Monroe County Community College
IT Computer and User Policy

Policy Type: District Policy

Policy Title: IT Computer and User Policy

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

Purpose: The purpose of this policy is to establish the guidelines for the general use of end user computing devices at MCCC. This policy covers all desktop, laptop, tablets or other end-user device that may be in use by an MCCC Computer User. This policy covers the general usage rights and expectation for all MCCC Computer Users.

Compute Devices

Information technology resources are used by individual employees, students, and other persons affiliated with the Monroe County Community College (MCCC). These resources are to be used for educational and business purposes in serving the interests of MCCC. Information technology devices are an asset to MCCC and as such any device that is assigned to an employee for college use should be properly cared for. Any staff member that is assigned a device will agree to follow procedure 6.50 (a).

Misuse of information technology resources poses legal, privacy and security risks, and the inappropriate use of privileged accounts significantly contributes to breaches of information security. To reduce the risks associated with potential misuse, the issuance of privileged accounts for performing local workstation and systems administration functions must be restricted and controlled. When privileged account access is required the employee will need to agree to procedure 6.50(b). Due to the widespread security issues of allowing privileged access to open access systems, there will be no administrative access given to an employee that are not a member of the IT department for a device that is not assigned to them as their single workstation.

Software

Software is an integral part of any computer system, and it can cause some of the greatest threats to any computer. All software must be vetted and approved by the Information Technologies Department to verify it should not damage computer systems nor allow external entities unauthorized access. To be able to accommodate the needs of the campus and to keep the college computer environment safe all software needs must follow procedure 6.50(c).

User Accounts

All IT access is assigned based on user account access. With the varying degrees of access to protected system there will be no sharing of individual accounts. Sharing of account credentials exposes not only the credential owner but the college to security risks. This does include any sharing of account credentials including sharing with your direct or indirect supervisor. To maintain the security and integrity of protected college documents all access must be approved through appropriate channels.

.

Adopted by the Board of Trustees 9-23-24