**Vendor Risk Management Policy (VRMP)**

**Policy ID:** SEC-VRMP-001  
**Version:** 1.0  
**Approval Date:** [Insert Date]  
**Next Review Date:** [Insert Date + 12 months]  
**Owner:** Chief Information Security Officer (CISO) / Procurement Lead  
**Applies To:** All employees, business units, and third-party service providers engaged in sourcing, onboarding, or managing vendor relationships

**1. Purpose**

This policy establishes the requirements for identifying, assessing, and managing risks associated with third-party vendors. The objective is to protect [COMPANY NAME]’s systems, data, and operations from threats introduced by external parties.

**2. Scope**

This policy applies to all third-party relationships where vendors, suppliers, contractors, or service providers may access, process, transmit, or manage company data or systems. This includes:

* Cloud and SaaS providers
* Outsourced IT, support, or security services
* Consultants, contractors, and subcontractors
* Data hosting, analytics, and managed service partners

**3. Policy Statements**

**3.1 Vendor Risk Classification**

* All vendors must be risk-ranked based on the criticality of their services, access level, data sensitivity, and regulatory exposure. *(NIST SR-3; ISO 27001 A.5.19)*
* Risk levels (e.g., Low, Medium, High) must drive due diligence depth and review frequency. *(NIST PM-11; ISO 27001 A.5.20)*

**3.2 Due Diligence and Onboarding**

* Vendors must complete a formal security and privacy assessment before contract execution. *(NIST SA-12, SA-9; ISO 27001 A.5.20; GDPR Art. 28)*
* Due diligence may include reviewing SOC 2 reports, ISO 27001 certifications, or security questionnaires. *(NIST CA-2; ISO 27001 A.5.23)*
* All contracts must include data protection clauses, audit rights, breach notification obligations, and termination terms. *(NIST SA-4; ISO 27001 A.5.21; GDPR Art. 28(3); CCPA §1798.140(w))*

**3.3 Access and Data Controls**

* Vendors may only access systems or data necessary to deliver their contracted service (least privilege). *(NIST AC-6; ISO 27001 A.5.18)*
* All external access must use secure channels (e.g., VPN, MFA) and be logged and monitored. *(NIST AC-17, AU-2; ISO 27001 A.5.20)*
* Vendors must not use company data for any purpose outside the scope of the agreement. *(GDPR Art. 5(1)(b); CCPA §1798.105(c))*

**3.4 Ongoing Monitoring**

* High-risk vendors must be reviewed annually, with updated assessments and contract refreshes as needed. *(NIST SR-6; ISO 27001 A.5.20)*
* Vendors must notify [COMPANY NAME] of any security incident, control failure, or material business change within 72 hours. *(NIST IR-6; ISO 27001 A.5.25; GDPR Art. 33)*
* Vendor performance and compliance must be monitored using KPIs, SLAs, or third-party risk management tools. *(NIST CA-7; ISO 27001 A.5.23)*

**3.5 Offboarding and Contract Termination**

* Upon termination, vendor access must be revoked immediately and all company data must be returned or securely destroyed. *(NIST MP-6, AC-2(5); ISO 27001 A.8.11)*
* Recovery of hardware, credentials, encryption keys, and confidential information must be documented and confirmed. *(NIST PE-3; ISO 27001 A.8.10)*

**4. Roles and Responsibilities**

|  |  |
| --- | --- |
| **Procurement** | Initiates vendor onboarding, ensures required assessments and contracts are in place. |
| **Business Units** | Define vendor requirements, ensure alignment with functional and compliance goals. |
| **Security/GRC Team** | Conducts vendor risk assessments and manages technical/contractual controls. |
| **Legal/Compliance** | Reviews vendor agreements and ensures regulatory clauses meet requirements. |
| **IT Operations** | Implements and monitors secure technical access for vendor accounts or integrations. |

**5. Compliance and Enforcement**

Failure to follow this policy may expose the organization to data breaches, compliance violations, or operational disruption. Violations may result in internal disciplinary action, vendor contract suspension, or termination.

**6. Review and Maintenance**

The CISO and Procurement Lead shall review this policy annually or after significant changes in the vendor ecosystem, regulatory landscape, or business operations. All updates must be approved by executive leadership.

**7. Acknowledgment and Agreement**

I acknowledge that I have read, understand, and agree to comply with [COMPANY NAME]’s Vendor Risk Management Policy. I commit to managing third-party risks in accordance with the procedures and responsibilities described.

|  |  |  |
| --- | --- | --- |
| **Name (Print):**  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | **Signature:** \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | **Date:** \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |