Monroe Community College
STATE UNIVERSITY OF NEW YORK

7.2 Password Policy

Category: Technology

Name of Responsible Office: Technology Services

Title of Responsible Executive: CFO / Vice President, Administrative Services

Date Established: June 3, 2013

Date Last Approved: January 29, 2024

Summary

To protect the security and privacy of College and personal information and to be compliant with auditing recommendations and governmental requirements, MCC will enforce password standards to ensure all authorized individuals accessing MCC resources follow proven management practices. The password standards will be enforced by automated system controls whenever possible, and the standards will be implemented on all MCC platforms when technically feasible.

Policy

Background

A college-wide password policy is widely accepted as the first line of defense against unauthorized access to network resources. Passwords are essential to protect sensitive data, for compliance, and for security of the college's systems. In addition to user ID and password requirements, multi-factor authentication is also required for MCC system access. This provides a second layer of protection for college systems and data in the event that a user's primary credentials are compromised.

Policy Statement

- Users are responsible for establishing unique passwords that comply with MCC password standards including length and complexity requirements.
- Users must protect their passwords from disclosure and should not record or store them insecurely. Passwords must never be revealed to anyone including other employees.
- The same password should not be used for MCC and non-MCC / personal accounts.
- Users must not share multi-factor authentication (MFA) codes or approve prompts unless they are for their own login.
- Password standards for length and complexity will change as needed to protect college data and systems from escalating cyber threats and to comply with increasing information security controls requirements.
- Passwords must not be re-used.
- Passwords will have a validity period and will expire at regular intervals and under certain conditions:
    - Users past due on cyber security awareness training will be subject to frequent password expiration until the training is completed
    - Passwords will be disabled upon detection of a compromised account (e.g. hacked as a result of a successful phishing attack)

  - New passwords will need to be established if and when password standards change.
  - Upon expiration, users must change to a new password that complies with current standards for length and complexity.
- Repeated failed login attempts will result in the account locking, disabling it for a period of time to defend against brute force attacks.
  - The account will automatically unlock once enough time passes with no further invalid attempts.
  - An account can be unlocked by contacting the Technology Help Desk and providing acceptable identification.

Enforcement

Individuals who violate this policy will be subject to College disciplinary action in accordance with all applicable collective bargaining agreements.

Applicability

This policy applies to any and all members of the College community to whom an individual standard-user MCC Network account has been provided, including but not limited to affiliated organizations, board members, faculty, staff, students, volunteers, vendors, guests, and visitors.

Responsibility

Associate Vice President, Technology Services / CIO

Contact Information

Technology Services

Related Information

- 7.1 MCC Acceptable Use of College Technology Policy
- 7.3 Information Technology Security Policy