Local Administrative Rights and Privileges Policy 6026

Policy Statement

Southeastern Illinois College (the "College") provides electronic information resources and other technological resources to support the College's educational mission and business purposes. Students, faculty, staff and all members of the College community who use the College's technology and computer-based resources are required to adhere to this Policy. Misuse of information technology resources presents security and privacy risks both to the College and user.

Scope

Policy applies to all computer hardware and software owned or operated by the College as well as the College's electronic mail, systems, websites, on-line classes and any other College network resources. "Use" of the College's network includes use of or obtaining access to its wired or wireless network from any electronic device whether or not owned or operated by the College.

There are many different types of administrator access levels and accounts for College's equipment, hardware and software. Frequently, the roles and access of the "administrator" is determined by the hardware or software vendor.

This Policy addresses what is commonly referred to as Local Administrative Rights and Privileges on an individual user's computer, tablet or device.

Definitions

Local administrative rights and privileges means online access that allows a single user total control over the operating system and files on a specific computer or similar device.

Principal of Least Privilege (POLP)

The principle of least privilege (POLP) recommends that users, systems, and processes only have access to resources (networks, systems, and files) that are absolutely necessary for normally assigned duties and nothing more. Ransomware is most commonly spread through phishing emails that contain malicious attachments or when a user unknowingly visits an infected website and then malware is downloaded and installed without the user's knowledge. By imposing POLP restrictions on users of computer systems, there is significantly reduced risk of an attacker gaining access to a higher-privilege or administrator account needed to install malware, ransomware, or use accounts undetected to perform malicious and destructive acts to steal and destroy data.

Local Administrative Rights and Privileges

Local administrative rights and/or privileges are limited to IT department staff. This limitation serves to significantly reduce risks to the College and is consistent with the Principle of Least Privilege. Decisions on who has local administrative rights and privileges within the College's IT Department is determined by the Senior Network and Security Administrator and Chief Information Officer (CIO) in consultation with the Cabinet Supervisor. Final approval rests with the Chief Executive Officer (CEO).

Disclaimer

This Policy and all its provisions are subordinate to local, state, and federal statutes.

Adopted: January 18, 2022
Amended: July 19, 2022
Legal Ref:
Cross Ref: