Policy Title	**Password Creation Standards Policy**
Policy Number	8011
Category	Technology (8000s)
Applicability	College-wide
Responsible Office	Information Technology Services
Effective Date	January 6, 2025

I. Policy Statement

All users of College systems are responsible for following the minimum standards established within and in accordance with this Policy for creating, maintaining, and securing their user passwords for access to College systems.

II. Rationale

Password standards are established to ensure the security and integrity of user accounts and sensitive information. Here are some key rationales behind common password standards:

- Security: The primary goal of password standards is to enhance security by making it harder for unauthorized users to guess or brute-force passwords. Strong passwords reduce the risk of unauthorized access to systems and data.
- Complexity: Password standards often require a combination of uppercase letters, lowercase letters, numbers, and special characters. This complexity increases the number of possible combinations, making passwords more resistant to automated attacks.
- Length: Longer passwords are generally more secure because they increase the time and effort required to crack them. Password standards often specify a minimum length to ensure sufficient complexity.
- Resistance to Dictionary Attacks: Password standards discourage the use of easily guessable words or commonly used passwords (like "password" or "123456"). This reduces the risk of successful dictionary attacks.
- Regular Updates: Standards often recommend or require regular password updates to mitigate the risk of passwords being compromised and used maliciously over time.
- Compliance: Many industries and organizations are required by regulations and standards (such as GDPR,[1] HIPAA,[2] and PCI DSS[3]) to implement specific password policies to protect sensitive data and comply with legal requirements.

[1] The European Union's General Data Protection Regulation.
[2] The U.S. Health Insurance Portability and Accountability Act.
[3] The Payment Card Industry Data Security Standard.

- Best Practices: Following password standards aligns with cybersecurity best practices recommended by security experts and organizations, helping to establish a baseline level of security across systems and networks.

Overall, password standards are designed to balance usability with security, aiming to create a barrier that is strong enough to protect against common attacks while still being practical for users to remember and use effectively.

III. Scope and Applicability

This Policy governs password requirements for all Suffolk County Community College accounts, computers, and systems, and applies college-wide to all administrative units, departments, employees, and students of the college and to any other user of the college's accounts, computers, and systems.

IV. Responsible Office/Executive

The Office of Information Technology Services has responsibility for the implementation and review of this Policy. Individuals with questions about this Policy should contact the Office of Information Technology Services for more information.

V. Definitions

A password length policy refers to rules and guidelines set by organizations or systems regarding the minimum and maximum length requirements for passwords used by users. Here are some definitions and components commonly included in such policies:

Minimum Length: Specifies the shortest allowable length for a password. For example, a policy might require passwords to be at least 12 characters long.

Maximum Length: Specifies the longest allowable length for a password. This is less common but sometimes used to prevent excessively long passwords that could cause system issues.

Complexity Requirements: Rules about what types of characters must be included in the password (e.g., uppercase letters, lowercase letters, numbers, special characters) to increase its complexity and security.

Dictionary Words: Policies may forbid the use of common dictionary words or easily guessable sequences to prevent easy cracking of passwords.

Expiration and Change Frequency: Guidelines on how often passwords must be changed and expire to ensure ongoing security.

Password history: Rules about how frequently passwords can be reused or whether new passwords must differ significantly from previous ones.

Account Lockout: Parameters defining how many unsuccessful login attempts trigger an account lockout and for how long.

Multi-Factor Authentication (MFA): Encouragement or requirement for users to use additional authentication factors along with passwords for enhanced security.

Educational Material: Information provided to users about creating strong passwords and the importance of password security.

Compliance: Ensure that password policies comply with industry standards and regulations, such as GDPR or PCI DSS, where applicable.

These definitions and policies are designed to balance security requirements with usability and practicality for users.

VI. Policy Elaboration

The Office for Information Technology Services (ITS) has established password creation and security standards applicable to the College community, inclusive of minimum length, maximum length, complexity requirements, and password history rules, as well as password change history, expiration and change frequency, account lockout, and multi-factor authentication standards and requirements applicable to the College community. These are provided to affected members of the College community but not included within public-facing policy documents or webpages so as not to jeopardize the capacity of the College to guarantee the security of its information technology assets.

- *Password length requirements are withheld from the public-facing version of this policy.*[4]
- *Password minimum character requirements are withheld from the public-facing version of this policy.* [5]
- Passwords cannot contain the individual's full first or last name.
- *Password reuse requirements are withheld from the public-facing version of this policy.* [6]
- Passwords should not be easily guessed.
- Passwords should never be written down and stored where someone else might see them.
- College passwords should be unique and not used for other purposes or in other systems (e.g. your bank account, outside email systems or for shopping sites).

[4] Members of the College community needing to access the full version of this policy may do so in the Technology Policies for Employee Access repository after logging in with their College credentials: 8011 Password Creation Standards - for internal use only.pdf.
[5] See FN 4.
[6] See FN 4.

- *Password change frequency requirements are withheld from the public-facing version of this policy.*[7]

Some systems may require slightly different rules; any System specific rules will be available through the system login page.

VII. Related Administrative Procedures

- Policy and Procedures on Access Control and Password Security
- College Encryption and Key Management Standard

VIII. Cross-References

- Information Technology Policies and Guidelines for Faculty, Staff and Administrators
- Employee Email and Cell Phone Policy
- Information Technology Policies and Guidelines for Students

IX. References

- Middle States Commission on Higher Education (MSCHE) Standards IV, VI
- SUNY Information Security Policy and Information Security Guidelines

X. History / Revision Dates

Adoption Date:	November 3, 2009
Revised:	July 13, 2015
Revised:	September 16, 2024, effective January 6, 2024 (President's Cabinet)

[7] See FN 4.