# Third-Party Supplier Policy Template

## 1. Purpose

The purpose of this policy is to establish a framework for managing third-party suppliers to ensure they comply with [Organization Name]'s security, privacy, and operational standards. This policy aims to mitigate risks associated with third-party relationships and ensure alignment with ISO/IEC 27001:2022 requirements.

## 2. Scope

This policy applies to all third-party suppliers, contractors, vendors, and service providers engaged by [Organization Name]. It encompasses all services, products, and systems accessed or used by these parties in the course of their work with the organization.

## 3. Objectives

The objectives of this policy are to:  
- Ensure third-party compliance with applicable legal, regulatory, and contractual obligations.  
- Protect [Organization Name] information assets from unauthorized access, use, or disclosure.  
- Establish clear accountability for third-party actions and access.  
- Minimize the risk of supply chain disruptions.  
- Foster secure and transparent relationships with third-party suppliers.  
  
The organization will measure these objectives using key performance indicators (KPIs) such as the number of non-compliance incidents reported, supplier audit outcomes, and the resolution time for supplier-related issues.

## 4. Roles and Responsibilities

4.1 Procurement Team: Responsible for ensuring third-party agreements include necessary security and compliance clauses.  
4.2 Information Security Officer (ISO): Oversees the security assessments of third-party suppliers and ensures ongoing compliance.  
4.3 Third-Party Suppliers: Comply with all applicable policies, procedures, and contractual agreements.  
4.4 Relationship Managers: Act as primary points of contact for third-party suppliers and monitor their performance and compliance.  
4.5 Escalation Procedures: In cases of non-compliance or significant issues, a defined escalation path will be followed, involving the ISO, Relationship Managers, and senior management as necessary.

## 5. Third-Party Risk Management

[Organization Name] will:  
- Conduct due diligence and risk assessments for all third-party suppliers before engagement.  
- Categorize suppliers based on the criticality and sensitivity of their services or access to information.  
- Require high-risk suppliers to undergo periodic security assessments.  
- Establish criteria for termination of agreements in cases of non-compliance or significant risk.  
  
Examples of risks include data breaches, supply chain interruptions, regulatory violations, and unauthorized access to sensitive systems.

## 6. Security Requirements

All third-party suppliers must:  
- Adhere to [Organization Name]'s information security policies and standards.  
- Implement access controls to protect [Organization Name] assets.  
- Securely handle, store, and dispose of information assets according to contractual obligations.  
- Notify [Organization Name] promptly of any security breaches or incidents.  
- Use encryption and other technical safeguards for protecting sensitive data during transmission and storage.

## 7. Contractual Obligations

All agreements with third-party suppliers must include clauses that address:  
- Data protection and confidentiality.  
- Right-to-audit provisions to assess compliance.  
- Incident reporting timelines and procedures.  
- Responsibilities for regulatory compliance.  
- Termination conditions for breaches of policy or security incidents.  
- Liability and indemnification provisions to protect [Organization Name] in case of breaches or non-compliance by suppliers.

## 8. Monitoring and Auditing

[Organization Name] will:  
- Regularly monitor third-party compliance with security policies and contractual obligations.  
- Conduct audits or assessments based on the risk level associated with the supplier.  
- Maintain records of all audits and follow up on any findings or non-conformities.  
  
Audits will be conducted annually for high-risk suppliers, with specific criteria such as adherence to contractual security measures, incident management protocols, and data handling practices.

## 9. Training and Awareness

Third-party suppliers will receive training or guidelines on [Organization Name]'s security policies and procedures as necessary. Training sessions will be provided annually and tailored to the scope of each supplier's engagement with [Organization Name].

## 10. Incident Management

Third-party suppliers must report security incidents promptly to [Organization Name]. Incident response activities will be coordinated to minimize impact and prevent recurrence.  
  
Suppliers are required to report incidents within 24 hours of detection to ensure timely response and mitigation.

## 11. Continuous Improvement

The third-party supplier management process will be reviewed and improved periodically based on:  
- Audit findings.  
- Incident trends.  
- Changes in regulatory requirements or organizational priorities.  
- Feedback from suppliers to address challenges or suggest process enhancements.

## 12. Policy Review

This policy will be reviewed annually or when significant changes occur to ensure its relevance and effectiveness. Ad-hoc reviews will also be conducted following significant incidents or regulatory updates. The Information Security Officer (ISO) is responsible for overseeing the review.

## 13. Approval

Approved by: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
Title: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
Date: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_