

# Policy Exception Policy

## Purpose

The purpose of this policy is to ensure that exceptions to security policies are documented and approved through an exception process.

## Scope

This policy applies to all published Nested Knowledge information security policies. Employees and contractors must abide by this exception process.

## Policy

An exception to an information security policy may be granted in the following cases:

- The implicated system does not have the capacity to comply with the relevant security standard.
- Immediate compliance would disrupt critical business
- A more secure or superior solution exists
- Compliance would adversely affect business operations
- A lawsuit or investigation requires exception to the relevant security policy.
- Compliance would cause a major adverse financial loss
- An emergency situation requires violation of the relevant security policy.

### To Request an Exception:

Email or slack the [information security team](#) to request an exception. Your request must contain the following information:

- Your name
- The implicated policy.
- The device or application affected by the request.
- [Data classification](#) category of the associated systems.
- The rationale for non-compliance with the policy.
- Duration of non-compliance expected.
- Assessment of risks.
- Controls in place to mitigate risks.

### Example Exception Request

Steve would like to share Carl's Pizza Planet Account to order Pies for after-hour work events. This

violates our access control policy, which Steve is well-acquainted with, as he pays close attention during annual trainings. Steve's request might look like the following:

- Request: I would like share access to Carl's Pizza Planet online account.
- Policy: I'm attaching the access control policy:  
<https://wiki.nested-knowledge.com/doku.php?id=wiki:policies:access>
- Device/Application: Carl's account on the Pizza Planet web application, accessible at the website: <https://www.pizza-planet.org/portal>.
- Rationale: Pizza Planet only permits one account per each business credit card.
- Duration: Four - Six months.
- Risk: Passwords shared online may be intercepted, compromising Carl's account and our business credit card information.
- Mitigation: To limit risks, credentials will be shared face-to-face verbally. We will change the account password every 6-8 weeks.

## Revision History

Author	Date of Revision/Review	Comments/Description
K. Cowie	02/07/2023	Draft Completed

[Return to Policies](#)

From:  
<https://wiki.nested-knowledge.com/> - **Nested Knowledge**

Permanent link:  
<https://wiki.nested-knowledge.com/doku.php?id=wiki:policies:exception&rev=1675805566>

Last update: **2023/02/07 21:32**