Queens College Technology Standard	No: QC-ITS-Cyber-032
Security Awareness and Training 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 the appropriate level of information security awareness training is provided to all Information Technology (IT) users.

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 users for which Queens College has administrative responsibility, including Faculty, Staff, Administrators, Students as well as outside Contractors as applicable.

4.0 Information Statement

1. Security Awareness Training
    a. Schedule security awareness training as part of initial training for new users.

b. Schedule security awareness training when required by information system changes and then yearly at minimum thereafter.

c. ITS shall determine the appropriate content of security awareness training and security awareness techniques based on the specific organizational requirements and the information systems to which personnel have authorized access. The content shall:

    i. Include a basic understanding of the need for information security and user actions to maintain security and to respond to suspected security incidents.

    ii. Address awareness of the need for operations security. Security awareness techniques can include, for example, displaying posters, offering supplies inscribed with security reminders, generating email advisories/notices from senior organizational officials, displaying logon screen messages, and conducting information security awareness events.

2. Security Awareness | Insider Threat

    a. Include security awareness training on recognizing and reporting potential indicators of insider threat.

3. Role-Based Security Training

    a. Provide role-based security training to personnel with assigned security roles and responsibilities

        i. Before authorizing access to the information system or performing assigned duties

        ii. When required by information system changes and at minimum yearly thereafter.

4. Practical Exercises

    a. Provide practical exercises in security training that reinforce training objectives; practical exercises may include, for example, security training for software developers that includes simulated cyber-attacks exploiting common software vulnerabilities (e.g., buffer overflows), or spear/whale phishing attacks targeted at senior leaders/executives. These types of practical exercises help developers better understand the effects of such vulnerabilities and appreciate the need for security coding standards and processes.

5. Suspicious Communications and Anomalous System Behavior

    a. Provide training to its specified staff on how to recognize suspicious communications and anomalous behavior in organizational information systems.

6. Security Training Records

Queens College shall:

a. Designate personnel to document and monitor individual information system security training activities including basic security awareness training and specific information system security training.

b. Retain individual training records for a minimum of 1 year.

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
10/13/22	Initial changes to apply to Queens College	DVogel
07/12/2023	Continues Changes to Apply to Queens College	DVogel
09/08/2023	Add #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: NIST SP 800-53 – Awareness and Training (AT), NIST SP 800-12, NIST SP 800-16, NIST SP 800-50, NIST SP 800-100; Electronic Code of Federal Regulations (CFR): 5 CFR 930.301