Queens College Information Technology Policy	No: PR.AT.1.1 Personnel Security
IT Policy: **Personnel Security Policy**	Updated: 10/18/2022
	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 & 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. Position Risk Designation
   Information Technology (IT) shall:

   a. Assign a risk designation to all positions.
   b. Review and update position risk designations annually.

2. Personnel Termination
    a. Departments shall, upon termination of individual employment:
    b. Provide information of termination to disable information system access within 24 hrs
    c. Terminate/revoke any authenticators/credentials associated with the individual.
    d. Retrieve all security-related information system-related property.
    e. Retain access to information and information systems formerly controlled by terminated individual.

    Information system-related property includes, for example, hardware authentication tokens, system administration technical manuals, keys, identification cards, and building passes. Exit interviews ensure that terminated individuals understand the security constraints imposed by being former employees and that proper accountability is achieved for information system-related property. Security topics of interest at exit interviews can include, for example, reminding terminated individuals of nondisclosure agreements and potential limitations on future employment. Exit interviews may not be possible for some terminated individuals.

    Queens College shall:

    a. Notify terminated individuals of applicable, legally binding post-employment requirements for the protection of information.

    b. Require terminated individuals to sign an acknowledgment of post-employment requirements as part of the termination process as directed by Counsel and Human Resources (HR).

    c. Employ automated mechanisms to notify correct areas upon termination of an individual.
3. Personnel Transfer
    Departments shall:

    a. Review and confirm ongoing operational need for current logical and physical access authorizations to information systems/facilities when individuals are reassigned or transferred to other positions.
    b. Modify access authorization as needed to correspond with any changes in operational need due to reassignment or transfer.

        This control applies when reassignments or transfers of individuals are permanent or of such extended durations as to make the actions warranted.

4. Access Agreements
   IT Department shall:

    a. Develop and document access agreements for information systems.
    b. Review and update the access agreements annually.
    c. Ensure that individuals requiring access to information and information systems:
        a. Sign appropriate access agreements prior to being granted access.
        b. Re-sign access agreements to maintain access to information systems when access agreements have been updated or annually.

    Access agreements include, for example, nondisclosure agreements, acceptable use agreements, rules of behavior, and conflict-of-interest agreements.

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
10/18/2022	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 800-53a – Personnel Security (PS), NIST SP 800-12, NIST SP 800-60, NIST SP 800-73, NIST SP 800-78, NIST SP 800 -100; Electronic Code of Federal Regulations (CFR): 5 CFR 731.106; Federal Information Processing Standards (FIPS) 199 and 201; Intelligence Community Directive (ICD) 704 Personnel Security Standards