Exception Standard

Last Modified on 04/24/2025 2:38 pm EDT

For more details about the Information Security Office, **please visit our website**!

To submit an Exception Request, **click here**.

1. Purpose and Scope

This Exception Standard outlines the process for requesting, assessing, approving, and managing risk-based exceptions to Penn policies, Wharton's Information Security Policy and/or related Standards. This Standard ensures that all exceptions are carefully evaluated to mitigate risks to the confidentiality, integrity, and availability of Wharton assets.

This Standard applies to all academic and administrative units, centers, initiatives, third-party agents, as well as any Wharton affiliate authorized to access institutional data, services, and systems. Exceptions to Wharton/Penn policies and standards will be reviewed by ISO and submitted to Penn's IT Policy Committee (ITPC).

2. Roles and Responsibilities

Requestor

The individual or group responsible for submitting the exception request. This includes providing justification, identifying security/privacy compensating controls, and collaborating with ISO to assess risks.

Risk Owner

The individual or group responsible for managing and accepting the risk associated with the exception.

Information Security Office (ISO)

ISO is responsible for reviewing, assessing, approving or denying exception requests, and maintaining a record of all exceptions.

Approval Authority

Depending on the level of risk, approval may require:

- **ISO Approval:** For low and moderate-risk exceptions.
- **Wharton Executive Approval**: For high-risk exceptions.
- **ITPC Variance Submission:** For exceptions to Penn policy.

3. Exception Request Process

Step 1: Identify the Need for an Exception or Exemption

The Requestor identifies a situation where adherence to Penn policies, Wharton's Information Security Policy and/or related Standards is not feasible and gathers relevant details for submission. Exceptions are granted for one fiscal quarter with the potential renewal not to exceed one fiscal year.

In limited circumstances, exemptions to Penn policies, Wharton's Information Security Policy and/or related Standards are granted permanently if risk is accepted. Exemptions are automatically High-risk and will be thoroughly evaluated.

Step 2: Submit an Exception Request

The Requestor submits the exception request to ISO using the Exception Request Form. Exemptions should also be submitted to ISO via this form. Required examples include:

- Policy or Standard in question.
- Justification for the exception, including business or academic impact.
- Security/privacy compensating controls proposed to mitigate risks.

Step 3: Risk Assessment

ISO conducts a risk assessment to evaluate:

- Risk Impact: Confidentiality, integrity, and availability of impacted systems.
- Likelihood of Exploitation: Potential threats and vulnerabilities.
- Proposed Compensating Controls: Effectiveness in mitigating risks.
- Compliance Impact: Alignment with regulatory requirements and institutional obligations.

Risk Severity Calculation

Likelihood (frequency) **Impact**	**Critical**	**High**	**Moderate**	**Low**
Critical (monthly)	Critical	Critical	Critical	High
High (annually)	Critical	High	High	Moderate
Moderate (less than annually)	Critical	High	Moderate	Low
Low (unlikely to ever occur)	High	Moderate	Low	Low

Step 4: Approval or Denial

Based on the risk assessment:

- Low/Moderate-Risk: ISO may approve or deny the exception.

- High-Risk: ISO will escalate to Wharton executive leadership for approval.
- Documentation: Approved exceptions are recorded in the Exception Repository.

4. Risk Assessment and Mitigation

ISO will analyze the risks associated with a requested exception, identify potential impacts on systems and stakeholders, and evaluate the adequacy of proposed compensating controls.

If an exception is granted, the Requestor must:

- Implement the approved security/privacy compensating controls.
- Ensure adherence to all conditions outlined in the exception approval.
- Collaborate with ISO to address any residual risks.

5. Notification and Consultation

ISO is responsible for notifying stakeholders, including affected departments and system owners, of approved exceptions.

ITPC Variance Review: Exceptions to Penn policies require escalation by ISO to ITPC to evaluate compliance, operational, and reputational risks.

6. Recordkeeping

ISO is responsible for maintaining a centralized Exception Repository that includes:

- Requestor details.
- Risk assessment documentation.
- Approved compensating controls.
- Exception duration and expiration date.
- Review and renewal status.

ISO will review exceptions quarterly, to ensure exceptions remain justified, relevant systems move towards compliance, and expired exceptions are resolved or renewed with updated risk assessments.

7. Duration and Renewal

All exceptions are granted for one fiscal quarter, with the potential for renewal not to exceed one fiscal calendar year. Expiring exceptions must be:

- Reviewed and updated if needed.

- Rescinded if compliance has been achieved.

To renew an exception, the Requestor must:

- Submit a renewal request 30 days before expiration.
- Provide updated justification and risk assessment.
- Collaborate with ISO to reassess risks and controls.