

Example Security Policy Exception Process

This is an example security policy exception process. Use this as a guide to write a security policy exception process for your organization.

~~~~~

## Security Policy Exception Process

### 1.0 Purpose

At our organization, we prioritize security for all information assets governed by our security policies and standards. However, in some scenarios, full compliance isn't feasible. In such cases, our exception process documents and secures approval, aligning with our security strategy while maintaining our commitment to security.

### 2.0 Purpose

The purpose of this process is to establish a method for documenting exceptions to compliance with our established information security policies, standards, and practices.

### 3.0 Scope

This process applies to all information assets and processes within our organization.

### 4.0 Process

#### 4.1 Request Initiation

- Any employee or stakeholder who believes that an exception to a security policy, standard, or practice is necessary can initiate the exception process.
- An exception can be approved under the following circumstances:
  - **Legacy system retention:** It is necessary for business continuity despite noncompliance.
  - **Compliance cost vs. risk:** Significant financial burden outweighs risk reduction.
  - **Temporary exception:** Immediate compliance would disrupt critical operations.
  - **Long-term exception:** Compliance negatively affects ongoing operations.
  - **Regulatory conflict:** A specific regulation conflicts with internal security policies.
  - **Technological limitations:** A technology or system cannot meet security standards, and no alternatives exist.

- **Alternative solution:** An alternative solution with equivalent protection is better suited to the situation.
- **Superior solution:** A superior security solution is more effective than the existing policy.
- **Emergency situations:** Immediate action is required to mitigate risks or maintain business continuity.
- **Third-party dependencies:** A third-party vendor's compliance directly impacts the organization.
- **Additional scenarios:** If an individual or team believes their situation warrants an exception not listed, they may submit a request for review. Approval decisions will be made on a case-by-case basis.

## 4.2 Exception Request

- Exception requests must be submitted using the Security Policy Exception Request form.
- The exception request must document:
  - The specific security policy/standard for which an exception is requested
  - Any relevant section or reference within the policy/standard (if applicable)
  - A clear description of the exception request
  - The reason for the exception, including how it aligns with business goals and objectives
  - An assessment of the potential impact of this exception on security, along with any associated risks
  - Details of mitigating controls or measures to minimize risks associated with this exception
  - The specified duration of the exception, including the start and end dates
  - The approval of the requester's immediate supervisor, including their name and approval date

## 4.3 Review and Approval

- **Guidelines:** Requests for exceptions are reviewed for validity and are not automatically approved. Periodic reviews of exception requests are conducted to confirm that assumptions or business conditions remain unchanged.
- **Alignment with policies and standards:** The exception process applies to all information security policies and standards.
- **Standardization of exception types:** Approved exception types will consistently follow the same ruling unless exceptional circumstances arise.
- **Stakeholder involvement:** Relevant stakeholders, such as legal, compliance, and business unit leaders, will be consulted or notified as needed.

- **Escalation procedure:** Disagreements or uncertainties will be escalated to higher management or executives.
- **Communication:** Requesters will be promptly informed of the status of their exception request.
- **Appeal process:** If denied, requesters may initiate an appeal by providing additional information or documentation.
- **Exception revocation:** Approvals may be revoked if a security incident occurs or if there is a policy violation.

#### 4.4 Documentation

- **Initial documentation submission:** The primary form of documentation is the completed Security Policy Exception Request form.
- **Recordkeeping:** All completed exception request forms are retained and accessible by the security team. The information security officer will securely maintain any supporting documentation.
- **Document retention:** All documentation related to exception requests and approvals will be retained in accordance with company retention procedures.

#### 4.5 Monitoring

- **Exception validity:** Exceptions are valid for one year unless specified otherwise.
- **Monthly review:** The information security officer reviews expired exceptions monthly to determine their status.
- **Renewal process:** The requesting supervisor must reaffirm the original request at the time of renewal.
- **Changed conditions:** A new request must be submitted if conditions have substantially changed.

#### 4.6 Closure

- **Closure determination:** The information security officer will determine the closure status of exceptions and communicate it to relevant parties.
- **Documentation update:** Exception documentation will be updated upon closure to reflect the final resolution status.
- **Retention and archival:** Closed exception records will be retained and archived securely for audit and reference purposes.

### 5.0 Definitions

None

### 6.0 Revision History

- **Version 1.0:** [Date]—first published version