Queens College Technology Standard	No: QC-ITS-Cyber-035
System and Information Integrity 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 system integrity monitoring to include areas of concern such as malware, application and source code flaws, industry supplied alerts and remediation of detected or disclosed integrity issues.

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) Flaw Remediation
    a) Identify, report, and correct information system flaws.

b) Test software and firmware updates related to flaw remediation for effectiveness and potential side effects before installation.
c) Install security-relevant software and firmware updates within 3 months of the release of the updates.
d) Incorporate flaw remediation into the configuration management process.
e) Employ automated mechanisms to determine the state of information system components with regard to flaw remediation.

2) Malicious Code Protection
   a) Update malicious code protection mechanisms whenever new releases are available in accordance with configuration management policy and procedures.
   b) Configure malicious code protection mechanisms to:
      i) Perform periodic scans of the information system and real-time scans of files from external sources at endpoint; network entry/exit points as the files are downloaded, opened, or executed in accordance with the security policy.
      ii) Block malicious code; quarantine malicious code; send alert to administrator in response to malicious code detection.
      iii) Address the receipt of false positives during malicious code detection and eradication and the resulting potential impact on the availability of the information system.
3) Information System Monitoring
   a) Monitor the information system to detect:
      i) Attacks and indicators of potential attacks.
      ii) Unauthorized local, network, and remote connections.
   b) Identify unauthorized use of the information system through defined techniques and methods.
   c) Deploy monitoring devices strategically within the information system to collect security and stability information and at ad hoc locations within the system to track specific types of above transactions of interest to the entity.
   d) Protect information obtained from intrusion-monitoring tools from unauthorized access, modification, and deletion.
   e) Heighten the level of information system monitoring activity whenever there is an indication of increased risk to operations and assets, individuals, other organizations, or based on law enforcement information, intelligence information, or other credible sources of information.
   f) Obtain legal opinion with regard to information system monitoring activities in accordance with applicable state and federal laws, directives, policies, or regulations.
   g) Provide information system monitoring information to authorized personnel or business units as needed.
4) System Generated Alerts

a) The information system that may be generated from a variety of sources, including, for example, audit records or inputs from malicious code protection mechanisms, intrusion detection or prevention mechanisms, or boundary protection devices such as firewalls, gateways, and routers will be disseminated to authorized personnel or business units that shall take appropriate action on the alert(s).
b) Alerts be transmitted telephonically, electronic mail messages, or by text messaging as required. Personnel on the notification list can include system administrators, mission/business owners, system owners, or information system security officers.

5) Security Alerts, Advisories and Directives
   a) Receive information system security alerts, advisories, and directives from selected relevant external organizations on an ongoing basis.
   b) Generate internal security alerts, advisories, and directives as deemed necessary.
   c) Disseminate security alerts, advisories, and directives to various parties as needed.
   d) Implement security directives in accordance with established time frames, or notifies the issuing organization of the degree of noncompliance.
6) Software, Firmware and Information Integrity
   a) Employ integrity verification tools to detect unauthorized changes to Queens College ITS maintained information.
   b) Ensure the information system performs an integrity check at startup, and/or at reboot as well as regular defined intervals.
   c) Incorporate the detection of unauthorized changes into the incident response capability.
7) Spam Protection
   a) Employ spam protection mechanisms at information system entry and exit points to detect and take action on unsolicited messages.
   b) Update spam protection mechanisms when new releases are available in accordance with the configuration management policy and procedures.
   c) Manage spam protection mechanisms centrally.
   d) Ensure information systems automatically update spam protection mechanisms.
8) Information Handling and Retention
   a) Handle and retain information within the information system and information output from the system in accordance with applicable state and federal laws, directives, policies, regulations, standards, and operational requirements.

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
09/08/2023	Add #10, Convert to Standard, Align 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 – System and Information Integrity (SI), NIST SP 800-12, NIST SP 800-40, NIST SP 800-45, NIST SP 800-83, NIST SP 800-61, NIST SP800-83, NIST SP 800-92, NIST SP 800-100, NIST SP 800-128, NIST SP 800-137, NIST SP 800-147, NIST SP 800-155