Appendix B:
Vendor / Third-Party Security Requirements Addendum

This Vendor / Third-Party Security Requirements Addendum (the **"Addendum"**) is incorporated into and forms part of the agreement between **[Company Legal Name]** ("**Company**") and **[Vendor Legal Name]** ("**Vendor**") (the **"Agreement"**). In the event of a conflict between this Addendum and the Agreement, the more protective requirement for Company Data, Company Systems, and the security of services shall govern unless applicable law expressly requires otherwise.

1. Purpose and Scope

1.1 This Addendum establishes minimum information security, cybersecurity, privacy, resilience, and supply-chain risk management requirements applicable to any products, services, software, systems, personnel, facilities, or subcontractors used by Vendor to provide goods or services to Company.

1.2 This Addendum applies to Vendor to the extent Vendor:

- accesses, stores, processes, transmits, hosts, receives, or otherwise handles Company Data;
- connects to, integrates with, or otherwise has access to Company Systems;
- develops, supports, maintains, or provides software, SaaS, hosted services, infrastructure, consulting, managed services, professional services, or other technology-enabled services for Company; or
- relies upon subcontractors, subprocessors, cloud providers, or other fourth parties in performance of the Agreement.

1.3 Vendor shall implement and maintain administrative, technical, physical, and organizational safeguards appropriate to the sensitivity of the data involved, the criticality of the service, and the risks presented by the processing and service delivery activities.

2. Definitions

For purposes of this Addendum:

2.1 "Company Data" means all information or data provided by or on behalf of Company to Vendor, accessed by Vendor on Company's behalf, or created, received, maintained, processed, transmitted, or derived by Vendor in connection with the Agreement, including metadata, output, logs, reports, and backups containing such data.

2.2 "Company Systems" means Company networks, endpoints, software, applications, cloud environments, operational technology environments, collaboration platforms, email systems, interfaces, APIs, and any other information systems owned, leased, operated, or controlled by Company.

2.3 "Security Incident" means any actual, suspected, or reasonably likely unauthorized access to, acquisition of, disclosure of, alteration of, destruction of, corruption of, loss of control over, or unavailability of Company Data or Company Systems, or any material compromise of Vendor systems that could affect the confidentiality, integrity, availability, or resilience of Company Data, Company Systems, or the services.

2.4 "Subprocessor" or **"Subcontractor"** means any third party engaged by Vendor that stores, processes, transmits, hosts, supports, or can access Company Data or materially supports services provided under the Agreement.

2.5 "Applicable Law" means all laws, regulations, binding regulatory requirements, and legally enforceable industry obligations applicable to Vendor's performance under the Agreement.

3. Information Security Program and Governance

3.1 Vendor shall maintain a documented, risk-based information security program appropriate to its size, complexity, service offerings, and the sensitivity and criticality of the data and services involved.

3.2 Vendor's information security program shall include, at a minimum:

- documented policies and procedures;

- assigned security roles and responsibilities;
- periodic risk assessments;
- asset and data management processes;
- access control standards;
- vulnerability and patch management;
- logging and monitoring;
- incident response;
- business continuity and disaster recovery;
- supplier and fourth-party risk management;
- secure systems and software practices where applicable; and
- periodic review and continuous improvement.

3.3 Vendor shall have executive accountability for cybersecurity and, upon request, shall identify the person or function responsible for information security governance.

3.4 Vendor shall review its security program no less than annually and after any material change to its systems, services, risk posture, or threat environment.

4. Compliance, Risk Assessment, and Assurance

4.1 Vendor shall comply with Applicable Law and with any security requirements expressly stated in the Agreement, statement of work, security exhibit, or written Company requirements.

4.2 Vendor shall perform periodic security and privacy risk assessments appropriate to the services provided and shall promptly address material findings through documented remediation plans.

4.3 Upon reasonable request, Vendor shall provide Company with current evidence of Vendor's security posture, which may include one or more of the following, as applicable:

- SOC 2 Type II report;
- ISO/IEC 27001 certification;
- independent security assessment or attestation;
- Shared Assessments SIG or equivalent questionnaire responses;
- summaries of penetration testing results;
- vulnerability management summaries;

- incident response and business continuity test summaries; and
- relevant policies, standards, or evidence reasonably necessary to assess risks related to the services.

4.4 If Vendor is unable to provide one of the foregoing artifacts, Vendor shall provide alternative evidence reasonably acceptable to Company.

5. Personnel Security and Workforce Management

5.1 Vendor shall ensure that personnel with access to Company Data or Company Systems are authorized, appropriately trained, and bound by written confidentiality obligations no less protective than those in the Agreement.

5.2 Vendor shall implement personnel security practices appropriate to the risk of the services, including onboarding, transfer, and termination controls; revocation of access upon separation or role change; and security awareness and role-based training.

5.3 Where permitted by law and appropriate to the role, Vendor shall conduct background checks on personnel with privileged access or access to sensitive Company Data.

5.4 Vendor shall ensure that Vendor personnel use unique accounts and that shared accounts are prohibited except where technically necessary, strictly controlled, and auditable.

6. Asset Management, Configuration Management, and Change Control

6.1 Vendor shall maintain an inventory of systems, software, service components, cloud resources, and dependencies used to deliver the services or process Company Data.

6.2 Vendor shall establish and maintain secure baseline configurations, hardening standards, and change management procedures for relevant systems and software.

6.3 Vendor shall implement processes to identify unauthorized or unsupported assets and software and promptly remove, isolate, replace, or remediate them.

6.4 Vendor shall not use end-of-life or unsupported software or hardware in providing the services where such use creates unreasonable risk to Company Data,

Company Systems, or service delivery. If temporary use is unavoidable, Vendor shall document compensating controls and obtain Company's prior written approval if the affected component materially supports the services.

6.5 Vendor shall notify Company in advance, where practicable, of material changes to architecture, hosting, major subprocessor dependencies, identity architecture, or service delivery models that may materially affect security, privacy, resilience, or compliance.

7. Identity and Access Management

7.1 Vendor shall implement identity and access controls based on least privilege, need-to-know, role-based access, separation of duties where appropriate, and periodic access review.

7.2 Vendor shall require multi-factor authentication for:

- all administrative or privileged accounts;
- remote access to Vendor environments used to support the services;
- access to Company Systems;
- access to Company Data in hosted or administrative contexts; and
- all internet-accessible management interfaces.

7.3 Vendor shall promptly disable or remove accounts that are no longer required and shall review privileged access no less than quarterly.

7.4 Vendor shall manage service accounts, API keys, secrets, certificates, and tokens securely, including inventory, rotation, access restrictions, and protection against unauthorized disclosure.

7.5 Vendor shall use strong authentication and password controls consistent with industry standards and shall prohibit use of default credentials in production environments.

8. Data Classification, Use, Protection, and Privacy

8.1 Vendor shall use Company Data solely for the purpose of performing the Agreement and for no other purpose unless expressly authorized in writing by Company.

8.2 Vendor shall not:

- sell Company Data;
- share Company Data except as necessary to perform the Agreement and only with approved Subprocessors bound by equivalent obligations;
- mine, profile, de-identify, aggregate, train models on, or otherwise derive value from Company Data for Vendor's own benefit, product improvement, model training, advertising, analytics unrelated to the services, or any other secondary purpose, except as expressly authorized in writing by Company; or
- combine Company Data with other customer data, except to the limited extent necessary to provide the contracted services, and only with adequate segregation and access controls.

8.3 Vendor shall classify and protect Company Data in accordance with its sensitivity and any classification, handling, or written instructions provided by Company.

8.4 Vendor shall maintain appropriate data flow, retention, minimization, segregation, deletion, masking, and disposal practices.

8.5 Vendor shall comply with all agreed privacy, confidentiality, data protection, and cross-border transfer requirements applicable to the services.

8.6 Vendor shall promptly notify Company if Vendor determines that any Company instruction conflicts with Applicable Law.

8.7 In the event that the Vendor, pursuant to applicable law or regulation or legal process, is requested or required to disclose Company Data, the Vendor shall provide the Company with prompt notice of such requirement in order to enable the Vendor to confer with the Company concerning the steps that may be taken to reduce the extent of Company Data that must be disclosed and/or to enable the Company to seek an appropriate protective order or other remedy reducing the extent of Company Data that must be disclosed. In any event, the Vendor shall disclose only such Company Data that the Vendor is advised by legal counsel is legally required to be disclosed in order to comply with such applicable law or regulation or legal process (as such may be affected by any protective order or other remedy obtained by the Company) and shall use reasonable efforts to ensure that all Company Data is so disclosed will be accorded confidential treatment.

9. Encryption and Key Management

9.1 Vendor shall encrypt Company Data in transit over public or untrusted networks using strong, industry-standard cryptographic protocols.

9.2 Vendor shall encrypt Company Data at rest where such data is stored on servers, databases, backups, portable media, or other storage media, except where Company has expressly approved an alternative in writing.

9.3 Vendor shall protect cryptographic keys using industry-standard key management practices, including logical separation of duties where feasible, controlled access, rotation, secure storage, and revocation procedures.

9.4 Vendor shall not store Company Data in plaintext in logs, debug traces, or support artifacts except where strictly necessary and appropriately protected.

10. Logging, Monitoring, Detection, and Record Retention

10.1 Vendor shall generate and maintain audit logs for security-relevant events associated with systems used to provide the services, including, as applicable:

- authentication events;
- privileged access;
- account creation, modification, and deletion;
- administrative actions;
- data access and export activity for sensitive data;
- configuration changes;
- security tool alerts;
- system failures and recovery events; and
- access to production environments.

10.2 Logs shall be protected from unauthorized access, alteration, and deletion and retained for a minimum of **12 months**, with no less than **90 days** readily available online, unless a different period is required by Applicable Law or the Agreement.

10.3 Vendor shall maintain capabilities to detect anomalous, unauthorized, or malicious activity affecting the services or Company Data and shall investigate alerts in a timely manner.

10.4 Upon reasonable request related to an actual or suspected Security Incident, Vendor shall preserve and provide relevant logs and records to Company, subject to legal restrictions.

11. Vulnerability Management, Patching, and Security Testing

11.1 Vendor shall maintain a documented vulnerability management program that includes asset coverage, authenticated or otherwise effective scanning as appropriate, severity evaluation, remediation tracking, exception handling, and retesting.

11.2 Vendor shall monitor authoritative vulnerability and threat intelligence sources relevant to the technologies used in the services and evaluate exposure in a timely manner.

11.3 Vendor shall remediate vulnerabilities according to risk and exploitability, including, unless Company approves otherwise in writing:

- **Critical vulnerabilities**: as soon as practicable, and in no event later than **15 calendar days** from identification or vendor advisory, and more quickly where evidence of active exploitation exists;
- High vulnerabilities: within 30 calendar days;
- Medium vulnerabilities: within 90 calendar days.

11.4 Where remediation cannot be completed within the above timeframes, Vendor shall document the reason, apply compensating controls, assess residual risk, define a revised remediation target date, and provide such information to Company upon request.

11.5 Vendor shall conduct periodic security testing of relevant environments and services, including internal testing and, where appropriate to the service, independent penetration testing no less than annually and after material changes.

11.6 Upon request and subject to confidentiality protections, Vendor shall provide Company with an executive summary of the most recent penetration test and status of remediation for material findings.

12. Secure Development and Application Security

If Vendor develops, customizes, maintains, hosts, or provides software, applications, APIs, integrations, or SaaS for Company, the following apply:

12.1 Vendor shall maintain a documented secure development lifecycle that includes security requirements, design review, threat modeling appropriate to the risk, secure coding practices, testing, release controls, and vulnerability remediation.

12.2 Vendor shall use commercially reasonable measures to prevent introduction of malicious code, insecure dependencies, tampered components, or unauthorized changes into software or build pipelines.

12.3 Vendor shall perform security testing appropriate to the application risk profile, which may include static analysis, dynamic analysis, software composition analysis, secrets scanning, dependency and container scanning, and manual review or penetration testing.

12.4 Vendor shall maintain an inventory of software components and dependencies materially used in the services and, upon reasonable request for higher-risk software or hosted services, provide a software bill of materials or equivalent dependency inventory.

12.5 Vendor shall have a vulnerability disclosure or coordinated vulnerability intake process for security reports affecting the services.

12.6 Vendor shall not deploy to production any application component known to contain unresolved critical vulnerabilities unless Vendor has documented compensating controls and obtained Company's prior written approval.

13. Malware Protection, Endpoint Security, and Network Security

13.1 Vendor shall implement appropriate endpoint, server, email, and network security controls to reduce risk of malware, ransomware, unauthorized access, data exfiltration, and lateral movement.

13.2 Vendor shall use anti-malware, endpoint detection and response, or equivalent protective capabilities where appropriate to the service environment.

13.3 Vendor shall logically segment production, development, and test environments and restrict administrative access to production environments.

13.4 Vendor shall protect internet-facing services using secure configuration, access restrictions, monitoring, and where appropriate, web application firewall, DDoS protection, rate limiting, and other relevant controls.

14. Cloud, Hosting, and Infrastructure Security

14.1 Vendor shall ensure that cloud and hosted environments used to provide the services are securely configured and administered in accordance with documented standards.

14.2 Vendor shall use separate environments and logical segregation controls sufficient to prevent unauthorized access between tenants, customers, environments, or workloads.

14.3 Vendor shall maintain documented responsibilities for security in shared-responsibility environments and ensure its controls address Vendor's assigned responsibilities.

14.4 Vendor shall maintain backup, recovery, availability, and resilience controls appropriate to the services and any commitments in the Agreement.

14.5 Upon request, Vendor shall identify the hosting model and primary hosting regions applicable to Company Data.

15. Incident Response and Notification

15.1 Vendor shall maintain a written incident response plan with defined roles, escalation paths, investigation procedures, containment, eradication, recovery, evidence preservation, communications, and post-incident review.

15.2 Vendor shall notify Company of any Security Incident **without undue delay and in no event later than twenty-four (24) hours** after becoming aware of the Security Incident if the incident:

- affects or may affect Company Data;
- affects or may affect Company Systems;
- materially affects the confidentiality, integrity, availability, or resilience of the services; or

- is reasonably likely to require Company to investigate, notify, respond, or take action.

15.3 Such notification shall include, to the extent known at the time:

- the nature of the incident;
- date and time of discovery;
- affected systems, services, and data types;
- actual or reasonably suspected impact;
- containment actions taken or planned;
- Vendor contact information for the incident lead; and
- any immediate actions reasonably recommended for Company.

15.4 Vendor shall provide regular updates as material information becomes available and shall cooperate fully with Company in investigation, containment, remediation, recovery, regulatory analysis, evidence preservation, customer communications, and reasonable requests for information.

15.5 Vendor shall not notify regulators, affected individuals, customers, media, or other third parties about a Security Incident specifically involving Company Data or Company Systems in a manner that identifies Company without Company's prior written approval, unless legally required to do so. In that case, Vendor shall, to the extent legally permitted, provide Company advance notice and coordinate the content of the notice.

15.6 Vendor shall retain relevant evidence and logs and conduct root cause analysis and corrective action planning following any material Security Incident.

16. Business Continuity, Disaster Recovery, and Operational Resilience

16.1 Vendor shall maintain business continuity and disaster recovery plans appropriate to the nature of the services and associated risks.

16.2 Vendor shall back up systems and data necessary to restore the services and protect such backups appropriately.

16.3 Vendor shall test business continuity and disaster recovery capabilities at least annually, or more frequently where required by the Agreement or service criticality, and shall address material deficiencies in a timely manner.

16.4 Upon request for critical services, Vendor shall provide Company with a summary of its recovery objectives, recent test results, and material corrective actions.

16.5 Vendor shall promptly notify Company of any event that materially degrades service continuity, resilience, or agreed recovery capabilities.

17. Subcontractors, Subprocessors, and Fourth-Party Risk

17.1 Vendor shall not engage any Subprocessor or Subcontractor to access, host, or process Company Data, or to materially support the services, without:

- prior written authorization from Company, where required by the Agreement; or
- at a minimum, advance written notice and an opportunity for Company to object, if that mechanism is permitted by the Agreement.

17.2 Vendor shall conduct appropriate due diligence and ongoing oversight of Subprocessors and Subcontractors commensurate with the risk they present.

17.3 Vendor shall ensure all approved Subprocessors and Subcontractors are bound by written obligations no less protective than those in this Addendum, including obligations relating to confidentiality, security, privacy, incident reporting, audit cooperation, data return/deletion, and restrictions on use of Company Data.

17.4 Vendor remains fully liable for acts and omissions of its Subprocessors and Subcontractors relating to this Addendum and the Agreement.

17.5 Upon request, Vendor shall provide a current list of Subprocessors and Subcontractors that may access Company Data or materially support the services, including a description of the service provided and hosting location, where relevant.

18. Artificial Intelligence and Automated Processing

18.1 Vendor shall not use Company Data in any artificial intelligence, machine learning, large language model, or similar automated system for training, fine-tuning, model improvement, generalized analytics, or product development purposes unless expressly authorized in writing by Company.

18.2 If Vendor uses AI or automated decision-support capabilities in delivering the services, Vendor shall:

- document the purpose and scope of such use;
- assess security, privacy, confidentiality, bias, accuracy, reliability, and operational risks;
- implement governance, oversight, and controls appropriate to the risk;
- maintain transparency sufficient for Company to understand the role of AI in the services; and
- promptly disclose to Company any material changes in such use that may affect Company's risk, compliance, or obligations.

18.3 Vendor shall ensure that AI-enabled features processing Company Data are subject to the same or stronger access, logging, data protection, and incident response controls as other service components.

19. Physical and Environmental Security

19.1 Where Vendor facilities or third-party facilities are used to store or process Company Data or to support critical service components, Vendor shall implement physical security controls appropriate to the risk, including controlled access, visitor management, environmental safeguards, and protection against unauthorized removal or damage.

19.2 If Vendor relies on third-party hosting providers, Vendor may satisfy this requirement through documented assurance from those providers, where appropriate.

20. Audit Rights and Cooperation

20.1 During the term of the Agreement and for a reasonable period thereafter, Company or its designated representatives may, upon reasonable notice and during normal business hours, assess Vendor's compliance with this Addendum through questionnaires, document review, interviews, or audits, subject to reasonable confidentiality, safety, and operational constraints.

20.2 Vendor shall reasonably cooperate with such assessments and promptly remediate material deficiencies identified.

20.3 In lieu of an onsite audit, Company may accept current independent assessments, certifications, reports, or other assurance artifacts where such evidence reasonably addresses the relevant risks.

20.4 If a material Security Incident occurs, Vendor shall provide enhanced cooperation, evidence, and access reasonably necessary for Company to assess impact and fulfill its legal, regulatory, operational, or contractual obligations.

21. Data Return, Deletion, and Transition Assistance

21.1 Upon expiration or termination of the Agreement, or upon Company's written request, Vendor shall promptly return Company Data in a mutually agreed usable format and securely delete Company Data from Vendor systems and media, including backups according to Vendor's documented backup lifecycle, except where retention is required by Applicable Law.

21.2 Vendor shall provide written certification of deletion upon request, signed by an authorized representative.

21.3 Vendor shall provide reasonable transition assistance to support migration of services, data, and operations to Company or its designee in a secure manner that minimizes disruption.

21.4 Vendor shall continue to protect retained Company Data in accordance with this Addendum for so long as such data is retained.

22. Insurance

22.1 Vendor shall maintain cyber liability and technology errors and omissions insurance, or equivalent coverage, in commercially reasonable amounts appropriate to the services and associated risks, but in no event less than **[USD $X,000,000]** per claim and in the aggregate, unless otherwise agreed in writing.

22.2 Upon request, Vendor shall provide a certificate of insurance or other reasonable evidence of such coverage.

23. Materiality, Remedies, and Survival

23.1 Compliance with this Addendum is a material obligation of Vendor.

23.2 If Vendor fails to comply with this Addendum, Company may require corrective action, suspend data sharing, suspend connectivity or access, require additional controls, or exercise any other rights and remedies available under the Agreement or law.

23.3 Company may terminate the Agreement for cause if Vendor materially breaches this Addendum and fails to cure such breach within the time period specified in the Agreement, or immediately where the breach creates an unacceptable risk to Company Data, Company Systems, or Company operations.

23.4 Obligations relating to confidentiality, incident cooperation, audit cooperation, return/deletion, restrictions on use of Company Data, and any provisions that by their nature should survive shall survive termination of the Agreement.