Collin College Technology Services (CC-TS)
Policy/Procedure Exception – Information Security Procedure (ISP)

PURPOSE

This ISP aims to provide a method for obtaining an exception to compliance with a published information security policy, ISP, or standard.

SCOPE

Any exception to Collin College's information security policies, procedures, processes, and operational standards must be reviewed and approved for continued network connectivity.

STATEMENT

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

- Implementation of a solution with equivalent protection to the policy, ISP, or standard requirements.
- Implementation of a solution with superior protection to the policy, ISP, or standard requirements.
- Impending retirement of a system.
- Inability to implement the policy, ISP, or standard due to some limitation (i.e., technical constraint, business limitation, or statutory requirement).

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

The exception request must be submitted on a completed Exception Request Form found at the bottom of this ISP 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:

- System Owner
- Chief Information Security Officer (CISO)
- Chief Information Officer
- SVP/Campus Operations

If non-compliance is due to a superior solution, an exception is still required and will normally be granted until the published policy, ISP, 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, reviewed, and approved by all parties, the CISO will 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.

If the request is denied, the SVP/Campus Operations and the CIO who signed the Exception Request Form may request a meeting with the CISO to discuss the circumstances giving rise to the request and the means of addressing those circumstances.

COMPLIANCE

This ISP shall take effect upon publication. Compliance with all policies, ISPs, and standards is expected. Policies, ISPs, and standards may be amended at any time.

If compliance with this ISP is not feasible or technically possible, or if deviation from this ISP is necessary to support a business function, entities shall request an exception through the Chief Information Security Officer's exception process.

IMPLEMENTATION INFORMATION

Review Frequency:	Annually
Responsible Person:	CISO
Approved By:	Abe Johnson, Ed. D.
Approval Date:	01/12/2024

REVISION HISTORY

Version:	Date:	Description:
1.0	01/11/2024	Initial document

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:	ISP/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 System Owner:	X_____	**Date:**
2.2 Chief Information Security Officer (CISO)	X_____	**Date:**
2.3 Chief Information Officer (CIO):	X_____	**Date:**
2.4 SVP/Campus Operations:	X_____	**Date:**
Return to: [email]	[address]	

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:**