Queens College Technology Standard	No: QC-ITS-Cyber-030
Security Assessment and Authorization 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 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 (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. 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. Security Assessment and Authorization Standard And Procedures

    a. Develop, document, and disseminate:

i. A security assessment and authorization standard that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance.

ii. Procedures to facilitate the implementation of the security assessment and authorization standard and associated security assessment and authorization controls.

b. Review and update the current security assessment and authorization standard and procedures annually.

2. Security Assessments

a. Develop a security assessment plan that describes the scope of the assessment including:

i. Security controls and control enhancements under assessment.

ii. Assessment procedures to be used to determine security control effectiveness.

iii. Assessment environment, assessment team, and assessment roles and responsibilities.

b. Assess the security controls in the information system and its environment of operation annually to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting established security requirements.

c. Produce a security assessment report that documents the results of the assessment.

d. Provide the results of the security control assessment to the CISO's office

3. System Interconnections

    a. Authorize connections from the information system to other information systems through the use of Interconnection Security Agreements.

    b. Document, for each interconnection, the interface characteristics, security requirements, and the nature of the information communicated.

    c. Review and update Interconnection Security Agreements annually.

    d. Employ an allow-all, deny-by-exception, deny-all, permit-by-exception, policy for allowing all information systems to connect to external information systems.

4. Plan Of Action and Milestones

    a. Develop a plan of action and milestones for the information system to document the planned remedial actions to correct weaknesses or deficiencies noted during the assessment of the security controls and to reduce or eliminate known vulnerabilities in the system.

    b. Update existing plan of action and milestones annually based on the findings from security controls assessments, security impact analyses, and continuous monitoring activities.

5. Security Authorization

    a. Assign a senior-level executive or manager as the authorizing official for the information system.

    b. Ensure that the authorizing official authorizes the information system for processing before commencing operations.

    c. Update the security authorization annually.

6. Continuous Monitoring
    a. Develop a continuous monitoring strategy and implement a continuous monitoring program that includes:

        i. Establishment of metrics to be monitored.

        ii. Establishment of regular scheduling for monitoring and regular scheduling for assessments supporting such monitoring.

        iii. Ongoing security control assessments in accordance with the organizational continuous monitoring strategy.

        iv. Ongoing security status monitoring of organization-defined metrics in accordance with the organizational continuous monitoring strategy.

        v. Correlation and analysis of security-related information generated by assessments and monitoring.

        vi. Response actions to address results of the analysis of security-related information.

        vii. Reporting the security status of organization and the information system to CISO's Office regularly

7. Internal System Connections

    a. Authorize internal connections to the information system.

    b. Document, for each internal connection, the interface characteristics, security requirements, and the nature of the information communicated.

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**
11/10/22	Initial changes to apply to Queens College	DVogel
09/08/2023	Added #10, Converted to Standard, Aligned to Gartner Recommendations	DVogel

9.0 Related Documents

10.0 External Documents

National Institute of Standards and Technology (NIST) Special Publications (SP): NIST SP 800-53a – Security Assessment and Authorization (CA), NIST SP 800-12, NIST SP 800-37, NIST SP 800-39, NIST SP 800-47, NIST SP 800-100, NIST SP 800-115, NIST SP 800-137; NIST Federal Information Processing Standards (FIPS) 199