Queens College **Information Technology Policy**	**No: PR.DS.1.7 Media Protection**
IT Policy: **Media Protection Policy**	**Updated: 10/13/22**
	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) controls access to and disposes of media resources in compliance with IT security policies, standards, and procedures.

2.0 Authority

- **Responsible Office(s):** Queens College Information Technology Services & Queens College General Counsel
- **Responsible Executive(s)**: General Counsel
- **Responsible Officer(s)**: Chief Information Security Officer

3.0 Scope

This is a college-wide policy 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 policy 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 policy 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. Media Access:
    a. Restrict access to Sensitive and/or Confidential media to needed Faculty/Staff/Admins
    b. Mark information system media indicating the distribution limitations, handling caveats, and applicable security markings of digital and non-digital information media.

2. Media Storage
    a. Specify staff to physically control and securely store media within defined controlled areas.
    b. Protect information system media until the media are destroyed or sanitized using approved equipment, techniques, and procedures.
3. Media Transport
    a. Protect and control media during transport outside of controlled areas.
    b. Maintain accountability for information system media during transport outside of controlled areas.
    c. Document activities associated with the transport of information system media.
    d. Restrict the activities associated with the transport of information system media to authorized personnel.
4. Media Sanitization
    a. Sanitize prior to disposal, release out of organizational control, or release for reuse using Queens College Policies in accordance with applicable federal and organizational standards and policies.
    b. Employ sanitization mechanisms with the strength and integrity commensurate with the security category or classification of the information.
5. Media Use
    a. Prohibit the use of unsecured media on Queens College owned equipment when handling Confidential/Sensitive materials.

5.0 Compliance

This policy 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 policy 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 policy owner at:

Chief Information Security Officer
Aaron Wheeler
Aaron.Wheeler@qc.cuny.edu

8.0 Revision History

This standard shall be subject to periodic review to ensure relevancy.

Date	Description of Change	Reviewer
10/13/22	Initial changes to apply to Queens College	DVogel
03/20/25	Added number convention and control title	AWheeler
	Policy Implemented	

9.0 Related Documents

National Institute of Standards and Technology (NIST) Special Publications (SP): NIST SP 800-53 – Media Protection (MP), NIST SP 800-12, NIST SP 800-56, NIST SP 800-57, NIST SP 800-60, NIST SP 800-88, NIST SP 800-100, NIST SP 800-111;
NIST Federal Information Processing Standards (FIPS) 199