Queens College **Technology Standard**	**No: QC-ITS-Cyber-018**
Security Maintenance Standard	**Updated: 08/25/2023**
	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 are maintained 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

4.1. Controlled Maintenance

4.1.1. Schedule, perform, document, and review records of maintenance and repairs on information system components in accordance with manufacturer or vendor specifications and/or requirements conducted by local IT and/or outsourced IT entities.

4.1.2. Approve and monitor all maintenance activities, whether performed on site or remotely and whether the equipment is serviced on site or removed to another location.

4.1.3. Require that system owners explicitly approve the removal of the information system or system components from facilities for off-site maintenance or repairs.

4.1.4. Sanitize equipment to remove all information from associated media prior to removal from Queens College facilities for off-site maintenance or repairs.

4.1.5. Check all potentially impacted security controls to verify that the controls are still functioning properly following maintenance or repair actions.

4.1.6. Include IT and system owner's defined maintenance-related information in maintenance records.

4.1.7. For those components not directly associated with information processing such as scanners, copiers, and printers, maintenance records must include date and time of maintenance, entity performing the maintenance, maintenance performed, components replaced or removed including identification/serial numbers as applicable.

4.2. Maintenance Tools

4.2.1. Ensure that IT approve, control, and monitor information system maintenance tools.

4.2.2. If needed, inspect the maintenance tools carried into a facility by maintenance personnel for improper or unauthorized modifications.

4.2.3. If needed, check media containing diagnostic and test programs for malicious code before the media are used in the information system.

4.3. Non-Local Maintenance

4.3.1. Approve and monitor non-local maintenance and diagnostic activities.

4.3.2. Allow the use of nonlocal maintenance and diagnostic tools only as consistent with policy and documented in the security plan for the information system.

4.3.3. Employ strong authenticators in the establishment of nonlocal maintenance and diagnostic sessions.

4.3.4. Maintain records for nonlocal maintenance and diagnostic activities.

4.3.5. Terminate session and network connections when nonlocal maintenance is completed.

4.3.6. Document in the security plan for the information system, the policies and procedures for the establishment and use of nonlocal maintenance and diagnostic connections.

4.4. Maintenance Personnel

4.4.1. Establish a process for maintenance personnel authorization and maintain a list of authorized maintenance organizations or personnel.

4.4.2. Ensure that non-escorted personnel performing maintenance on the information system have required access authorizations.

4.4.3. Designate personnel with required access authorizations and technical competence to supervise the maintenance activities of personnel who do not possess the required access authorizations.

4.5. Timely Maintenance

4.5.1. Obtain maintenance support and/or spare parts for information systems as agreed upon within the service level agreement between IT and the system owner.

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**
9/27/22	Initial changes to apply to Queens College	DVogel
08/25/2023	Conversion to Standard, Add #10, Alignment to Gartner Recommendations	DVogel

9.0 Related Documents

10.0 External Documents

National Institute of Standards and Technology (NIST) Special Publications (SP): NIST SP 800-53 – System Maintenance (MA), NIST SP 800-12, NIST SP 800-63, NIST SP 800-88, NIST SP 800-100; Federal Information Processing Standards (FIPS) 140-2, FIPS 197, FIPS 201