any level of local administrative rights. However, in exceptional cases CEHS faculty and staff are given some of those rights when needed to more easily do their job. Those rights come with responsibilities that are important for preventing future technical problems.

It is essential to make computer security a priority—that is, to maintain a secure computing environment free from risk or danger by mitigating the vulnerabilities associated with computer use. A vulnerability can be caused by the installation of a program available on the internet that has malicious or poorly written code that could cause a program to stop working (e.g., a new screen saver, tool bar, game).

A computer's performance may also degrade over time due to potentially legitimate software that includes features that slow down the computer—for example, software that is bundled together (containing more than one application upon installation). Also, when a computer's system disk is running out of space, users may assume that deleting files and/or folders is appropriate. But without proper knowledge, this can be dangerous as important systems files can be deleted accidentally. These actions make an administrator's job more difficult because s/he needs to spend more time troubleshooting issues that could have been avoided.

Faculty and staff who have administrative rights for their computers should adhere to the following recommended best practices to avoid potential technology issues:

- **Only download software directly from the vendor or developer websites.**
 - Software should ONLY be installed by CEHS Technology Services. If you need to download free software, please consult the CEHS Technology Services staff prior to downloading to ensure that the program is safe.
- **Avoid installing any “Helper” or “Memory Booster” applications, e.g., MemCleaner or Registry Booster.**
- **Ensure that all operating systems and application-specific updates are enabled.**
 - Windows – Click on Start button – Click on Control Panel – Click on Automatic Updates (make sure “automatic” is selected). If you need assistance, please contact CEHS Technology Services.
 - MAC – Click on Apple Menu – Click on System Preferences – Click on System

Updates icon (make sure “check for updates” is enabled and “download important updates automatically is checked also). If you need assistance, please contact CEHS Technology Services.

- **Do not upgrade your operating system on your own.**
 - If you believe your system needs to be upgraded, please contact the CEHS Technology Services staff for assistance.
- **Keep local firewalls enabled at all times.**
 - Windows – Click on Start button – Click on Control Panel – Click on Windows Firewall (make sure “on” is selected on the general tab). If you need assistance, please contact CEHS Technology Services.
 - MAC – Click on Apple Menu – Click on System Preferences – Click on Security & Privacy – Click on Firewall tab – Click “Turn On Firewall.” If you need assistance, please contact CEHS Technology Services.
- **Double check your anti-virus protection to make sure it is receiving updates automatically.**
 - Windows – Click on Start button – Click on Programs – Click on Sophos Anti-Virus. Open the application look at the “last update” date and make sure it is current with today’s date. If the date is not current, please contact CEHS Technology Services staff immediately for assistance.
 - MAC – Click on the doc bar – Click on Applications – Click on Sophos Anti-Virus. Open the application click on “scan this mac”. If any viruses appear please contact CEHS Technology Services immediately for assistance.

***** CEHS Technology Services reserves the right to adopt the University policy and not provide technical support to individuals who violate the safeguards listed in the procedures above. *****