Queens College Technology Standard	No: QC-ITS-Cyber-034
System and Communications Protection Standards	**Updated: 08/09/2023**
	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. Application Partitioning

    a. Separate user functionality from information system management functionality either logically or physically.

Information system management functionality includes, for example, functions necessary to administer databases, network components, workstations, or servers, and typically requires privileged user access.

2. Information In Shared Resources

    a. Prevent unauthorized and unintended information transfer via shared system resources.

    This control prevents information, including encrypted representations of information, produced by the actions of prior users/roles from being available to any current users/roles (or current processes) that obtain access to shared system resources (e.g., registers, main memory, hard disks) after those resources have been released back to information systems.

3. Denial Of Service Protection

    a. Ensure that the information system protects against or limit the effects of the denial of service attacks by employing security safeguards.

    b. The information system restricts the ability of individuals to launch denial of service attacks against other information systems.

4. Boundary Protection

    a. Monitor and control communications at the external boundary of the system and at key internal boundaries within the system.

    b. Implement sub-networks for publicly accessible system components that are [physically; logically] separated from internal organizational networks, and connected to external networks or information systems only through managed interfaces consisting of boundary protection devices arranged in accordance with an organizational security architecture.

    Managed interfaces include, for example, gateways, routers, firewalls, guards, network-based malicious code analysis and virtualization systems, or encrypted tunnels implemented within security architecture.

5. Transmission Confidentiality And Integrity

    a. Deploy information systems that protect the [confidentiality; integrity] of transmitted information.

This control applies to both internal and external networks and all types of information system components from which information can be transmitted (e.g., servers, mobile devices, notebook computers, printers, copiers, scanners, facsimile machines).

6. Network Disconnect

    a. Ensure information systems are configured to terminate the network connection associated with a communications session at the end of the session or after an QC defined time period of inactivity; this control applies to both internal and external networks.

    Terminating network connections associated with communications sessions include, for example, de-allocating associated TCP/IP address/port pairs at the operating system level, or de-allocating networking assignments at the application level if multiple application sessions are using a single, operating system-level network connection.

7. Cryptographic Key Establishment And Management

    a. Establish and manage cryptographic keys for required cryptography employed within the information system.

8. Cryptographic Protection

    a. Implement cryptography in accordance with applicable federal and state laws, directives, policies, regulations, and standards.

    Cryptography can be employed to support a variety of security solutions including, for example, the protection of classified and Controlled Unclassified Information, the provision of digital signatures, and the enforcement of information separation when authorized individuals have the necessary clearances for such information but lack the necessary formal access approvals.

9. Collaborative Computing Devices

    a. Prohibit remote activation of collaborative computing devices with the following exceptions: Written Approval from CISO's Office.

    b. Provide an explicit indication of use to users physically present at the devices.

    Collaborative computing devices include, for example, networked white boards, cameras, and microphones. Explicit indication of use includes, for example, signals to users when collaborative computing devices are activated.

10. Public Key Infrastructure Certificates

    a. Issue public key certificates under a QC policy or obtain public key certificates from an approved service provider.

    b. Manage information system trust stores for all key certificates to ensure only approved trust anchors are in the trust stores.

11. Mobile Code

    a. Define acceptable and unacceptable mobile code and mobile code technologies.

    b. Establish usage restrictions and implementation guidance for acceptable mobile code and mobile code technologies.

    c. Authorize, monitor, and control the use of mobile code within the information system.

       Decisions regarding the employment of mobile code within organizational information systems are based on the potential for the code to cause damage to the systems if used maliciously.

12. Voice Over Internet Protocol

    a. Establish usage restrictions and implementation guidance for Voice over Internet Protocol (VoIP) technologies based on the potential to cause damage to the information system if used maliciously.

    b. Authorize, monitor, and control the use of VoIP within the information system.

13. Secure Name / Address Resolution Service (Authoritative Source)

    a. Provide additional data origin authentication and integrity verification artifacts along with the authoritative name resolution data the system returns in response to external name/address resolution queries.

    b. Provide the means to indicate the security status of child zones and (if the child supports secure resolution services) to enable verification of a chain of trust among parent and child domains, when operating as part of a distributed, hierarchical namespace.

       This control enables external clients including, for example, remote Internet clients, to obtain origin authentication and integrity verification assurances for the host/service name to network address resolution information obtained through the service.

14. Secure Name / Address Resolution Service (Recursive Or Caching Resolver)

    a. Ensure information systems that requests and performs data origin authentication and data integrity verification on the name/address resolution responses the system receives from authoritative sources.

       Each client of name resolution services either performs this validation on its own, or has authenticated channels to trusted validation providers. Information systems that provide name and address resolution services for local clients include, for example, recursive resolving or caching domain name system (DNS) servers.

15. Architecture And Provisioning For Name / Address Resolution Service

    a. Ensure the information systems that collectively provide name/address resolution service for an organization are fault-tolerant and implement internal/external role separation.

    b. Employ at least two authoritative domain name system servers, one configured as the primary server and the other configured as the secondary server, to eliminate single points of failure and to enhance redundancy.

       Information systems that provide name and address resolution services include, for example, domain name system (DNS) servers.

16. Session Authenticity

    a. Ensure the information system protects the authenticity of communications sessions.

       This control addresses communications protection at the session versus packet level (e.g., sessions in service-oriented architectures providing web-based services) and establishes grounds for confidence at both ends of communications sessions in ongoing identities of other parties and in the validity of information transmitted.

17. Protection Of Information At Rest

    a. Ensure the information system protects the [confidentiality; integrity] of information at rest.

       This control addresses the confidentiality and integrity of information at rest and covers user information and system information. Information at rest refers to the

state of information when it is located on storage devices as specific components of information systems.

18. Process Isolation

    a. Ensure the information system maintains a separate execution domain for each executing process.

Information systems can maintain separate execution domains for each executing process by assigning each process a separate address space. Each information system process has a distinct address space so that communication between processes is performed in a manner controlled through the security functions, and one process cannot modify the executing code of another process.

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
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 SP800-53a - System and Communications Protection (SC), NIST SP 800-12, NIST SP 800-28, NIST SP 800-41, NIST SP 800-52, NIST SP 800-56, NIST SP 800-57, NIST SP 800-58, NIST SP 800-77, NIST SP 800-81, NIST SP 800-95, NIST SP 800-100, NIST SP 800-111, NIST SP 800-113; NIST Federal Information Processing Standards (FIPS) 140-2, FIPS 197, FIPS 199