CUNY Password Standard

City University of New York Cybersecurity Standards

Standard Owner:	CUNY Office of Computing and Information Services
Approver:	Eusebio Formoso, Vice Chancellor for Information Technology and University CIO
Effective Date:	April 3, 2025

1.0 Purpose

All passwords used to protect City University of New York (CUNY) systems shall be appropriately configured, periodically changed, and issued for individual use.

This password standard applies to the following types of accounts in use at CUNY:

User Accounts	Administrative Accounts	Service Accounts
Are for use by individuals, often referred to as end-users.	Are also for use by individuals, but carry an elevated degree of privilege (e.g., root, administrator). They are intended for use solely by authorized IT personnel to perform such tasks as managing systems and user accounts or performing password resets.	Are intended for use solely by automated processes that require authentication to access system resources or perform tasks.

2.0 Standard Statements

2.1 CUNY Passwords

Passwords used by a person on CUNY systems must be different from any passwords used by the same person on non-CUNY systems (for example, on social networking, e-commerce, and other personal online sites). This reduces the risk to CUNY systems if a personal (non-CUNY) account password is compromised.

Additionally, CUNY passwords must:

- Never be shared or displayed on-screen.
- Be classified and handled as Confidential Data.
- Be changed when there is any indication of system or password compromise.

2.1.1 Password Format, Length, and Complexity

CUNY passwords must meet the following requirements (where system allows it):

- Must not match or contain first name.
- Must not match or contain last name.
- Must be at least 13 characters long.
- Must be at least 20 characters long for service accounts and Domain administration accounts.
- Must contain at least 3 alphanumeric characters, 2 of which must be letters.
- Must contain at least 1 lowercase letter.
- Must contain at least 1 uppercase letter.
- Must contain at least 1 numeric character.
- Must contain at least 1 special character.
- Must not match any of the previous 12 passwords.
- Must not match or contain the username (user ID).

Mobile devices (such as cell phones and iPads) issued by CUNY may use strong biometric (face or fingerprint) recognition with a backup password or PIN of at least six alphanumeric characters.

Passwords must not be derived from easily guessed, common words or phrases such as those found in dictionaries (English and non-English), proper names, or other names, words, numbers, or dates readily associated with the individual user (e.g., telephone extension, Social Security number, or ZIP code).

2.1.2 Password Encryption and Hashing

CUNY passwords must be:

- Encrypted when transmitted electronically with a protocol compliant with the CUNY IT Security policy and standards.
- Encrypted or hashed when held in storage.
- Either encrypted or secured with compensating controls, providing a comparable level of protection, when embedded in configuration files, source code, or scripts.

2.1.3 Password Changes

A user wishing to change a CUNY password must be positively identified by demonstrating knowledge of the current password, or by other comparable methods that validate that the account owner initiated the password change request.

2.1.4 Password Delivery

CUNY passwords must be delivered securely to the recipient (authorized user) via an approved transmission method. Although passwords must never be shared, initial passwords may be delivered to the recipient's manager. In all cases, the recipient or manager must be positively identified before the password is delivered.

2.2 Screen Locks

A password-protected screen lock must be activated within fifteen minutes of user inactivity.

2.3 Account Lockout

All accounts which provide access to Sensitive or Confidential information must be automatically disabled after a series of sequential invalid login attempts.

2.3.1 Password Expiration and Re-use

- Temporary or initial user account passwords must be set to expire after initial use. Default passwords and PINs must be changed immediately upon the completion of the installation process or at first login.
- If a user is not prompted to change a temporary or initial password, the account may have been inappropriately accessed, and the user should contact the CUNY Service Desk immediately.
- College security administrators can reset all passwords where proper authorization and audit logs are in place.
- Additional password expiration requirements and related guidelines and restrictions are provided in the following tables for the three account types:

Account Expiration

User Accounts	Administrative Accounts	Service Accounts
User account passwords and PINs must expire at least every 180 days and be enabled with MFA.	Administrative account passwords must expire at least every 60 days, have a minimum length of 20 characters, and be enabled with MFA.	Service account passwords must expire at least every 180 days and every time an Administrator leaves CUNY, and have a minimum length of 20 characters.

Account Sharing

User Accounts	Administrative Accounts	Service Accounts
Do not share password with others.	When a staff member who knows an administrative account password leaves CUNY or changes job function, that password must be changed.	Password must be known only by a limited number of staff on a need-to-know basis. The names of staff who know the password for any service account must be documented and the list must be kept current. When a staff member who knows a service account password leaves CUNY or changes job function, that password must be changed.

Account Access Restriction

User Accounts	Administrative Accounts	Service Accounts
Generally, no access restriction.	Administrative accounts should be restricted to logging in from specified IP subnets/addresses or locations.	Service accounts must be restricted to logging in from specified IP subnets/addresses.

2.4 Password Standard Enforcement

Whenever possible, the system must automate the enforcement of these requirements. When this is not possible, equivalent controls must be established through alternative methods or procedures. For example, as an alternative to enforcing password complexity, the administrator could periodically use tools to detect weak passwords and require users with weak passwords to change them.

The City University of New York may, at any time, adopt more stringent controls than those specified in this standard.

All security policies and standards are to be reviewed and updated every three years.

2.5 Password Best Practices

- Where feasible, the use of password management software and/or certificate-based authentication is recommended.
- Use passphrases instead of passwords, as they are longer and easier to remember. A passphrase is a memorized phrase consisting of a sequence of mixed words. Passphrases should be unique, complex, and hard to predict.
- Do not save CUNY passwords in web browsers, especially on shared devices such as shared family computers and lab computers.

3.0 Approvals

This standard was approved by the University officer listed below and is now in force:

Approved on April 3, 2025, by Eusebio Formoso, Vice Chancellor for Information Technology and University CIO

4.0 Revision History

Version	Change	Author	Date of Change
1.0	Initial publication of this standard	CUNY Offices of Cybersecurity and Information Security	4/3/2025