Vendor Management Policy (Supply Chain Security)

- **Purpose:** This policy establishes the framework for identifying, assessing, mitigating, and monitoring risks arising from the World Bank's reliance on third-party vendors, suppliers, and service providers. The objective is to ensure the security, integrity, and resilience of the Bank's supply chain, protecting WDB's information assets, operations, and reputation from vendor-related threats.
- **Scope:** This policy applies to all third-party relationships where the vendor:
  - Accesses, processes, stores, or transmits WDB information, particularly sensitive or classified data.
  - Provides critical products, software, or services that support WDB's operations.
  - Connects to WDB's networks or systems.
  - Represents WDB or acts on its behalf in a manner that could impact the Bank's security or reputation.
- **Cybersecurity Supply Chain Risk Management (C-SCRM) Program:** The WDB maintains an enterprise-wide C-SCRM program, potentially coordinated by a C-SCRM Program Management Office (PMO). This policy forms a key component of that program, emphasizing a proactive and resiliency-focused approach rather than a purely reactive one. The aim is to prevent supply chain compromises by integrating security throughout the vendor lifecycle.
- **Roles and Responsibilities:**
  - **Business Unit/Requestor:** Identifies the need for a vendor service/product, provides business context for risk assessment, and acts as the primary relationship owner.
  - **Procurement Department:** Manages the vendor selection and contracting process, ensuring compliance with this policy.
  - **Legal Department:** Reviews and approves contractual terms, including security and data protection clauses.
  - **CISO Team/Cybersecurity Department:** Conducts security risk assessments of vendors, defines security requirements, and monitors vendor compliance.
  - **Data Protection Officer (DPO):** Assesses data protection risks and ensures appropriate data processing agreements (DPAs) are in place for vendors handling personal data.
  - **C-SCRM PMO (if established):** Coordinates C-SCRM activities, maintains vendor risk profiles, and provides guidance.

Vendor Lifecycle Management

Security considerations are integrated into each phase of the vendor relationship:

1. **Planning and Due Diligence:**

- Before engaging a vendor, a risk assessment of the proposed service or product is conducted to determine the potential security impact.
- Potential vendors undergo an initial security assessment, which may include questionnaires, review of certifications (e.g., ISO 27001, SOC 2), and independent security ratings. The depth of due diligence is proportionate to the risk level associated with the vendor and the service.
- Understanding sub-tier supplier risks, where feasible and relevant, is part of this process.

2. **Contracting:**

- Contracts with vendors must include specific cybersecurity requirements, such as adherence to WDB security policies, data protection obligations, and relevant industry standards.
- Clauses granting WDB the right to audit the vendor's security controls (or receive third-party audit reports).
- Clear Service Level Agreements (SLAs) for security performance, availability, and incident response.
- Mandatory incident notification requirements, specifying timelines and procedures for reporting security breaches affecting WDB data or services.
- Data Processing Agreements (DPAs) for vendors processing personal data on behalf of WDB.
- Confidentiality and intellectual property protection clauses.

3. **Onboarding:**

- Secure integration of vendor services or products into WDB's environment.
- Configuration of access controls based on the principle of least privilege.
- Security testing of integrations before go-live.

4. **Ongoing Monitoring:**

- Periodic security risk assessments of vendors, with frequency based on their risk tier (e.g., annual for high-risk, biennial for medium-risk).
- Continuous monitoring of the vendor's security posture through threat intelligence, vulnerability disclosures, and public security ratings.

- Review of vendor performance against contractual security SLAs.
- Tracking and managing vulnerabilities identified in vendor products or services used by WDB.

5. **Termination/Offboarding:**

- Formal procedures for terminating vendor relationships.
- Secure return or destruction of WDB data held by the vendor, with certification of destruction where required.
- Revocation of all vendor access to WDB systems, data, and facilities.
- Final review to ensure all contractual obligations have been met.

Vendor Risk Assessment Methodology

WDB employs a risk-based methodology to classify vendors into tiers (e.g., **Critical, High, Medium, Low**) based on factors such as the criticality of the service provided, the sensitivity of data accessed, the level of integration with WDB systems, and the vendor's inherent security posture.

The risk tier determines the level of due diligence, contractual scrutiny, and ongoing monitoring required.

- **Security Requirements for Vendors:**
  - WDB maintains a baseline set of security controls expected from all vendors. These may be augmented with more stringent requirements for higher-risk vendors. Examples include:
    - Strong access control mechanisms.
    - Data encryption at rest and in transit for sensitive information.
    - Robust vulnerability management programs.
    - Documented incident response capabilities.
    - Security awareness training for vendor personnel handling WDB data.
    - Secure software development practices (for software vendors).
- **Incident Response Collaboration:** Procedures are established for managing security incidents that involve or originate from a vendor, ensuring coordinated response and communication between WDB and the vendor.

- **Anti-Counterfeit Measures:** For procurement of critical hardware or software where counterfeit products pose a risk, WDB implements measures to verify authenticity and supply chain integrity, where applicable.