Allegany College of Maryland

TECHNOLOGY PASSWORD STANDARD

Adopted date 2/4/2020
Revised Date 6/17/2022
Reviewed by ITAC 3/6/2021
Implementation 2/4/2020
Type of Standard: Operational

BACKGROUND AND PURPOSE

This standard describes the College's requirements for acceptable password selection and maintenance to maximize security of the password and minimize its misuse or theft.

STANDARD

I. SCOPE OF THE STANDARD

This standard applies to anyone accessing or utilizing the College network or data. This use may include, but is not limited to, the following: personal computers, laptops, hand-held computing devices (e.g., USB memory keys, electronic organizers), as well as College electronic services, systems and servers. This standard covers departmental resources as well as resources managed centrally.

II. STANDARD STATEMENT

All passwords (e.g., email, web, desktop computer, etc.) should be strong passwords and follow the standards listed below. In general, a password's strength will increase with length, complexity and frequency of changes. To enhance password protection, employee accounts will also utilize Multi-factor authentication.

III. Responsibilities

Users are responsible for assisting in the protection of the network and computer systems they use. The integrity and secrecy of an individual's password is a key element of that responsibility. Each individual has the responsibility for creating and securing an acceptable password per this standard. Failure to conform to these restrictions may lead to the suspension of rights to college systems or other actions as provided by College Policy, Federal, State or Local laws.

IV. Password Creation

Passwords are initially assigned when a new account is created. Users have the right and the ability to change passwords on their accounts at any time.

All passwords are required to meet the "strong password" definition.

- Passwords must be at least nine (9) characters in length and a max of (16) characters.
- Passwords must contain upper- and lower-case letters, numbers and special symbols.
- Passwords cannot contain all or part of your username, colleague ID, SSN or phone #.
- Passwords cannot match any of your five (5) previous passwords.

V. Password Expiration

Any account holder may change his or her password at any time through their active directory account, Microsoft 365 account management, or Self-service online password change utility – it is not necessary to wait for a recommended change cycle (180 days' faculty/staff and 90 days' tech staff). Passwords should be changed immediately and the helpdesk notified whenever there is a belief that the password has been compromised.

VI. Password Protection

Password protection is a vital part of any security plan please observe the following standards:

- Do not use the same password for College accounts as for other non-College accounts, such as personal internet accounts, benefits, banking, and shopping accounts.
- Do not share College passwords with anyone, in or outside the institution.
- All passwords are to be treated as restricted College information.

Good practices to follow:

- Don't reveal a password over the phone to ANYONE
- Don't reveal a password in an email message to ANYONE
- Don't reveal a password to a supervisor
- Don't talk about a password in front of others
- Don't hint at the format of a password (e.g., "my family name")
- Don't reveal a password on questionnaires or security forms to ANYONE
- Don't share a password with family members.
- Don't reveal a password to co-workers (e.g., when going on vacation or leave of any kind).
- Don't use the "Remember Password" feature of applications.
- Don't store passwords in a file on ANY computer system without encryption.
- Use a recommended password manager to store and secure all College related passwords.
- When IT works on your computer, your password will not be needed.

If someone demands a password, refer that person to this password standard or have them call the information technology department helpdesk at 301-784-5444.

The Information Technology Department or its delegates will perform a periodic review of account user's password strength through various means. If a password is guessed or cracked during one of these scans, the user will be required to change it.

VII. Enforcement

Users found to have violated this standard may be denied access to College computing resources and may be subject to other penalties and disciplinary action, both within and outside of the College. Any corrective measures taken shall be administrated in accordance with appropriate disciplinary procedures applicable to the relevant user.

VIII. Related Policies and Standards

Technology Security Standard

IX. Administration of Policy

The office of the Dean of Information Technology, in consultation with The Vice President of Finance and Administration, shall be responsible for maintaining this policy.

X. Changes

Substantive changes to this policy require approval by the Board of Trustees; editorial changes, title/position changes, and/or changes to its implementation procedures may be made as required by federal or state mandate and/or institutional need with timely notice to students and employees.