Purpose

The purpose of this procedure is to formalize the steps required to describe, document, and obtain appropriate approvals for information systems, networks, devices, applications, users, or other objects that cannot be brought into alignment with Central's security program. For the duration of this procedure the former list will be summarized as information systems.

Step 1: Describe the Exception

The requester (individual or department) and the Information Technology Division will meet to outline the information system and clearly document why it cannot be brought into alignment with the security program.

Step 2: Identify Mitigation Measures

Mitigation planning is a joint effort that may include internal staff, external vendors, or contractors. Mitigation measures fall into two categories:

Technical Controls

Examples include, but are not limited to:

- Network isolation
- Data isolation
- Segregated accounts
- Access restrictions

Administrative Controls

Examples include, but are not limited to:

- Agreements to limit certain behaviors
- Commitments not to share passwords
- Separation of duties
- Restrictions on making configuration changes
- Restrictions on accessing protected data classes

Step 3: Define Roles and Responsibilities

Both parties will document their responsibilities:

Information Technology Division

IT will outline the controls it will perform to ensure the information system operates safely.

Requester (Person or Department)

The requester will outline the controls they will perform to ensure safe system operations.

If either party fails to follow the agreed-upon controls, the information system will be powered off or disabled until both parties fulfill their obligations.

Step 4: Approvals and Annual Renewals

A formal exception request form will be completed and submitted for approval.
The form will summarize Steps 1–3 and must be signed by:

1. **Requester**
2. **Requester's Supervisor** (Chair or Director)
3. **Executive-Level (**Chief, VP, or Dean)
4. **CIO, CISO, or Designee**

By signing the exception request, all parties acknowledge the risk of deviating from the security program and accept responsibility for the decision.

Annual Renewal

Each security exception is valid for **one year**.
Exceptions must be reviewed annually to determine whether the information system can now be brought into alignment with the security program. If not, both parties must reassess roles and responsibilities and complete the approval process again.

Document Control

Document Title	Security Exception Procedure
Version	2.0
Status	Prod
Owner	Information Technology Division
Approval Date	7/7/2026
Next Review	7/7/2028