Queens College **Technology Standard**	**No: QC-ITS-Cyber-024**
Planning Standard	**Updated: 09/08/2023**
	Issued By: Queens College, Chief Information Security Officer **Owner: Queens College Information Technology Services**

1.0 Purpose and Benefits

To ensure that Information Technology (IT) resources and information systems are established with effective security controls and control enhancements that reflect applicable federal and state laws, Executive Orders, directives, regulations, policies, standards, and guidance.

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 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. System Security Plan
   i. Develop a security plan for each information system that:
      a. Is consistent with the Queens College enterprise architecture.

        b. Defines explicitly the authorization boundary for the system.
        c. Describes the operational context of the information system in terms of missions and business processes.
        d. Provides the security categorization of the information system including supporting rationale.
        e. Describes the operational environment for the information system and relationships with or connections to other information systems.
        f. Provides an overview of the security requirements for the system.
        g. Identifies any relevant overlays, if applicable.
        h. Describes the security controls in place or planned for meeting those requirements including a rationale for the tailoring decisions.
        i. Is reviewed and approved by the authorizing official or designated representative prior to plan implementation.
    ii. Distribute copies of the security plan and communicate subsequent changes to the plan to authorized personnel and/or business units.
    iii. Review the security plan for the information system at least annually.
    iv. Update the plan to address changes to the information system/environment of operation or problems identified during plan implementation or security control assessments.
    v. Protect the security plan from unauthorized disclosure and modification.

2. Rules of Behavior
    i. Establish, and make readily available to individuals requiring access to the information system, the rules that describe their responsibilities and expected behavior with regard to information and information system usage.
    ii. Receive a signed acknowledgment from such individuals, indicating that they have read, understand, and agree to abide by the rules of behavior, before authorizing access to information and the information system.
    iii. Review and update the rules of behavior.
    iv. Require individuals who have signed a previous version of the rules of behavior to read and resign when the rules of behavior are revised and updated.

3. Information Security Architecture
    i. Develop information security architecture for the information system that will:
        a. Describe the overall philosophy, requirements, and approach to be taken with regard to protecting the confidentiality, integrity, and availability of organizational information.
        b. Describe how the information security architecture is integrated into and supports the enterprise architecture.
        c. Describe any information security assumptions and dependencies on external services.

    ii. Review and update the information security architecture no less than annually, to reflect updates in the enterprise architecture.
    iii. Ensure that planned information security architecture changes are reflected in the security plan, the security operations and procurements/acquisitions.

4. Defense-in-Depth Approach
    i. Design security architecture using a defense-in-depth approach that:
        a. Allocates security safeguards to Queens College defined locations and architectural layers.
        b. Will ensure that the allocated security safeguards operate in a coordinated and mutually reinforcing manner.

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**
9/20/22	Initial changes to apply to Queens College	DVogel

07/12/2023	Added New Policy Number Scheme & Tagging	DVogel
09/08/2023	Added #10, Converted to Standard, Aligned to Gartner Recommendations.	DVogel

9.0 Related Documents

10.0 External Documents