Queens College Technology Standard	No: QC-ITS-Cyber-009
Configuration Management 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. Baseline Configuration
    a. Develop, document, and maintain under configuration control, a current baseline configuration of information systems.

b. Review and update the baseline configuration of the information system annually

c. Review and update the baseline configuration of the information system when required as a result of change management and as an integral part of information system component installations and upgrades.

d. Retain one previous version of baseline configurations of information systems to support rollback.

2. Configuration Change Control

   a. Determine the types of changes to the information system that are configuration-controlled.

   b. Review proposed configuration-controlled changes to the information system and approve or disapprove such changes with explicit consideration for security impact analyses.

   c. Document configuration change decisions associated with the information system.

   d. Implement approved configuration-controlled changes to the information system.

   e. Retain records of configuration-controlled changes to the information system for seven years.

   f. Audit and review activities associated with configuration-controlled changes to the information system.

   g. Coordinate and provide oversight for configuration change control activities through Change Advisory Board.

   h. Test, validate, and document changes to the information system before implementing the changes on the operational system.

3. Security Impact Analysis

   a. Analyze changes to the information system to determine potential security impacts prior to change implementation.

4. Access Restrictions for Change

   a. Define, document, approve, and enforce physical and logical access restrictions associated with changes to the information system.

5. Configuration Settings

   a. Establish and document configuration settings for information technology products employed within the information system using NIST – National

Checklist Program that reflect the most restrictive mode consistent with operational requirements.

b. Implement the configuration settings.

c. Identify, document, and approve any deviations from established configuration settings.

d. Monitor and control changes to the configuration settings in accordance with policies and procedures.

6. Least Functionality

    a. Configure the information system to provide only essential capabilities.

    b. Review the information system annually to identify unnecessary and/or non-secure functions, ports, protocols, and services.

    c. Disable functions, ports, protocols, and services within the information system deemed to be unnecessary and/or non-secure.

    d. Prevent program execution in accordance with policies regarding software program usage and restrictions and rules authorizing the terms and conditions of software program usage.

    e. Identify software programs not authorized to execute on information systems.

    f. Employ an allow-all, deny-by-exception policy to prohibit the execution of unauthorized software programs on the information system.

    g. Review and update the list of unauthorized software programs annually.

7. Information System Component Inventory

    a. Develop and document an inventory of information system components that:

        i. Reflects the current information system accurately.

        ii. Includes all components within the authorization boundary of the information system.

        iii. Is at the level of granularity deemed necessary for tracking and reporting.

        iv. Includes information deemed necessary to achieve effective information system component accountability.

    b. Review and update the information system component inventory annually.

    c. Update the inventory of information system components as an integral part of component installations, removals, and information system updates.

d. Employ automated mechanisms quarterly to detect the presence of unauthorized hardware, software, and firmware components within the information system.

e. Take the following actions when unauthorized components are detected:

    i. Disable network access by such components, or

    ii. Isolate the components and notifies the Chief Information Officer and system owner.

f. Verify that all components within the authorization boundary of the information system are not duplicated in other information system component inventories.

8. Configuration Management Plan

IT shall develop, document, and implement a configuration management plan for the information system that:

a. Addresses roles, responsibilities, and configuration management processes and procedures.

b. Establishes a process for identifying configuration items throughout the system development life cycle and for managing the configuration of the configuration items.

c. Defines the configuration items for the information system and places the configuration items under configuration management.

d. Protects the configuration management plan from unauthorized disclosure and modification.

9. Software Usage Restrictions

a. Use software and associated documentation in accordance with contract agreements and copyright laws.

b. Track the use of software and associated documentation protected by quantity licenses to control copying and distribution.

c. Control and document the use of peer-to-peer file sharing technology to ensure that this capability is not used for the unauthorized distribution, display, performance, or reproduction of copyrighted work.

10. User Installed Software

a. Establish policies governing the installation of software by users.

b. Enforce software installation policies through controlling privileged access and blocking the execution of files using policy applied by directory service and/or application whitelisting.

c. Monitor policy compliance regularly.

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**
10/17/22	Initial changes to apply to Queens College	DVogel
06/13/2023	Additional 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): NIST SP 800-53a – Configuration Management (CM)