Queens College Information Technology Policy	No: ID.RM.1.3 Information Security Exception
IT Policy: **Information Security Exception Policy**	**Updated: 9/21/22**
	Issued By: Queens College, Chief Information Security Officer **Owner: Queens College Information Technology Services**

1.0 Purpose and Benefits

This purpose of this policy is to provide a method for obtaining an exception to compliance with a published information security policy or standard.

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 other Information Security Policies for which Queens College has administrative responsibility.

4.0 Information Statement

An exception may be granted by the Chief Information Security Officer (CISO) of Queens College, or their designee, for non-compliance with a policy or standard resulting from:

- Implementation of a solution with equivalent protection to the requirements in the policy or standard.
- Implementation of a solution with superior protection to the requirements in the policy or standard.

- Impending retirement of a system.
- Inability to implement the policy or standard due to some limitation (i.e., technical constraint, business limitation or statutory requirement).

Exceptions are reviewed on a case-by-case basis and their approval is not automatic. Exceptions that are granted will be for a specific period of time, not to exceed one year. Upon expiration of the exception, an extension of the exception may be requested, if it is still required.

The exception request must be submitted on a completed Exception Request Form and must include:

- Description of the non-compliance
- Anticipated length of non-compliance
- Proposed assessment of risk associated with non-compliance
- Proposed compensating controls for managing the risk associated with non-compliance
- Proposed corrective action plan
- Proposed review date, if less than one year, to evaluate progress toward compliance
- The Exception Request Form must be signed by the following:
    - Information/Business Process Owner
    - Information/Business Process Owner's Supervisor
    - Dean/VP

If the non-compliance with the security policy or standard is due to a superior solution, an exception is still required and will normally be granted until the published policy or standard can be revised to include the new solution.

Upon submission of the Exception Request Form, the CISO's office will contact the requester to confirm receipt and request additional information, if needed. Once all required information has been received, the CISO will either grant or deny the request.

Upon approval, the CISO's office will send the approved Exception Request Form to the requestor. If the request is denied, the Exception Request Form will be returned with a brief explanation of why the CISO denied the request.

In the event that the request is denied, the Dean/VP and the CIO who signed the Exception Request Form may request a meeting with the CIO and the CISO to discuss the circumstances giving rise to the request and means of addressing those circumstances.

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.

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 policy shall be reviewed at least once every year to ensure relevancy.

Date	**Description of Change**	**Reviewer**
09/21/2022	Initial Setup of Policy	DVogel
03/20/25	Added number convention and control title	AWheeler
03/20/25	Updated contact info on form	AWheeler
	Policy Implemented	

9.0 Related Documents

Exception Request Form

Confidential when completed

Section 1: Exception		
1.1 Requestor Information		
Name:	Phone:	Date:
Business Unit:		
Email:		
1.2 Exception Details		
Policy Reference:	Standard Reference:	Exception End Date: (no more than one year)
Entity Impacted:		
System(s) Hardware Impacted (if applicable):		
Will this impact the process, stage and/or transmission of PII? **Yes _____** **No _____**		
1.3 Reason for Exception Request		
1.4 Description/Assessment Risk		
1.5 Compensating Controls (to mitigate risk associated with non-compliance)		
1.6 Corrective Action Plan		

Section 2: Requestor Authorizations		
2.1 Information/Business Process Owner:	X_____ [Information/Business Process Owner]	**Date:**
2.2 Information/Business Process Owner's Supervisor:	X_____ [Information/Business Process Owner's Supervisor]	**Date:**
2.3 Chief Information Officer (CIO):	X_____ [CIO]	**Date:**
2.4 Dean/VP	X_____ [Dean/VO]	**Date:**
Return to: Aaron Wheeler@qc.cuny.edu	Mail to: Aaron Wheeler I-Building 151 Queens College	

Section 3: Exception Approval/Denial ***(For CISO Use Only)***		
Exception: **Approved** ____ **Denied** ____	**Proposed Review Date:**	
Reason for Denial:		
3.1 Chief Information Security Officer/Deputy CISO:		**Date:**