Queens College Technology Standard	No: QC-ITS-Cyber-026
Risk Assessment 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) performs risk assessments 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 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. SECURITY CATEGORIZATION

IT Department shall:

a. Apply proper security controls to data categorized as confidential by system owners, including protected health information (PHI) and personally identifiable information (PII), in accordance with applicable federal and state laws, directives, policies, regulations, standards, and guidance.

b. Document the security controls (including supporting rationale) in the security plan for the information system.

2. RISK ASSESSMENT

IT Department shall:

a. Conduct (or have conducted by a qualified third-party) an assessment of risk, including the likelihood and magnitude of harm, from the unauthorized access, use, disclosure, disruption, modification, or destruction of the information system and the information it processes, stores, or transmits.

b. Document risk assessment results in annual IT Risk Assessment.

c. Review risk assessment results quarterly.

d. Disseminate risk assessment results to stakeholders.

e. Update the risk assessment quarterly or whenever there are significant changes to the information system or environment of operation (including the identification of new threats and vulnerabilities), or other conditions that may impact the security state of the system.

3. VULNERABILITY SCANNING

IT Department shall:

a. Scan for vulnerabilities in the information system and hosted applications quarterly and/or randomly in accordance with CUNY policy and Queens

College ITS timing determinations and when new vulnerabilities potentially affecting the system/applications are identified and reported.

b. Employ vulnerability scanning tools and techniques that facilitate interoperability among tools and automate parts of the vulnerability management process by using standards for:

    i. Enumerating platforms, software flaws, and improper configurations.

    ii. Formatting checklists and test procedures.

    iii. Measuring vulnerability impact.

c. Analyze vulnerability scan reports and results from security control assessments.

d. Remediate legitimate vulnerabilities within one month in accordance with an organizational assessment of risk.

e. Share information obtained from the vulnerability scanning process and security control assessments with the Chief Information Officer to help eliminate similar vulnerabilities in other information systems (i.e., systemic weaknesses or deficiencies).

f. Employ vulnerability scanning tools that include the capability to readily update the information system vulnerabilities to be scanned.

g. Update the information system vulnerabilities scanned monthly, prior to a new scan, or when new vulnerabilities are identified and reported.

h. Ensure that information systems implement privileged access authorization to all systems for selected vulnerability scanning.

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**
11/09/22	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 – Risk Assessment (RA), NIST SP 800-12, NIST SP 800-30, NIST SP 800-39, NIST SP 800-40, NIST SP 800-60, NIST SP 800-70, NIST SP 800-100, NIST SP 800-115; NIST Federal Information Processing Standards (FIPS) 199