Monroe County Community College
Local Administrative Privilege Procedures

Policy Type: District Procedure

Policy Title: Local Administrative Privilege Procedure

Who Does the Policy Affect: Administrators, Faculty, and Staff

Purpose: The purpose of this procedure is to allow employees the ability to be granted privileged access to the workstation they are assigned

Definitions:

Local administrative rights is defined as computer access that allows a single user total control over the operating system and files on a specific computer. This access allows for some software updates and installation based only on their assigned computer.

Local Administrative Rights Application Process:

The colleges Chief Information Officer must establish a local administrative rights management process to ensure that only authorized individuals working at the college have total control of the operating system and files on their assigned computer. The process must at a minimum include: review of business need with direct supervisor prior to granting local administrative rights to those personnel who require such rights to perform their duties. Assessment of business need shall include review of availability of IT support staff to install or update software. When granting local administrative rights, the principle of least privilege will be strictly observed, *i.e.*, users will only be granted access to the minimum resources required for them to perform their official functions.

1) All users requesting local administrative rights (except for those who need access in the normal performance of their job responsibilities) must complete the Administrative Rights Access Form. The completed form will be reviewed and the need for local administrative access rights will be validated by the institution's Chief Information Officer.
2) A system for tracking and managing all users who have been granted local administrative rights shall be established, which shall include standard procedures requiring a recurring review and revalidation of all privileged access rights, at least annually.
3) Personnel who have been granted administrative access rights must adhere to all IT policies and lack of adherence may cause revocation of local administrative access rights.
4) Personnel who have been granted administrative access right must accept liability of any software installed along with the results of the software that is installed

Requirements for Use of Local Administrative Rights Privilege:

Users who are granted local administrative rights shall:

1) Use their administrative privileges only when needed to install or update software necessary to perform their job and report to IT any software that is installed
2) Apply changes only to an end-user device assigned to them
3) Adhere to the end-user license agreement associated with any software added

4) Comply with all existing MCCC policies including MCCC Acceptable Use Policy
5) Ensure that their end-user device is properly connected to the MCCC network so that it can receive scheduled software patches and upgrades
6) Take all reasonable steps to protect against viruses and other threats
7) Submit all software applications installed to IT
8) Be responsible for restoring any applications, configurations and associated data beyond the standard base image in the event of any failure of the device