

Administrative User Accounts

Administrative user accounts are by far the number one target for someone trying to gain illegal access to a network and its resources. This type of account must be protected above all other accounts to ensure that we/you are not left vulnerable to the tools, tricks, and exposure that this account accommodates.

When you log on to your computer as an administrator to perform common application-based tasks, you make it and other computers on a network vulnerable to malicious software and other security risks because malicious software will run with the **same privileges** you used to log on. If you visit an internet site or open an e-mail attachment, you can damage the computer because malicious code could be deployed that will download and execute on your computer. Malicious code can, among other things, reformat your hard disk drive, delete your files, and create a new user account that has administrative privileges.

Because of the risks associated with local administrative user accounts ITS at MCC employs what is known as “The Principle of Least Privilege”. Created by Microsoft, this principle is designed to achieve the lowest risk level possible in a network environment.

The principle is simple, and the impact of applying it correctly greatly increases our security and reduces our risk. The principle states that all users should log on with a user account that has the absolute minimum permissions necessary to complete the current task and nothing more. According to Microsoft most organizations have this principle in place and most security-related training courses and documentation discuss the implementation of a principle of least privilege, but many organizations fail to enforce them.

In order for this principal to be effective at MCC it is applied to all college owned computers.