Supply Chain Risk Management Plan (SCRM)

This plan outlines the organization's strategy for identifying, assessing, and mitigating risks associated with external providers and the supply chain for information systems, software, and services.

1. Scope and Policy Objectives

This plan applies to all **vendors, suppliers, service providers, and partners** that develop, integrate, deliver, or support the organization's critical information systems, processing facilities, or sensitive data.

Objectives:

- To identify and categorize risks introduced by external entities.
- To establish minimum security requirements for all suppliers.
- To ensure the confidentiality, integrity, and availability of our systems are not compromised by supply chain vulnerabilities.

2. Risk Assessment and Due Diligence

2.1. Supplier Tiers and Criticality

Suppliers are categorized into tiers based on the level of risk they introduce to the organization's operations and data:

Tier	Access and Impact	Security Due Diligence Required
Tier 1 (Critical)	Direct, privileged access to production systems or handle highly sensitive/confidential data (e.g., Cloud IaaS/SaaS providers, core application developers).	Mandatory annual security audit, SOC 2 Type 2 or ISO 27001 certification, contractually required right-to-audit.

Tier	Access and Impact	Security Due Diligence Required
Tier 2 (High)	Limited system access or handle non-critical but sensitive data (e.g., HR platforms, non-critical software vendors).	Annual security questionnaire, review of security policies and controls.
Tier 3 (Standard)	No access to organizational systems or data (e.g., office supply vendors, facility maintenance).	Basic contractual requirements for confidentiality.

2.2. Pre-Contract Due Diligence

Before contracting with any Tier 1 or Tier 2 supplier, a formal risk assessment is conducted, including:

1. **Security Questionnaire:** Assessing the supplier's security posture, including physical security, personnel screening, patch management, and incident response capabilities.
2. **Certification Review:** Verification of relevant security certifications (e.g., ISO 27001, SOC 2, FedRAMP).
3. **Vulnerability Review:** For software suppliers, a review of known vulnerabilities in their product and the effectiveness of their Patch Management Program.

3. Contractual Requirements and Control

3.1. Contractual Obligations

All formal agreements with suppliers must include mandatory security clauses that hold the supplier accountable for maintaining agreed-upon security controls. These clauses must address:

- **Data Protection:** Requirements for data segregation, encryption, and regulatory compliance (e.g., GDPR, HIPAA).
- **Security Incidents:** Mandatory notification requirements and timelines in the event of a security breach involving the organization's data or systems.

- **Right-to-Audit:** The right for the organization to conduct or commission independent security audits/penetration tests on the supplier's environment (particularly for Tier 1).

3.2. Software Supply Chain Integrity (SSCI)

For all procured or developed software:

- **Source Code Review:** Critical third-party libraries and open-source components are subject to review to prevent known vulnerabilities.
- **Approved Sources:** All software and hardware components must be sourced directly from the manufacturer or an approved, trusted distributor.

4. Monitoring and Off-boarding

4.1. Continuous Monitoring

Compliance for Tier 1 and Tier 2 suppliers is monitored continuously through:

- **Annual Reassessment:** Suppliers undergo a security re-assessment (questionnaire and/or audit) at least annually.
- **Vulnerability Tracking:** Monitoring for public announcements of vulnerabilities related to the products and services provided by critical suppliers.

4.2. Off-Boarding

When a relationship with a supplier ends, a formal off-boarding process is executed to mitigate residual risk:

- **Access Revocation:** All logical and physical access provided to the supplier (accounts, VPNs, physical badges) is immediately and permanently revoked.
- **Data Sanitization:** The supplier must provide certification that all organizational data stored on their systems has been securely sanitized or returned, as defined by the contract.