

# World Bank Policy on Vendor Contract and SLA Security Requirements

## Preamble

This policy document outlines the non-negotiable security standards and service level expectations World Bank mandates for all third-party vendor engagements, particularly those involving access to bank data or systems, including cloud service providers. Its implementation has been crucial in establishing a clear baseline for vendor accountability and mitigating risks associated with outsourced services. The proactive establishment of such a policy, rather than relying on ad-hoc contract negotiations, signifies a mature risk management approach within World Bank. This approach shifts the burden of initial compliance onto vendors, ensuring a consistent security baseline across all engagements and streamlining the procurement and legal review processes by pre-defining the bank's security expectations.

## Section 1: Purpose and Scope

The purpose of this policy is to protect World Bank's information assets, ensure compliance with applicable legal and regulatory requirements, and maintain operational resilience by establishing minimum cybersecurity and service level requirements for all vendor contracts. This policy applies to all new and renewing contracts with vendors, suppliers, and service providers, with a particular emphasis on cloud service providers (CSPs), that process, store, transmit, or access World Bank data or connect to World Bank networks. Financial institutions must establish strong contractual agreements with vendors, and this policy serves as the foundation for those agreements. The consistent application of these standards is fundamental to World Bank's strategy for managing vendor-related risks.

## Section 2: Mandatory Cybersecurity Clauses in Vendor Contracts

All vendor contracts falling within the scope of this policy must include the following cybersecurity clauses. These clauses are foundational elements of a robust security strategy, designed to mitigate vendor-related cybersecurity risks and establish clear liability. The comprehensiveness of these clauses reflects a "defense-in-depth" strategy extended to the supply chain, signifying a commitment to building resilience by contractually embedding security into vendor operations. This level of contractual rigor necessitates dedicated internal resources for monitoring and enforcement, reflecting the bank's investment in a higher assurance level.

The following table summarizes the standard cybersecurity clauses required by World Bank:

**Table 1: World Bank Standard Cybersecurity Clauses for Vendor Contracts**

Clause Title	Brief Description	World Bank Standard/Requirement Example	Rationale/Risk Mitigated
1. Data Security Requirements	Specifies security standards and controls for data lifecycle protection.	Vendor shall encrypt all World Bank Data at rest using AES-256 bit encryption and in transit using TLS 1.2 or higher. Access to World Bank Data shall be restricted based on the principle of least privilege and require multi-factor authentication for all administrative access. Vulnerability scans must be performed at least quarterly, with critical vulnerabilities patched within 48 hours of discovery.	Protects data confidentiality, integrity, and availability; reduces risk of unauthorized access and data exposure.
2. Data Breach Notification	Mandates prompt notification of security incidents affecting World Bank data or services.	Vendor shall notify World Bank of any suspected or confirmed Security Incident affecting World Bank Data or services within two (2) hours of discovery, providing full details (scope, impact, affected data, root cause analysis, remediation steps) via the designated World Bank Incident Response portal.	Enables timely response to breaches, minimizing impact and facilitating regulatory compliance.
3. Audit Rights	Grants World Bank the right to audit vendor's security practices and compliance.	World Bank reserves the right, upon reasonable notice (minimum 30 days for routine audits, shorter for incident-triggered audits), to conduct, or have a third-party conduct on its behalf, an audit of Vendor's security controls, policies, and procedures relevant to the Services provided, at least annually for high-risk vendors or in the event of a Security Incident. Vendor must provide access to relevant records, personnel, and facilities (physical or virtual).	Verifies vendor compliance with contractual and regulatory obligations; identifies security weaknesses.
4. Compliance with Laws and Regulations	Requires vendor to comply with all applicable laws, regulations, and industry standards.	Vendor warrants compliance with all applicable data protection laws, including but not limited to GDPR, CCPA, DORA, and relevant financial regulations such as GLBA, for all World Bank Data processed. Evidence of compliance must be provided upon request.	Ensures vendor operations meet legal and regulatory mandates, protecting World Bank from associated liabilities.
5. Indemnification	Establishes vendor liability for losses due to security breaches caused by vendor negligence or failure to meet contractual obligations.	Vendor shall indemnify, defend, and hold harmless World Bank from any claims, damages, losses, regulatory fines, and expenses (including legal fees) arising from Vendor's breach of its data security or confidentiality obligations under this Agreement.	Protects World Bank from financial and reputational damage resulting from vendor-caused breaches.
6. Security Certifications	Requires vendors handling sensitive data or providing critical services to maintain relevant security certifications.	For services involving PII or critical financial data, Vendor must maintain and provide evidence of a valid SOC 2 Type II certification and ISO 27001 certification annually.	Provides independent assurance of vendor's security controls and practices.
7. Business Continuity and Disaster Recovery (BCDR)	Requires vendor to have and regularly test a BCDR plan, specifying RTOs/RPOs acceptable to World Bank.	Vendor shall maintain a BCDR plan ensuring an RTO of no more than 4 hours and an RPO of no more than 1 hour for critical services provided to World Bank. The plan must be tested at least annually, with full test results and any remediation plans shared with World Bank within 30 days of test completion.	Ensures continuity of critical services in case of disruption at the vendor; minimizes data loss.

8. Data Residency and Sovereignty	Specifies permissible geographic locations for data storage and processing, requiring notification and approval for changes.	All World Bank customer data shall be stored and processed exclusively within [Approved Jurisdiction(s), e.g., European Economic Area for EU customer data] unless explicitly approved in writing by World Bank's Chief Information Security Officer. Vendor must notify World Bank 90 days in advance of any proposed changes to data storage or processing locations.	Ensures compliance with data sovereignty laws and regulatory expectations; manages geopolitical risks.
9. Subcontractor (Fourth-Party) Management	Requires vendor to notify World Bank of any subcontractors handling bank data and ensure subcontractors comply with the same security requirements.	Vendor shall not subcontract any services involving access to World Bank Data without prior written consent from World Bank and shall ensure all approved subcontractors contractually adhere to terms no less stringent than those in this Agreement. Vendor remains fully liable for the acts and omissions of its subcontractors.	Extends security protections to the extended supply chain; addresses nth-party risks.
10. Incident Response Obligations & Coordination	Details vendor's role in incident response beyond notification, including cooperation and forensic support.	Upon a Security Incident, Vendor shall cooperate fully with World Bank's incident response team, including providing access to logs, personnel, and systems for investigation, preserving evidence, and shall take immediate steps to contain and remediate the incident as directed by World Bank or in accordance with an agreed-upon plan.	Facilitates effective and coordinated response to security incidents, minimizing damage and recovery time.
11. Data Deletion/Return upon Termination	Mandates secure deletion or return of all World Bank data upon contract termination, with certification of destruction.	Within 30 days of contract termination, Vendor shall securely delete (using methods such as NIST SP 800-88 compliant sanitization) or return all World Bank Data in its possession and in the possession of its subcontractors, and provide a written certification of destruction signed by an authorized officer.	Prevents unauthorized retention or use of World Bank data after contract end; ensures data privacy.
12. Right to Inspect and Test Security	Grants World Bank the right to perform penetration testing and vulnerability assessments on vendor systems directly supporting World Bank services.	World Bank may, with 7 days prior notice and in coordination with Vendor to minimize operational disruption, conduct vulnerability scans and penetration tests on Vendor systems directly processing or storing World Bank critical data. Results will be shared with Vendor, and Vendor must remediate identified critical and high vulnerabilities within agreed timelines (e.g., critical within 30 days, high within 90 days).	Provides proactive assurance of vendor security posture beyond audits; verifies effectiveness of controls.

### Section 3: Minimum SLA Requirements for Cloud Service Providers

For Cloud Service Providers (CSPs), specific Service Level Agreements (SLAs) are critical to ensure the performance, availability, and security of services upon which World Bank relies. Defining granular SLA metrics demonstrates an understanding that cloud services require quantifiable performance and security commitments, essential for operational stability and customer trust. These metrics are vital where downtime or data loss can have severe financial and reputational consequences. Holding CSPs to these standards necessitates robust monitoring capabilities.

**Table 2: World Bank Standard SLA Metrics for Critical Cloud Services**

Metric	World Bank Target	Monitoring Method Example	Consequence of Breach Example	Responsible WB Team for Monitoring
1. Availability/Uptime Commitments	Critical online banking services: ≥99.99% monthly uptime. Internal core systems: ≥99.95% monthly uptime. Uptime calculation methodology to be mutually agreed, excluding pre-approved scheduled maintenance (max 4 hours/month, notified 7 days in advance).	CSP Portal Dashboard, Third-Party Synthetic Monitoring Tool (e.g., Dynatrace, New Relic), Internal Monitoring Probes.	Tiered service credits: e.g., 10% of monthly fee for uptime between 99.9% and 99.99%; 25% for uptime between 99.5% and 99.9%. Root Cause Analysis (RCA) required for any breach.	IT Operations, Application Support Teams.
2. Mean Time to Recovery (MTTR)	Payment processing systems: MTTR <30 minutes. Core banking database services: MTTR <1 hour. Other critical services: MTTR <4 hours.	CSP Incident Reports, Internal Incident Management System Timestamps.	Escalating penalties for exceeding MTTR targets. Mandatory RCA and corrective action plan for repeated failures.	IT Operations, Incident Management Team.
3. Latency and Performance Standards	Customer-facing API responses: <200ms at 95th percentile. Batch processing completion windows: As defined per service (e.g., end-of-day processing completed by 2 AM local time).	Application Performance Monitoring (APM) tools, CSP performance metrics.	Service credits if performance consistently falls below agreed thresholds. Joint performance review if degradation persists.	Application Development, IT Operations.
4. Data Durability/Recovery Point Objective (RPO)	Core banking database RPO: <5 minutes. Customer document storage RPO: <15 minutes. Data Durability: ≥99.99999999% (eleven 9s) for object storage.	CSP Backup Logs, Regular Restore Tests (at least quarterly for critical data).	Significant financial penalties for data loss. Immediate notification and joint investigation for any data loss event.	Data Management Team, IT Operations.
5. Security Incident Response Time (from CSP)	CSP notification of security events impacting World Bank tenant/environment: within 1 hour of CSP detection. Provision of initial impact assessment: within 4 hours of notification.	CSP Security Notifications, SIEM alerts.	Contractual penalties for delayed notification. Right to conduct independent investigation.	Cybersecurity Operations Center (CSOC), Incident Response Team.
6. Patch Management Timelines (for CSP-managed components)	CSP to patch critical vulnerabilities (CVSS 9.0-10.0) in underlying IaaS/PaaS infrastructure within 72 hours of patch availability or vendor disclosure. High vulnerabilities (CVSS 7.0-8.9) within 7 days.	CSP Advisories, Vulnerability Scan Reports (where applicable to CSP infrastructure).	Right to request immediate remediation or risk mitigation plan. Potential for service suspension if critical patches are consistently missed.	Cybersecurity Risk Management, IT Operations.

## Section 4: Contract Review and Approval Process

To ensure compliance with this policy, all vendor contracts must undergo a formalized, multi-stakeholder review process. This structured approach ensures that vendor security is not solely an IT or security concern but a business-wide responsibility, reducing the risk of signing contracts with unacceptable security terms or SLAs.

The internal process for reviewing and approving vendor contracts includes the following minimum steps:

1. **Initial Review by Procurement and Business Unit:** The sponsoring Business Unit, in conjunction with Procurement, conducts an initial review for commercial viability, alignment with business needs, and ensures World Bank's standard security addendum (derived from this policy) is included in the draft contract.
2. **Detailed Cybersecurity and Technical Review:** The Cybersecurity team, along with relevant IT SME's (Subject Matter Experts), performs a thorough review of the proposed contract against the mandatory clauses and SLA requirements detailed in this policy. They assess the vendor's responses to security questionnaires and any VRA findings. Any deviations or gaps must be identified, and risk acceptance or remediation requirements documented.
3. **Legal and Final Business Owner Approval:** The Legal department reviews the contract for legal soundness, enforceability of security clauses, and overall risk allocation. The final contract, incorporating all feedback and required amendments, must be approved by the authorized Business Owner and, for high-risk contracts, by a designated executive (e.g., CISO, CRO, or relevant committee).

## **Section 5: Monitoring and Enforcement**

Contractual clauses and SLAs are effective only if monitored and enforced. World Bank is committed to ongoing oversight of vendor compliance. This requires continuous effort and resources, and a willingness to hold vendors accountable, which may include remediation plans, invoking penalties, or, in severe cases, contract termination. This active management is crucial for maintaining the intended security posture.

Monitoring and enforcement activities include:

1. **Regular Performance Reviews:** Quarterly reviews of vendor performance against agreed SLAs for all critical and high-risk vendors, utilizing reports from CSPs and internal monitoring tools. These reviews will be documented, and any deviations discussed with the vendor.
2. **Annual Documentation Review:** Annual collection and review of updated SOC 2 reports, ISO 27001 certificates, penetration test summaries, BCDR test results, and insurance certificates from critical and high-risk vendors.
3. **Formal Non-Compliance Process:** A documented process for issuing formal notices of non-compliance or SLA breach to vendors. This includes requiring the vendor to submit a corrective action plan (CAP) with defined timelines, and World Bank tracking these CAPs to completion. Failure to remediate may result in penalties, service credits as defined in the contract, or initiation of contract termination procedures.

- 4. **Periodic Audits:** Exercising contractual audit rights based on vendor risk tier and specific triggers (e.g., post-incident, significant change in vendor environment). Audits will verify compliance with contractual security obligations.

**Appendix A: Sample Cybersecurity Clause Template**

*(This appendix would contain template language for a key clause, e.g., Data Breach Notification, incorporating World Bank's specific requirements.)*

**Appendix B: Sample Cloud SLA Metrics Table**

*(This appendix would provide a more detailed table summarizing minimum SLA targets for different categories of cloud services, expanding on Table 2.)*