# ISO 27001-Compliant 3rd Party Supplier Procedure Template

## Introduction

This 3rd Party Supplier Procedure aligns with ISO 27001 standards, providing a structured framework for managing relationships with third-party suppliers. Examples of third-party services include cloud hosting, data processing, IT support, and outsourced business operations. The procedure ensures that risks associated with third-party services are identified, assessed, and mitigated to protect the confidentiality, integrity, and availability of organizational information assets.

## Purpose

The purpose of this procedure is to define a systematic approach for managing third-party suppliers. This includes evaluating, onboarding, monitoring, and offboarding suppliers to ensure compliance with security requirements and mitigate potential risks to the organization.

## Scope

This procedure applies to all third-party suppliers that provide services, systems, or access to organizational information assets, including:

* IT service providers and software vendors
* Cloud service providers and data storage providers
* Consultants, contractors, and outsourced teams
* Suppliers with access to physical facilities or sensitive data

## Policy Statement

The organization is committed to managing third-party supplier relationships in alignment with ISO 27001 standards to ensure:

* Identification of risks associated with third-party services
* Assessment and approval of suppliers based on security criteria
* Documentation of agreements, including security and privacy clauses
* Continuous monitoring of supplier performance and compliance
* Secure offboarding of suppliers when contracts are terminated

The procedure includes the following six steps:

1. Supplier Identification: Identify suppliers that require access to information assets or provide critical services.
2. Risk Assessment: Conduct a risk assessment to evaluate potential risks posed by the supplier to the organization’s information security.
3. Contractual Agreements: Establish contracts that include security requirements, service-level agreements (SLAs), and compliance obligations.
4. Onboarding: Implement a structured onboarding process to ensure suppliers meet all security and compliance requirements.
5. Monitoring and Review: Regularly monitor supplier performance and compliance with contractual obligations through audits, reviews, and performance metrics.
6. Offboarding: Securely terminate relationships with suppliers, ensuring access is revoked and data is handled in compliance with organizational policies.

## Roles and Responsibilities

* Procurement Manager: Oversees the supplier selection process and ensures contractual agreements include security requirements.
* Information Security Officer: Conducts risk assessments and ensures alignment with ISO 27001 requirements.
* IT Operations Team: Implements technical controls to manage supplier access and monitor compliance.
* Department Heads: Ensure suppliers in their areas comply with organizational policies.
* Third-Party Suppliers: Adhere to agreed-upon security and compliance obligations.

## Compliance and Monitoring

Compliance with this procedure will be ensured through:

* Regular audits and reviews of supplier contracts and performance
* Implementation of key performance indicators (KPIs), such as:

- Percentage of suppliers with completed risk assessments

- Frequency of supplier compliance reviews

- Number of non-compliance incidents involving suppliers

Supplier compliance reviews will be documented using standardized audit reports, which include findings, corrective actions, and deadlines for resolution. In cases of non-compliance, a formal process will be initiated to address issues, including escalating concerns to senior management and reevaluating the supplier's suitability.

## Related Documentation

* Information Security Policy
* Vendor Risk Assessment Procedure
* Access Control Policy
* Incident Response Plan

## Review and Revision

This procedure will be reviewed annually or when significant changes occur in supplier relationships or regulatory requirements. The Procurement Manager will initiate the review process, and updates will be communicated to stakeholders through official channels. All updates will be documented and approved through a formal review process.

## Narrative Guidance

This procedure emphasizes the importance of managing third-party supplier relationships to ensure organizational security and compliance. It aligns with ISO 27001 principles of risk management, accountability, and continuous improvement. Organizations should adapt this template to address specific supplier risks and operational needs.

## Instructions for Use

* Replace placeholders with organization-specific details.
* Ensure alignment with related policies and standards.
* Collaborate with stakeholders to address unique risks associated with third-party suppliers.