Queens College **Technology Standard**	**No: QC-ITS-Cyber-004**
Access Control Standard	**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 access controls are implemented and 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
- **Responsible Officer(s)**: Chief Information Security Officer

3.0 Scope: College-Wide

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

1. Account management

    a. identify and select the following types of information system accounts to support organizational missions and business functions: individual, shared, group, system, guest/anonymous, emergency, developer/manufacturer/vendor, temporary, and service.

b. assign account managers for information system accounts.

c. establish conditions for group and role membership.

d. specify authorized users of the information system, group and role membership, and access authorizations (i.e., privileges) and other attributes (as required) for each account.

e. require approvals by system owners for requests to create information system accounts.

f. create, enable, modify, disable, and remove information system accounts in accordance with approved procedures.

g. monitor the use of enhanced access information system accounts.

h. require system owners to notify appropriate parties when accounts are no longer required, when users are terminated or transferred, and when individual information system usage or need-to-know changes.

i. authorize access to the information system based on a valid access authorization or intended system usage.

j. review accounts for compliance with account management requirements annually at a minimum.

k. minimize usage of shared/group

l. establish a process for reissuing shared/group account credentials (if deployed) when individuals are removed from the group.

m. employ automated mechanisms to support the management of information system accounts.

n. ensure that the information system automatically disables temporary and emergency accounts after usage.

o. ensure that the information system automatically disables inactive enhanced access accounts after 90 days.

p. ensure that the information system automatically audits account creation, modification, enabling, disabling, and removal actions, and notifies appropriate Queens College ITS personnel.

2. Access enforcement

    a. Ensure that the information system enforces approved authorizations for logical access to information and system resources in accordance with applicable access control policies.

3. Information flow enforcement

    a. Ensure that the information system enforces approved authorizations for controlling the flow of information within the system and between interconnected systems based on applicable Standard.

4. Separation of duties

    a. Separate duties of individuals as necessary, to prevent malevolent activity without collusion.

    b. Document the separation of duties of individuals.

    c. Define information system access authorizations to support separation of duties.

5. Least privilege

    a. Employ the principle of least privilege, allowing only authorized accesses for users (or processes acting on behalf of users) which are necessary to accomplish assigned tasks in accordance with organizational missions and business functions.

    b. Authorize explicitly access to hardware and software controlling access to systems and filtering rules for routers/firewalls, cryptographic key management information, configuration parameters for security services, and access control lists.

    c. Require that users of information system accounts, or roles, with access to enhanced privileged accounts, use non-privileged accounts or roles, when accessing non-security functions.

    d. Restrict enhanced access accounts on the information systems to Queens College Information Technology Services approved personnel.

    e. Ensure that the information system audits the execution of privileged functions.

    f. Ensure that the information system prevents non-privileged users from executing privileged functions to include disabling, circumventing, or altering implemented security safeguards/countermeasures.

6. System use notification

    a. Displays to users an approved system using a notification message or banner before granting access to the system that provides privacy and security notices consistent with applicable state and federal laws, directives, policies, regulations, standards, and guidance and states informing that:

        i. Users are accessing a Queens College information system.

        ii. Unauthorized use of the information system is prohibited.

7. Remote access

    a. Establish and document usage restrictions, configuration/connection requirements, and implementation guidance for each type of remote access allowed.

    b. Authorize remote access to the information system prior to allowing such connections.

    c. Ensure that the information system monitors and controls remote access methods.

    d. Ensure that the information system implements cryptographic mechanisms to protect the confidentiality and integrity of remote access sessions.

    e. Ensure that the information system routes all remote accesses through a minimum of managed network access control points to reduce the risk for external attacks.

    f. Authorize the execution of privileged commands and access to security-relevant information via remote access only for ITS employees only.

    g. Document the rationale for such access in the security plan for the information system.

8. Wireless access

    a. Establish usage restrictions, configuration/connection requirements, and implementation guidance for wireless access.

b. Authorize wireless access to the information system prior to allowing such connections.

c. Ensure that the information system protects wireless access to the system using authentication of users and devices and encryption.

9. Access control for mobile devices

a. Establish usage restrictions, configuration requirements, connection requirements, and implementation guidance for organization-controlled mobile devices.

b. Authorize the connection of mobile devices to organizational information systems.

10. Use of external information system

a. Establish terms and conditions, consistent with any trust relationships established with other organizations owning, operating, and/or maintaining external information systems, allowing authorized individuals to:

i. Access the information system from external information systems.

ii. Process, store, or transmit organization-controlled information using external information systems.

iii. Permit authorized individuals to use an external information system to access the information system or to process, store, or transmit organization-controlled information only when the organization:

1. Verifies the implementation of required security controls on the external system as specified in the organization’s information security Standard and security plan.

2. Retains approved information system connection or processing agreements with the organizational entity hosting the external information system.

11. Information sharing

a. Facilitate information sharing by enabling authorized users to determine whether access authorizations assigned to the sharing partner match the access restrictions on the information for [entity defined information sharing circumstances where user discretion is required].

12. Publicly accessible content

    a. Designate individuals authorized to post information onto a publicly accessible information system.

    b. Train authorized individuals to ensure that publicly accessible information does not contain nonpublic information.

    c. If required, determine department to review the proposed content of information prior to posting onto the publicly accessible information system to ensure that nonpublic information is not included.

    d. Require review the content on the publicly accessible information system for nonpublic information every semester and removes such information, if discovered.

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.

6.0 Definitions of Key Terms

Term	Definition

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
10/13/22	Initial changes to apply to Queens College	DVogel
06/12/2023	Further changes to align to QC & Tags	DVogel
08/21/2023	Conversion to Standard, Add #10, Alignment to Gartner Recommendations	DVogel

9.0 Related Documents

10.0 External Documents