Queens College **Information Technology Standard**	**No: QC-ITS-Cyber-028**
IT Standard: **Secure Configuration**	**Updated: 09/08/2023**
	Issued By: Queens College, Chief Information Security Officer **Owner: Queens College Information Technology Services**

1.0 Purpose and Benefits

The purpose of this standard is to establish baseline configurations for information systems that are owned and/or operated by the entity. Effective implementation of this standard will maximize security and minimize the potential risk of unauthorized access to information and technology.

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 – 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 policy 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 where determined necessary by the CISO's office.

4.0 Information Statement

Standard secure configuration profiles, based on any one or more of the industry consensus guidelines listed below, must be used in addition to the latest vendor security guidance. Alterations to the profile must be based on business need, policy or standard compliance, developed in consultation with the Information Security Officer/designated security representative, documented and retained for audit purposes.

Industry Consensus Guidelines

- Center for Internet Security (CIS) Benchmarks
- National Institute of Science and Technology (NIST) National Checklist Program
- United States Government Configuration Baselines (USGCB)

The initial setup, software installation, and security configuration of new systems must be performed in a secure environment isolated from other operational systems with minimal communication protocols enabled.

Changes to configurations are formally identified, proposed, reviewed, analyzed for security impact, tested, and approved prior to implementation in accordance with the change management procedures. Individuals conducting security impact analyses possess the necessary skills and technical expertise to analyze the changes to information systems and the associated security ramifications.

Entities must maintain configuration management plans that define detailed processes and procedures for how configuration management is used to support secure system development life cycle activities at the information system level. Configuration management plans are typically developed during the development/acquisition phase of the secure system development life cycle.

A configuration monitoring process must be in place to identify undiscovered or undocumented system components, misconfigurations, vulnerabilities, and unauthorized changes.

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.

If compliance with this standard is not feasible or technically possible, or if a deviation from this policy 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 policy 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
10/18/2022	Initial Changes to apply to Queens College	DVogel
09/08/2023	Add #10, Converted to Standard, Aligned to Gartner Recommendations.	

9.0 Related Documents

10.0 External Documents

National Institute of Standards and Technology (NIST) 800-128, Guide for Security-Focused Configuration Management of Information Systems