Queens College Technology Standard	No: QC-ITS-Cyber-014
Identification and Authentication Standards	**Updated: 08/21/2023**
	Issued By: Queens College, Chief Information Security Officer **Owner: Queens College Information Technology Services**

1.0 Purpose and Benefits

To ensure that only properly identified and authenticated users and devices are granted access to Information Technology (IT) resources in compliance with IT security policies, standards, and procedures.

2.0 Authority

- **Responsible Office(s):** Queens College Information Technology Services
- **Responsible Executive(s)**: Chief Information Officer (CIO)
- **Responsible Officer(s)**: Chief Information Security Officer (CISO)

3.0 Scope

This is a college-wide standard and includes requirements that must be followed if Queens College is to protect the information that is collected in the standard process of business. This standard is to be an additional layer of security on top of existing CUNY security policies and is not intended or able to supersede CUNY policies.

This standard encompasses all systems, automated and manual, for which Queens College has administrative responsibility, including systems managed or hosted by third parties on behalf of Queens College. It addresses all information, regardless of the form or format, which is created or used in support of business activities.

4.0 Information Statement

This standard is applicable to all departments and users of IT resources and assets.

4.1. Identification and Authentication

a. Ensure that information systems uniquely identify and authenticate users or processes acting on behalf of Queens College users.

b. Ensure that information systems implement multifactor authentication for network access to privileged accounts.
c. Ensure that information systems implement multifactor authentication for network access to non-privileged accounts.
d. Ensure that information systems implement multifactor authentication for local access to privileged accounts.
e. Ensure that information systems implement replay-resistant authentication mechanisms for network access to privileged accounts.
f. Web Applications with access to confidential or operational data must use the University approved single sign-on (SSO) whenever possible. Organizations that are designing or acquiring application systems which will maintain confidential or operational data must ensure they use approved authentication methods.
    i. Applications that use simple LDAP binds or other non-secure methods of authentication to QC's Active Directory LDAP are strictly prohibited.
    ii. Caching or storing of clear-text simple passwords is forbidden.
    iii. System maintenance scripts must use secure forms of authentication.
g. Ensure that information systems implement multifactor authentication for remote access to privileged and non-privileged accounts such that one of the factors is provided by a device separate from the system gaining access and the device utilizes a cryptographic strength mechanisms that protects the primary authentication token (secret key, private key or one-time password) against compromise by protocol threats including: eavesdropper, replay, online guessing, verifier impersonation and man-in-the-middle attacks.
h. Maintain a list of approved authentication methods and provide tools and assistance.
i. Ensure that information systems accept and electronically verify Personal Identity Verification (PIV) credentials.

4.2. Device Identification and Authentication

a. Ensure that information systems uniquely identify and authenticate all devices before establishing a network connection.

4.3. Authenticator Management

a. Manage information system authenticators by verifying, as part of the initial authenticator distribution, the identity of the individual, group, role, or device receiving the authenticator.
b. Establish initial authenticator content for authenticators defined by the organization.
c. Ensure that authenticators have sufficient strength of mechanism for their intended use.

d. Establish and implement administrative procedures for initial authenticator distribution, for lost/compromised or damaged authenticators, and for revoking authenticators.
e. Change default content of authenticators prior to information system installation.
f. Establish minimum and maximum lifetime restrictions and reuse conditions for authenticators.
g. Protect authenticator content from unauthorized disclosure and modification.
h. Require individuals and devices to implement specific security safeguards to protect authenticators.
i. Change authenticators for group/role accounts when membership to those account changes.
j. Ensure that information systems, for password-based authentication enforce minimum password complexity that must not contain the user's entire Account Name value or entire Full Name value.
k. Ensure passwords must contain characters from three of the following five categories:
    i. Uppercase characters of European languages (A through Z, with diacritic marks, Greek and Cyrillic characters);
    ii. Lowercase characters of European languages (a through z, sharp-s, with diacritic marks, Greek and Cyrillic characters);
    iii. Base 10 digits (0 through 9);
    iv. Non-alphanumeric characters ~!@#$%^&*_-+=`|\(){}[]:;"'<>,.?/; and
    v. Any Unicode character that is categorized as an alphabetic character, but is not uppercase or lowercase. This includes Unicode characters from Asian languages.
l. Require passwords to have a minimum length of 8 characters.
m. Enforce at least one changed character when new passwords are created.
n. Store and transmit only cryptographically-protected passwords.
o. All passwords must be changed at least every 180 days. Accounts which have privileged access must be changed at least every 60 days.
p. Allow the use of a temporary password for system logons with an immediate change to a permanent password.
q. Ensure that information system, for PKI-based authentication, validates certifications by constructing and verifying a certification path to an accepted trust anchor including checking certificate status information.
r. Enforce authorized access to the corresponding private key.
s. Map the authenticated identity to the account of the individual or group.

t. Implement a local cache of revocation data to support path discovery and validation in case of inability to access revocation information via the network.

4.4. Authenticator Feedback

a. Ensure that information systems obscure feedback of authentication information during the authentication process to protect the information from possible exploitation/use by unauthorized individuals.

4.5. Cryptographic Module Authentication

a. Ensure that information systems implement mechanisms for authentication to a cryptographic module that meet the requirements of applicable state and federal laws, directives, policies, regulations, standards, and guidance for such authentication.

4.6. Identification and Authentication

a. Ensure that information systems uniquely identify and authenticate non-entity users or processes acting on behalf of non-entity users.

5.0 Compliance

This standard shall take effect upon publication. Compliance is expected with all enterprise policies and standards. Policies and standards may be amended at any time; compliance with amended policies and standards is expected.

If compliance with this standard is not feasible or technically possible, or if deviation from this standard is necessary to support a business function, entities shall request an exception through the Chief Information Security Officer's exception process.

Commented [A1]: Was this process outlined above or would this process be referenced on another document?

6.0 Definitions of Key Terms

Term	Definition
Multi-Factor Authentication	Multi-Factor Authentication: is an authentication method in which a computer user is granted access only after successfully presenting two or more pieces of evidence (or factors) to an authentication mechanism: knowledge (something the user and only the user knows), possession (something the user and only the user has), and inherence (something the user and only the user is).
Identification	Identification is the act of stating or otherwise attesting to a person or thing's identity.
Authentication	Authentication is the process of confirming that identity.

Term	Definition
Application Systems:	Application Systems are any computer programs or group of programs.

7.0 Contact Information

Submit all inquiries and requests for future enhancements to the standard owner at:

Chief Information Security Officer
Damon Vogel
CISO@qc.cuny.edu

8.0 Revision History

This standard shall be subject to periodic review to ensure relevancy.

Date	Description of Change	Reviewer
9/22/22	Initial changes to apply to Queens College	DVogel
08/21/2023	Conversion to Standard, Add #10, Alignment to Gartner Recommendations	DVogel

9.0 Related Documents

10.0 External Documents

National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53a – Identification and Authentication (IA), NIST SP 800-12, NIST SP 800-63, NIST SP 800-73, NIST SP 800-76, NIST SP 800-78, NIST SP 800-100, NIST SP 800-116;

Homeland Security Presidential Directive (HSPD) 12 Policy for a Common Identification Standard for Federal Employees and Contractors; Federal Information Processing Standards (FIPS): FIPS 201, FIPS 140