Queens College Technology Standard	No: QC-ITS-Cyber-008
Computer Security Threat Response Standard	**Updated: 08/21/2023**
	Issued By: Queens College, Office of 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 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. Computer Emergency Response

a. A Computer Emergency Response Team (CCERT) shall be established. The CCERT shall be led by the Chief Information Security Officer (CISO) or the Chief Information Officer or their equivalent when the CISO is not available.
b. The CCERT shall consist of representatives from Operations, Client Services, the CIO's office, and any affected Academic Departments.
c. The CCERT shall communicate security information, guidelines for notification processes, identify potential security risks, and coordinate responses to thwart, mitigate, or eliminate security threats to IT resources.
d. Upon the activation of CCERT by the CISO, all CCERT representatives shall report directly to the CISO for the duration of the CCERT activation.

a. Computer Emergency Response Team
    a. Establish and implement Emergency Response Procedures that consist of the following, at minimum:
        i. Creating an incident response policy and plan.
        ii. Developing procedures for performing incident handling and reporting.
        iii. Setting guidelines for communicating with outside parties regarding incidents.
        iv. Selecting a team structure and staffing mode.
        v. Establishing relationships and lines of communication between the incident response team and other groups, both internal (e.g., legal department) and external (e.g., law enforcement agencies.
        vi. Determining what services the incident response team should provide.
        vii. Staffing and training the incident response team.

b. Each department shall develop a notification process, to ensure management notification within the department and to the CCERT, in response to IT security incidents.

c. The CCERT has the responsibility to take necessary corrective action to remediate IT security incidents. Such action shall include all necessary steps to preserve evidence in order to facilitate the discovery, investigation, and prosecution of crimes against IT resources.

d. Each department shall provide CCERT with contact information, including, without limitation, after-hours, for its primary and secondary CCERT representatives (e.g., DISO and Assistant DISO), and immediately notify CCERT of any changes to that information.

e. Each department shall maintain current contact information for all personnel who are important for the response to security threats to IT resources and/or the remediation of IT security incidents.

f. In instances where violation of any law may have occurred, proper notifications shall be made in accordance with IT policies. All necessary action shall be taken to preserve evidence and facilitate the administration of justice.

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

08/21/2023	Conversion to Standard, Add #10, Alignment Gartner Recommendations	DVogel

9.0 Related Documents

10.0 External Documents

National Institute of Standards and Technology (NIST) Special Publication (SP): NIST SP 800-61 - Computer Security Incident Handling Guide