# Vendor Risk Management Policy

Company Name: [Insert Company Name]

Effective Date: [Insert Effective Date]

Last Reviewed: [Insert Last Review Date]

Next Review Due: [Insert Next Review Date]

Version: 1.0

Contact for Questions: [Insert Contact Name, Title, Email, Phone]

## Table of Contents

1. Purpose
2. Scope
3. Policy Statement
4. Roles and Responsibilities
5. Vendor Classification
6. Risk Assessment and Due Diligence
7. Contractual Requirements
8. Ongoing Monitoring
9. Incident Response and Notification
10. Termination of Vendor Relationship
11. Documentation and Retention
12. Policy Review and Maintenance
13. Acknowledgment

## 1. Purpose

The purpose of this policy is to establish a structured and risk-based approach to managing third-party (vendor) relationships. It ensures that vendors who process, store, or transmit sensitive information or provide critical services to [Insert Company Name] are evaluated, monitored, and managed in a manner that mitigates risk to the organization.

## 2. Scope

This policy applies to all employees, contractors, departments, and business units of [Insert Company Name] who engage with or manage relationships with third-party vendors.

## 3. Policy Statement

[Insert Company Name] shall identify, assess, and manage risks associated with vendors that provide services, products, or access to organizational systems and data.

## 4. Roles and Responsibilities

Vendor Risk Manager / Compliance Officer:
- Oversees implementation of this policy.
- Approves vendor risk ratings and mitigation strategies.

Procurement / Purchasing Department:
- Ensures vendors are reviewed and approved per this policy before contract execution.

IT / Security Team:
- Assesses technical risks, system access, and data security controls.

Business Owners / Department Heads:
- Ensure ongoing monitoring of vendors within their function.

## 5. Vendor Classification

Vendors will be classified into the following tiers based on risk:
- Tier 1 – High Risk: Access to sensitive data or critical systems.
- Tier 2 – Moderate Risk: Handles non-sensitive but essential services.
- Tier 3 – Low Risk: Minimal to no data access or operational impact.

## 6. Risk Assessment and Due Diligence

Prior to engagement:
- A Vendor Risk Assessment must be completed for Tier 1 and Tier 2 vendors.
- Review of financial stability, legal history, security controls, and certifications (e.g., SOC 2, ISO 27001) is required.
- Data Protection Agreements (DPAs) must be signed if the vendor processes PII.

## 7. Contractual Requirements

All vendor contracts must include:
- Confidentiality and data protection clauses
- Right to audit and assess compliance
- Service Level Agreements (SLAs)
- Incident reporting timelines (e.g., within 24 hours of discovery)
- Termination rights for non-compliance

## 8. Ongoing Monitoring

High and moderate-risk vendors must be reviewed at least annually. Monitoring activities may include:
- Performance reviews
- Re-assessment of security controls
- Review of SOC reports or compliance attestations
- Vendor questionnaires

## 9. Incident Response and Notification

Vendors must notify [Insert Company Name] within [Insert Required Timeframe, e.g., 24 hours] of any security incident or data breach.
The [Insert Company Role, e.g., Compliance Officer] shall coordinate any response efforts and ensure appropriate escalation.

## 10. Termination of Vendor Relationship

Upon termination of a vendor relationship:
- All organizational data must be returned or securely destroyed
- System access must be revoked immediately
- An exit checklist must be completed and retained for audit purposes

## 11. Documentation and Retention

Vendor records, including risk assessments, contracts, monitoring reports, and offboarding documentation, must be retained for a minimum of [Insert Retention Period, e.g., 7 years] or as required by applicable regulations.

## 12. Policy Review and Maintenance

This policy shall be reviewed and updated at least annually or when significant changes to vendor management practices, regulations, or business processes occur.

## 13. Acknowledgment

I acknowledge that I have read, understand, and agree to comply with the Vendor Risk Management Policy.

Employee Name: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Signature: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Date: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_