Policy #:5.003

Responsible VP: Technology and Institutional Effectiveness
Responsible Office: Office of Technology
Approved By: Leadership Team
Approved: 12/5/18
Effective Date: 12/5/18
Status: APPROVED
Last Revised: 04/28/2022

PASSWORD POLICY

1. Policy Summary

This policy establishes a set of guidelines and regulations for passwords used by employees of Molloy College.

2. Policy Scope

This policy applies to all Molloy College employees and all College software applications and websites that require password authentication.

3. Policy

Based on industry standards and recommendations from Molloy College's auditors as well as from the Information Technology (IT) Management Team, the following password policy is in effect:

Enforce password history:	3 passwords remembered
Minimum password length:	8 characters
Password complexity requirements:	Enabled (see addendum)
Account lockout duration:	15 minutes
Account lockout threshold:	4 invalid logon attempts
Reset account lockout counter after:	15 minutes

The following additional security measures will be applied to users of programs containing sensitive information:

Hide Screen Saver tab:	Enabled
Password protect the screen saver:	Enabled
Screen Saver:	Enabled
Screen Saver executable name:	Lock Workstation
Screen saver timeout:	Enabled (15 minutes)

3.1 Password complexity requirements

Complexity requirements are enforced when passwords are changed or created. Passwords must meet the following minimum requirements when they are changed or created:

- Not contain the user's account name or parts of the user's full name that exceed two consecutive characters
- Be at least eight characters in length
- Contain characters from three of the following four categories:
    - English uppercase characters (A through Z)
    - English lowercase characters (a through z)
    - Base 10 digits (0 through 9)
    - Non-alphabetic characters (for example, !, $, #, %)
- Complexity requirements are enforced when passwords are changed or created.

3.2 Additional Information for Users

The College has provided users the ability to perform password self-service. The self-service system allows users to reset forgotten passwords or unlock a mistakenly locked account. Users must pre-register to use this service. Self service links can be found for both Employees and Students on the Molloy Portal: https://portal.molloy.edu/

3.3 Use of Active Directory Credentials:

Where possible, the IT Management team will work to integrate application credentials with domain credentials.

3.4 Social Media:

For official Molloy College affiliated accounts, please refer to the Social Media Policy for information regarding passwords.

5. Related Policies and/or Documents

- Accessibility Policy
- Computing Privileges and Acceptable Use Policy
- Copyright and Fair Use Policy
- Employee, Student and Faculty Handbooks
- FERPA Policy
- Mass Email Policy
- Use of Electronic Mail (Email) Policy
- Social Media Policy