Administrator Privileges Training Guide

What are Administrator Privileges?

The first step in understanding the responsibility and accountability when granted administrative control and access to a university-owned and -managed computer system is to define the concept of “Administrator Privileges.”

Modern computers, especially those based upon versions of Microsoft’s Windows operating system, often assume that users are the sole administrators of the device. Users are often responsible for performing regular software maintenance tasks like upgrades and software installation.

This assumption often makes sense when considering computers that are not a part of a formal Information Technology (IT) support area (such as in home networks or using mobile systems) or where the primary users are fully trained IT experts. However when computers and computing resources are fully supported by trained support staff, the need for the average user to undertake these maintenance tasks is unnecessary and in fact can pose a risk to the reliable operation of the devices.

Computers, like automobiles, are increasingly complicated tools. While many automobile owners may perform limited maintenance and service on their own cars, most take their problems to trained professionals who can diagnose and evaluate the complex set of inter-connected parts that make up a car. Users should consider relying on a trained expert for computer support.

It is expected that most users will not have administrator privileges when using supported computers. Operating without administrative privileges means they can focus upon the work they need the computer to do rather than the responsibility and accountability surrounding security, system updates, and maintenance.

Protecting university staff and resource time while allowing users to accomplish work requires that we adopt a philosophy called “least privilege”.

The concept of limiting access, or “least privilege,” is simply to provide no more authorizations than necessary to perform required functions. This is perhaps most often applied in the administration of the system. Its goal is to reduce risk by limiting the number of people with access to critical system security controls; i.e., controlling who is allowed to enable or disable system security features or change the privileges of users or programs.\(^1\)

\(^1\) NIST Special Publication 800-27, Engineering Principles for Information Technology Security. Principle 24 – Implement Least Privilege
Users granted administrator privileges have a greater ability to impact the operation of their computer than those operating under everyday system user privilege levels. User accounts on most operating systems carry a level of authorization (often referred to in computing terms as “privilege”) that ensures that users who are tasked to accomplish their regular daily work do not make inadvertent or accidental system changes.

Access to a computer at greater levels of privilege also confers a certain level of responsibility upon the user to follow safe security and administrative practices that doesn’t necessarily carry over to other roles.

Microsoft and other operating system designers recommend that everyday users maintain two distinct accounts to protect the system from accidental harm during normal operation.

**Local Administrator Privileges and IT Support**

The nature of computers today means that software updates and security patches often interrupt the regular business of the user. Upgrading software, performing regular security checks, and installing new applications or hardware are all services that the local unit provides to its faculty and staff, allowing users to instead focus on the important work they must accomplish.

Trained IT support staff manages these systems for the university, and while they are a finite resource, the university uses these trained professionals to maintain a reasonable level of support, as determined by local funding and availability. The local IT staff works to ensure the smooth operation of these tools. Using IT support resources allows faculty and staff to focus on accomplishing the goals of the department, college, and university to our students, peers, and community.

Maintaining the stability and smooth operation of our computer systems requires that the IT staff have a good understanding of the changes made to the computer systems and the needs of the users. The more users who can change the configuration and operation of a computer system the more complicated it becomes to diagnose and repair a system when an error occurs. Unexpected or untracked changes remove the computer from operation, leaving the system’s user without the resources for a period of time and impacting the efficiency and effectiveness of that employee.

Local Administrator Privilege Standard exist within a university area to make it clear what level of training and support is available for users who need “Administrator Privileges” outside the IT support organization.
“Administrator Privileges” are determined at different organizational levels to allow the most flexibility needed to support the goals of faculty and staff throughout the diverse landscape of the university.

The Fisher College of Business Local Administrator Privilege Standard can be found at the FCOB Information Technology Services web site (http://fisher.osu.edu/technology/).
Ohio State University Security Policies and Standards that All Administrator Privileged Users Must Understand

Computer administrators and IT support professionals at The Ohio State University need to be aware of the requirements and expectations placed upon them by the university and college security policies and standards. These requirements can be found in the following locations:

- Buckeye Secure website (http://buckeyesecure.osu.edu/Policy)
- University CIO (http://cio.osu.edu/policies/)
- Fisher Information Technology Services website (http://fisher.osu.edu/technology/)

A quick summary of some of the most important policies however can be found below:

**University Minimum Computer Security Standard (MCSS):**

Computer Administrators must ensure that all computers meet the following requirements:

- The device must be guarded by an up-to-date and active firewall set to protect it from unauthorized network traffic.
- Current operating system and application software with current security patches must be installed.
- The device must be protected against malicious or undesired software such as viruses, spyware, or adware.
- Access to the device must require appropriate authentication controls such as account identifiers and robust passwords.

**Policy on Institutional Data:**

- Computers containing data that the university classifies as restricted must be protected. On portable computers and removable media this requires the computer to be encrypted. A list of restricted data can be found at Buckeye Secure. (http://buckeyesecure.osu.edu/Policy/RestrictedDataElements).

Additional requirement administrators need to be aware:

- Each user on a computer must use an individual logon and may not share passwords.
How Do You Comply with These Requirements?

Making sure your computer meets the requirements varies depending on the operating system version installed on your computer. Typical Windows and Macintosh computers include some of the software needed to comply with the MCSS; however, Linux and other systems will require work to make compliant.

Windows:

Windows computer users will find that under Windows XP service pack 2, Windows Vista and Windows 7 has a firewall, and an automatic process which downloads and installs the latest critical security updates. Anti-malware is not included in all versions of Windows so you will need to research programs that will offer you this protection. Fisher Information Technology Services provides Trend Micro anti-virus software and Windows Defender for anti-malware protection. The university provides McAfee anti-virus and anti-spyware software via the University’s Site-Licensed Software service (http://osusls.osu.edu/).

Some versions of Windows also include a form of encryption that can be used to protect restricted data. The University and various departments also license programs to encrypt the data on portable computers. Information Technology Services recommends and provides PGP whole disk encryption.

When creating additional user accounts on the computer, ensure that they are not administrative accounts and that they have a password set.

Macintosh OS X:

OS X 10.5 (Leopard) and later versions (Snow Leopard) of the operating system include an Application Firewall. You should work with local IT Support staff or reference how to configure this tool on Apple’s support website.

Apple system update is configured to automatically download and install new system updates and patches.

Anti-malware offerings for the Macintosh include McAfee’s Virusscan product, which is licensed by the university. You can download the software via the University’s Site-Licensed Software service. (http://osusls.osu.edu/)

When creating additional user accounts on the computer, ensure that they are not administrative accounts and that they have a password set.
Macintosh OS X computers include the FileVault encryption software. This program encrypts information stored in user home directories and allows a master decryption password, separate from the user’s password to be set. More information about FileVault can be found online (http://www.apple.com/) or contact ITS for assistance enabling this program.

Linux:

Most distributions of Linux include rudimentary firewall software. Anti-malware may be more troublesome to find however. Linux distributions also use varied methods of maintaining patches and security updates, some common methods use the Application Manager (or Wheel) to download updates to installed packages but you should investigate how your particular version of Linux handles this process.

User accounts created in Linux should not be added to the Administrator group and must have passwords set upon creation.

Encryption products exist for Linux, such as TrueCrypt. Mobile Linux systems containing restricted data elements must be encrypted using some form of storage encryption.

What To Do If You Can't Comply

Due to the nature of the work done here in the academic environment of the university, there are often situations that make maintaining MCSS and other standard compliance difficult or impractical. Older software often breaks when installed on new or updated operating systems, instrumentation and accessories may not have drivers under new operating systems, etc.

If the computers you are managing cannot be made compliant contact ITS for assistance.

How To Ensure You Don't Do Something To Remove Compliance

Understanding the requirements and the nature of system administration is only the first step in remaining compliant with administrative requirements. Once you have met the requirements, it is also important that you do not install software that disables these protections or uninstall the components that make these protective programs function properly.

Don’t install random software you find on the Internet just because you think you need it. Even if you can install software on your own, your local IT staff often has a better sense of the provenance and potential risks of many packages you may consider installing: check with them first before installing software you are not VERY familiar with.
Conduct a regular check of your system to ensure that all the previously configured and installed software packages are still in place. Additionally be careful when adding new software that you do not make drastic changes to the protective software that makes it ineffective in protecting your system. For instance new programs often ask for permission to modify firewall configurations to allow communication – be aware of what that configuration change is before clicking OK and accepting the change.

Ensure that your anti-malware software is set to update regularly and regular scans or detection processes are occurring. Having anti-malware software that is out of date or not configured to run is the same as not having any at all when it comes to protecting the data and operation of your computer.
Administrative Privilege Risks

Regular use of computers using the enhanced privileges granted to administrative users may seem like the best way to keep the impact of constant program changes, software updates, and the flexibility to install software easily without disruption, but in fact, it exposes computers and users to risks that do not exist when running with normal user privileges.

The ability to make silent changes to the operating systems core components, a necessary privilege for system administration, can often lead to inadvertent changes being made by users, or the installation of hidden software by malicious software and websites.

Web Browsers and E-Mail Clients

The two most dangerous activities users engage in during normal everyday usage are browsing the Internet and reading e-mail. The criminal threats use both these behaviors to attack users and so it becomes important to segregate these activities from administrative accounts.

Users who browse the web and encounter a malicious website or a corrupted ad on an otherwise reputable web page increase the potential damage done by these applications when they have administrative privilege. E-mail attachments and infected messages also are common entries for malicious software changes.

While anti-malware software offers some measure of protection from these sorts of threats there is a period of time between the initiation of a new threat and when the security programs catch up and block it when a computer is vulnerable.

Newer versions of the Windows operating system are designed to minimize the ability of these programs to make changes to the system by isolating the everyday tasks of the user from that of an administrator. Operating a computer as an administrative user effectively negates these protections.