Queens College Technology Standard	No: QC-ITS-Cyber-036
System and Services Acquisition Standards	**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 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) Allocations of Resources
   a) Determine information security requirements for the information system or information system service in mission/business process planning.
   b) Determine, document, and allocate the resources required to protect the information system or information system service as part of its capital planning and investment control process.

c) Establish a discrete line item for information security in organizational programming and budgeting documentation.

2) System Development Life Cycle
   a) Manages the information system using the system development life cycle to ensure incorporation information security considerations.
   b) Defines and documents information security roles and responsibilities throughout the system development life cycle.
   c) Identifies individuals having information security roles and responsibilities.
   d) Integrates the information security risk management process into system development life cycle activities.
3) Acquisition Process
   a) IT shall ensure the acquisition process includes the following requirements, descriptions, and criteria, explicitly or by reference, in the acquisition contract for the information system, system component, or information system service in accordance with applicable federal, state, and local laws, Executive Orders, directives, policies, regulations, standards, guidelines, and mission and business needs:
      i) Security functional requirements.
      ii) Security strength requirements.
      iii) Security assurance requirements.
      iv) Security-related documentation requirements.
      v) Requirements for protecting security-related documentation.
      vi) Description of the information system development environment and environment in which the system is intended to operate.
      vii) Acceptance criteria.
4) Security Controls

Information Technology (IT) shall require the information system, system component, or information system service:

   a) Describe the functional properties of the security controls to be employed; security-relevant external system interfaces; high-level design, low-level design, source code or hardware schematics that meet the business requirements.
   b) Identify early in the system development life cycle, the functions, ports, protocols, and services intended for organizational use.
   c) Employ only information technology products on the FIPS 201-approved products list for Personal Identity Verification (PIV) capability implemented within information systems.
5) Information System Documentation
   a) Obtain administrator documentation for the information system, system component, or information system service that describes:
      i) Secure configuration, installation, and operation of the system, component, or service.
      ii) Effective use and maintenance of security functions/mechanisms.
      iii) Known vulnerabilities regarding configuration and use of administrative (i.e., privileged) functions.

b) Obtain user documentation for the information system, system component, or information system service that describes:
    i) User-accessible security functions/mechanisms and how to effectively use those security functions/mechanisms.
    ii) Methods for user interaction, which enables individuals to use the system, component, or service in a more secure manner.
    iii) User responsibilities in maintaining the security of the system, component, or service.
c) Document attempts to obtain information system, system component, or information system service documentation when such documentation is either unavailable or nonexistent.
d) Protect documentation as required, in accordance with the risk management strategy.
e) Distribute documentation to only authorized persons or entities.

6) Security Engineering Principles
    a) Apply industry standard information system security engineering principles in the specification, design, development, implementation, and modification of the information system.
7) External Information System Services
    a) Require that providers of external information system services comply with organizational information security requirements and employ security controls in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance.
    b) Define and document government oversight and user roles and responsibilities with regard to external information system services.
    c) Employ processes, methods, and techniques to monitor security control compliance by external service providers on an ongoing basis.
    d) Require providers of external information system services to identify the functions, ports, protocols, and other services required for the use of such services.
8) Developer Configuration Management
    a) IT Department shall ensure developers of the information system, system component, or information system service:
    b) Perform configuration management during system, component, or service design; development, implementation, and/or operation.
    c) Document, manage, and control the integrity of changes to configuration items under configuration management.
    d) Implement only organization-approved changes to the system, component, or service.
    e) Document approved changes to the system, component, or service and the potential security impacts of such changes.
    f) Track security flaws and flaw resolution within the system, component, or service and report findings to authorized personnel and/or business units.
9) Developer Configuration Management
    a) Require the developer of the information system, system component, or information system service to enable integrity verification of software and firmware components.

i) Provide an alternate configuration management process using organizational personnel in the absence of a dedicated developer configuration management team.
ii) Require the developer of the information system, system component, or information system service to enable integrity verification of hardware components.
iii) Require the developer of the information system, system component, or information system service to employ tools for comparing newly generated versions of security-relevant hardware descriptions and software/firmware source and object code with previous versions.
iv) Require the developer of the information system, system component, or information system service to maintain the integrity of the mapping between the master build data (hardware drawings and software/firmware code) describing the current version of security-relevant hardware, software, and firmware and the on-site master copy of the data for the current version.
v) Require the developer of the information system, system component, or information system service to execute procedures for ensuring that security-relevant hardware, software, and firmware updates distributed to the organization are exactly as specified by the master copies.

10) Developer Security Testing and Evaluation
   a) If determined to by the CISO's office, IT Department shall require the developer of the information system, system component, or information system service to:
      i) Create and implement a security assessment plan.
      ii) Perform unit; integration; system; regression testing/evaluation.
      iii) Produce evidence of the execution of the security assessment plan and the results of the security testing/evaluation.
      iv) Implement a verifiable flaw remediation process.
      v) Correct flaws identified during security testing/evaluation.
      vi) Employ static code analysis tools to identify common flaws and document the results of the analysis.
      vii) Perform threat and vulnerability analyses and subsequent testing/evaluation of the as-built system, component, or service.

11) Independent Verification of Assessment Plans / Evident
   a) If needed, require an independent agent satisfying to verify the correct implementation of the developer security assessment plan and the evidence produced during security testing/evaluation.
      i) Ensure that the independent agent either is provided with sufficient information to complete the verification process or has been granted the authority to obtain such information.
      ii) Perform a manual code review of defined processes, procedures, and/or techniques.
      iii) Perform penetration testing.
      iv) Verify that the scope of security testing/evaluation provides complete coverage of required security controls.
      v) Employ dynamic code analysis tools to identify common flaws and document the results of the analysis.

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**
10/18/2022	Initial changes to apply to Queens College	DVogel
09/08/2023	Conversion to Standard, Add #10, Alignment to Gartner Recommendations	DVogel

9.0 Related Documents

10.0 External Documents