Title: DOMAIN USER PASSWORD

- □ Initial Action: NEW
- □ Board Resolution: 24-025
- □ Last Revised:
  - Policy: 5/30/2024 (New)
  - Procedure: 5/30/2024 (New)
- □ Last Reviewed:
- □ Effective: July 1, 2024
- □ Next Review: July 1, 2027
- □ Responsibility: Division of Information Technology Services

---

Purpose

This information technology requirement establishes rules for the creation of strong passwords, the protection and management of passwords, and password privacy. The implementation of these requirements will better safeguard the personal and confidential information of all individuals and organizations affiliated with, associated with, or employed by Cecil College. Adhering to these rules strengthens the confidentiality, integrity, and availability of electronic assets and supports the college's comprehensive Information Security Program.

Scope

This requirement is applicable to all Cecil College domain users. Including, but not limited to, students, faculty, staff, and members of third-party organizations given access to Cecil College systems, such as vendors, contractors, and consultants.

Password Policy

1. Users are responsible for establishing unique passwords that comply with Cecil College password standards, including length and complexity requirements (see Password Standards, below).
2. Users must protect their passwords from disclosure and should not insecurely record or store them.
3. Passwords must never be revealed to anyone, including other employees.
4. The same password should not be used for Cecil College accounts and non-Cecil College accounts, including personal accounts.
5. Multi-Factor Authentication (MFA) is required for faculty and staff and is recommended for students. Users may be required to enroll in MFA under the Division of Information Technology Services' direction. An MFA exemption list will be maintained by the Division of Information Technology Services.
6. Users must not share MFA codes or approve prompts unless they are for their own login.
7. Password standards for length and complexity may change as needed, in the College's discretion, to protect college data and systems from escalating cyber threats and to comply with increasing information security controls requirements.

8. Passwords will be disabled upon detection of a compromised account (*e.g.*, an account accessed by a person not authorized to use the account).
9. Repeated failed login attempts will result in the account locking, which disables the account for a period of time to defend against brute force attacks.
    9.1. The account will automatically unlock once sufficient time passes with no further invalid attempts.
    9.2. An account can be unlocked by contacting the Information Technology Help Desk and providing acceptable identification.
10. Single Sign-On (an authentication method that allows users to sign in using one set of credentials to multiple independent software system) is recommended for all Cecil College technology systems and will be required for all new implementations. Exceptions must be approved by the Chief Information Officer.

Enforcement

Individuals violating this Policy may have their account either suspended or terminated given the severity of the offense, and may be subject to discipline up to and including termination of employment or enrollment. Refer to the enforcement section of the college's Responsible Use of Information Technology Resources for additional information.

Procedures

Establishing a Strong Password

Using passphrases instead of single words is strongly recommended for better security. Passphrases offer longer and more complex combinations of words, making authentication stronger. By using passphrases, users can protect their accounts and sensitive information more effectively from breaches and unauthorized access.

Passwords can be classified as weak or strong based on how difficult they are to guess and/or compute. Cecil College's password information technology requirements have been chosen to offer a level of protection beyond simple or weak but not to be so complex as to require being written down, which causes additional risk.

Password Standards for Length and Complexity

Cecil College users must adhere to the following 'strong password' construction criteria:

1. Must be at least fourteen (14) characters in length.
2. Must contain at least one (1) uppercase letter (A–Z).
3. Must contain at least one (1) lowercase letter (a-z).
4. Must contain at least one (1) or more numbers (0-9).
5. Must contain at least one (1) non-alphanumeric character (For example: !, $, #, or %).
6. May not contain the user's first or last name.
7. Must be changed every 365 days.
8. None of the previous twelve (12) passwords may be reused.

9. Employees with special administration accounts and those who process credit cards are required to change their passwords every 90 days, in accordance with the Payment Card Industry Data Security Standard (PCI DSS).