

IT SECURITY ADDENDUM

Exhibit D to Master Services Agreement

Client: [CLIENT LEGAL NAME]
Vendor: [VENDOR LEGAL NAME]
Version: 1.0 | Effective: [DATE]

CONFIDENTIAL

SECTION 1 – PURPOSE, SCOPE, AND APPLICABILITY

 **GUIDANCE:** *This addendum is Exhibit D to the MSA. It sets minimum-floor security requirements for Vendor. It should be updated at least annually and whenever Client's risk profile or regulatory obligations change significantly. The scope statement is critical: it should cover all systems, environments, and personnel that touch Client Data, including Vendor's cloud providers, Subprocessors, and remote-access tools.*

- 1.1** This IT Security Addendum ("Addendum") sets forth the minimum information security requirements that Vendor must implement and maintain throughout the Term of the Master Services Agreement (MSA) between Client and Vendor. This Addendum is incorporated into and governed by the MSA.
- 1.2** This Addendum applies to all: (a) Vendor systems, infrastructure, and applications used to deliver the Services or store, process, or transmit Client Data; (b) Vendor personnel (employees, contractors, and Subprocessors) with access to Client Data or Vendor systems that handle Client Data; (c) Vendor's physical facilities in which Client Data is processed or stored; and (d) Vendor's Subprocessors and their systems to the extent they process Client Data.
- 1.3** Client's rights to update security requirements are set forth in Section 8.2 of the MSA. Vendor shall implement any updated requirements within the notice period specified.
- 1.4** Where any requirement in this Addendum is in conflict with requirements in the MSA, the more protective requirement shall apply. Nothing in this Addendum limits Vendor's obligations under applicable law.

SECTION 2 – DEFINITIONS

 **GUIDANCE:** *Security-specific defined terms supplement those in the MSA. Ensure “Critical Vulnerability” and “High Vulnerability” align with the CVSS scoring definitions to make remediation timelines objective and measurable.*

"CISO" means Chief Information Security Officer, or the equivalent functional role responsible for Vendor's information security program.

"Critical Vulnerability" means a vulnerability with a CVSS base score of 9.0 or higher, or that is actively exploited in the wild regardless of CVSS score.

"High Vulnerability" means a vulnerability with a CVSS base score of 7.0–8.9.

"Encryption at Rest" means encryption of stored data using an approved algorithm and key management process.

"Encryption in Transit" means encryption of data during transmission using TLS 1.2 or higher, or an equivalent approved protocol.

"Least Privilege" means granting users, systems, and processes the minimum level of access rights required to perform their functions.

"MFA" means multi-factor authentication using at least two distinct authentication factors: something the user knows (password), something the user has (hardware token, authenticator app), or something the user is (biometric).

"Penetration Test" means a simulated cyberattack against Vendor's systems conducted by a qualified third party to identify exploitable vulnerabilities.

"SIEM" means Security Information and Event Management system used to aggregate, correlate, and analyze security events across Vendor's environment.

"SOC" means Security Operations Center, the function responsible for monitoring Vendor's security posture, detecting threats, and responding to Security Incidents.

"Zero Trust Architecture" means a security model based on the principle that no user, device, or network segment should be inherently trusted, requiring continuous verification of identity and authorization.

SECTION 3 – INFORMATION SECURITY PROGRAM

 **GUIDANCE:** A written, governed information security program is the foundation of all other security requirements. ISO/IEC 27001 is the international standard; NIST CSF 2.0 is the U.S. government-aligned framework. Require Vendor to align with at least one recognized framework and to document alignment. Board/executive-level accountability for security has become a regulatory expectation under DORA, the SEC cybersecurity disclosure rules, and many state laws.

- 3.1** Vendor shall maintain a comprehensive, documented Information Security Program (ISP) that: (a) is reviewed and updated at least annually; (b) is approved by Vendor's board of directors or equivalent governing body at least annually; (c) is aligned with a recognized security framework (ISO/IEC 27001, NIST Cybersecurity Framework 2.0, SOC 2, CIS Controls, or equivalent); (d) covers all systems, personnel, and physical facilities within the scope of Section 1.2; and (e) addresses the security domains set forth in this Addendum.
- 3.2** Vendor's ISP shall include, at minimum: (a) an information security policy and acceptable use policy; (b) asset inventory and classification procedures; (c) risk assessment and treatment procedures; (d) access control and identity management procedures; (e) cryptography and key management policy; (f) physical and environmental security controls; (g) operations security procedures; (h) network security architecture and controls; (i) supplier and third-party security requirements; (j) incident management procedures; (k) business continuity and disaster recovery plans; (l) compliance monitoring and audit procedures; and (m) security awareness and training programs.
- 3.3** Vendor shall designate a CISO or equivalent senior security executive with direct accountability for the ISP, who shall have sufficient authority, resources, and independence to carry out security obligations. Vendor shall provide Client with the name and contact information of the CISO upon request.
- 3.4** Vendor shall conduct a formal risk assessment covering all systems and processes within scope at least annually, or following any material change to Vendor's environment. Risk assessment results shall be documented, and identified risks shall be treated in accordance with Vendor's risk treatment methodology. Vendor shall provide Client with a summary of its most recent risk assessment upon request.
- 3.5** Vendor shall provide Client with the following documentation within thirty (30) days of execution of the MSA and annually thereafter: (a) most recent SOC 2 Type II report or equivalent third-party audit report; (b) current ISO/IEC 27001 or equivalent certification, if held; (c) written summary of Vendor's ISP; and (d) most recent penetration test executive summary (redacted for operational security).

SECTION 4 – ACCESS CONTROLS AND IDENTITY MANAGEMENT

 **GUIDANCE:** Access controls are the single most effective control against both external attacks and insider threats. According to Verizon DBIR, over 80% of breaches involve compromised credentials. MFA and Least Privilege are non-negotiable for any vendor handling sensitive Client Data. Privileged Access Management (PAM) is increasingly a regulatory expectation and an audit focus area.

4.1 Account Management

- 4.1.1** Vendor shall implement a formal user access management process that includes: (a) formal access provisioning and de-provisioning procedures; (b) access rights review at least quarterly for privileged accounts and semi-annually for standard accounts; (c) immediate revocation of access upon termination or role change; and (d) prohibition on shared or generic accounts for any access to systems processing Client Data.
- 4.1.2** Vendor shall de-provision all access to Client systems and Client Data within twenty-four (24) hours of any personnel departure or role change that removes the need for such access, and shall provide Client with written confirmation of de-provisioning within forty-eight (48) hours.

4.2 Multi-Factor Authentication

- 4.2.1** Vendor shall require MFA for: (a) all remote access to Vendor systems that process Client Data; (b) all access to cloud-based platforms and applications that process Client Data; (c) all privileged and administrative access; (d) all access to Vendor's VPN; and (e) all access to email systems by personnel with access to Client Data. MFA shall use phishing-resistant methods (hardware security keys, authenticator apps) where technically feasible; SMS-based OTP is not acceptable for privileged access.

4.3 Least Privilege and Role-Based Access Control

- 4.3.1** Vendor shall implement role-based access control (RBAC) based on the principle of Least Privilege. Access rights shall be granted based on job function, with no individual granted access beyond the minimum necessary to perform their duties. Default access rights shall be deny-all; access shall be affirmatively granted and documented.
- 4.3.2** Client Data shall be accessible only to Vendor personnel who have a specific, documented business need for such access. Vendor shall maintain an access control list for Client Data and shall provide this list to Client upon request.

4.4 Privileged Access Management

- 4.4.1** Vendor shall implement Privileged Access Management (PAM) controls for all privileged accounts, including: (a) use of a PAM solution to manage, vault, rotate, and audit privileged credentials; (b) just-in-time (JIT) access provisioning for privileged tasks where feasible; (c) prohibition on using privileged accounts for day-to-day activities; (d) dual-approval requirements for access to production environments that store Client Data; and (e) full session recording and logging of all privileged access sessions.

4.5 Password Requirements

- 4.5.1** Vendor shall enforce the following password standards for accounts with access to systems that process Client Data: (a) minimum password length of at least fourteen (14) characters; (b) prohibition on common, dictionary, or previously breached passwords (enforced via a password blacklist); (c) passwords shall not expire on a calendar schedule (per NIST SP 800-63B recommendations) but shall be reset immediately upon any suspected compromise; (d) prohibition on password reuse of the last twelve (12) passwords; and (e) use of a password manager for all corporate accounts.

SECTION 5 – NETWORK SECURITY AND ARCHITECTURE

 **GUIDANCE:** *Network segmentation is the most effective control for limiting blast radius in a breach — it is what separates the SolarWinds-type breach (full network traversal) from a contained incident. Zero Trust Architecture is the current best-practice model. Require Vendor to document its network architecture and provide a network diagram (marked confidential) for Client's own third-party risk assessment.*

- 5.1 Vendor shall implement network segmentation to isolate systems that process or store Client Data from other systems in Vendor's environment, including internet-facing systems, development environments, and corporate networks. Client Data shall not reside in or be accessible from any unsegmented network zone.
- 5.2 Vendor shall implement and maintain enterprise-grade firewalls at all network boundaries, configured according to a documented rule set reviewed and approved by Vendor's security team. Firewall rules shall follow a deny-all, allow-by-exception principle. Rule sets shall be reviewed and recertified at least quarterly.
- 5.3 Vendor shall implement intrusion detection and intrusion prevention systems (IDS/IPS) on all network segments that process Client Data, with alerting configured to notify Vendor's SOC of anomalous traffic patterns in near-real time.
- 5.4 Vendor shall prohibit direct internet access from systems that process Client Data, enforcing all internet traffic through a web proxy with content inspection capabilities. Vendor shall maintain a documented list of allowed outbound destinations for systems processing Client Data.
- 5.5 All remote access to Vendor's network by Vendor personnel or Subcontractors shall use a VPN with MFA. Vendor shall not use split-tunnel VPN configurations for remote access to systems that process Client Data.
- 5.6 Vendor shall maintain a documented network architecture diagram and shall provide it to Client upon request, subject to appropriate confidentiality protections. The diagram shall identify all network zones, trust boundaries, and Client Data flows.
- 5.7 Vendor shall implement DNS filtering, email security controls (including SPF, DKIM, and DMARC), and anti-phishing technical controls on all systems used by personnel with access to Client Data.
- 5.8 Where Vendor delivers Services via cloud infrastructure (IaaS, PaaS, or SaaS), Vendor shall implement a Cloud Security Posture Management (CSPM) solution to continuously monitor cloud configurations against security best practices and shall remediate identified misconfigurations within the timelines specified in Section 12.

SECTION 6 – ENCRYPTION AND CRYPTOGRAPHY

 **GUIDANCE:** Encryption requirements must specify both algorithms and key management. TLS 1.0 and 1.1 are deprecated. AES-256 is the current standard for data at rest. Key management is where most encryption implementations fail: keys stored alongside data they encrypt, keys shared among multiple Vendor clients, or keys controlled solely by Vendor with no Client key custody. Consider requiring Client-managed encryption keys (BYOK — Bring Your Own Key) for the most sensitive data classifications. Post-quantum cryptography is emerging; NIST finalized PQC standards in 2024.

- 6.1 Vendor shall encrypt all Client Data in transit using TLS 1.2 or higher. TLS 1.0 and TLS 1.1 shall be disabled on all systems that process or transmit Client Data. Vendor shall disable all insecure protocols (SSLv2, SSLv3, TLS 1.0, TLS 1.1) and shall not use self-signed certificates for production systems accessible by Client.
- 6.2 Vendor shall encrypt all Client Data at rest using AES-256 or equivalent. Encryption shall be applied at the volume, database, and/or file level as appropriate to the data classification. Encryption shall be implemented such that the compromise of storage media alone does not expose Client Data in readable form.
- 6.3 Vendor shall implement a formal cryptographic key management program that includes: (a) generation of encryption keys using a hardware security module (HSM) or equivalent hardware-backed key store; (b) documented key rotation schedules (annual rotation of data encryption keys; immediate rotation upon suspected compromise); (c) dual-control and split-knowledge procedures for master key operations; (d) documented key custodianship and access controls; (e) secure key storage separate from the data it encrypts; and (f) documented key destruction procedures for decommissioned or compromised keys.
- 6.4 Vendor shall support, upon Client request, Client-managed encryption keys (BYOK) or Client hold-their-own keys (HYOK) for Client Data stored in Vendor's cloud environments, where technically feasible.
- 6.5 Vendor shall prohibit the storage of Client Data on portable media (USB drives, external hard drives, laptops not protected by full disk encryption). Any permitted portable media shall use AES-256 full disk encryption.
- 6.6 In preparation for post-quantum threats, Vendor shall: (a) maintain a cryptographic inventory identifying all cryptographic algorithms in use across systems that process Client Data; (b) develop a post-quantum cryptography migration plan by [date, e.g., December 31, 2026]; and (c) begin migration to NIST-approved post-quantum cryptographic algorithms for long-term data protection upon mutual agreement with Client.

SECTION 7 – VULNERABILITY MANAGEMENT AND PATCH MANAGEMENT

 **GUIDANCE:** *Unpatched vulnerabilities are the leading cause of exploitable attack surfaces. CISA KEV (Known Exploited Vulnerabilities) catalog provides a priority list of vulnerabilities actively exploited in the wild. Require Vendor to subscribe to and act on KEV notifications. Remediation SLAs must be specific, measurable, and enforced. Log4Shell (CVE-2021-44228) and MOVEit (CVE-2023-34362) demonstrated that Vendors can take weeks or months to patch critical vulnerabilities without contractual pressure.*

- 7.1 Vendor shall operate a continuous vulnerability management program covering all systems within the scope of this Addendum. Vendor shall perform authenticated vulnerability scans of all in-scope systems at least weekly for internet-facing systems and at least monthly for internal systems.
- 7.2 Vendor shall remediate identified vulnerabilities within the following timeframes, measured from the date of discovery or publication of the vulnerability (whichever is earlier):
 - (a) Critical Vulnerabilities (CVSS 9.0+, or CISA KEV-listed): within seventy-two (72) hours of discovery (emergency patch or mitigating control applied);
 - (b) High Vulnerabilities (CVSS 7.0–8.9): within fifteen (15) days;
 - (c) Medium Vulnerabilities (CVSS 4.0–6.9): within thirty (30) days;
 - (d) Low Vulnerabilities (CVSS 0.1–3.9): within ninety (90) days or accepted per risk acceptance process.
- 7.3 Vendor shall subscribe to and monitor CISA's Known Exploited Vulnerabilities (KEV) catalog and shall treat all KEV-listed vulnerabilities as Critical regardless of CVSS score. Vendor shall notify Client within twenty-four (24) hours if any KEV-listed vulnerability is identified in systems that process Client Data.
- 7.4 Where immediate patching is not technically feasible, Vendor shall implement compensating controls within the applicable remediation window and shall document the risk acceptance in its exception management process. Client's approval shall be required for any exception involving systems that process Client Data where a Critical or High vulnerability cannot be remediated within the required timeframe.
- 7.5 Vendor shall provide Client with a quarterly vulnerability management report summarizing: (a) the number and severity of open vulnerabilities; (b) remediation rates by severity; (c) any exceptions and their compensating controls; and (d) mean time to remediate by severity level.
- 7.6 Vendor shall patch operating systems, middleware, and third-party libraries (including open source components) used in the Services, not only Vendor's proprietary software. Vendor shall maintain a software bill of materials (SBOM) for all software components used in the Services and shall provide Client with the SBOM upon request.

SECTION 8 – SECURITY TESTING AND PENETRATION TESTING

 **GUIDANCE:** Annual penetration testing is now a baseline expectation in virtually all enterprise security frameworks. For high-risk vendors, consider requiring quarterly red team exercises or continuous attack surface monitoring. Bug bounty programs are a cost-effective supplement. Client should have the right to conduct (or commission) its own penetration test, with sufficient notice and scope agreement, but must be prevented from disrupting Vendor's production environment.

- 8.1** Vendor shall commission an independent penetration test of all systems within the scope of this Addendum at least annually, conducted by a qualified third-party firm with relevant certifications (OSCP, GPEN, GWAPT, CEH, or equivalent). The penetration test scope shall include, at minimum: (a) external network penetration testing; (b) internal network penetration testing; (c) web application testing for all client-facing applications; (d) API security testing; and (e) social engineering testing (phishing simulation) at Vendor's election.
- 8.2** Vendor shall provide Client with: (a) the executive summary of each penetration test report within thirty (30) days of completion; and (b) a remediation plan for all Critical and High findings within fifteen (15) days of receiving the final report. Vendor shall remediate all Critical findings within thirty (30) days and High findings within sixty (60) days of the final report, and shall provide Client with written confirmation of remediation.
- 8.3** Client reserves the right to conduct (or commission) its own security assessment of Vendor's systems, upon sixty (60) days' prior written notice and subject to execution of a separate rules of engagement agreement. Any such assessment shall be conducted in a non-production environment or during a maintenance window, shall be limited to Client-specific systems and Client Data flows, and shall be conducted by a qualified security firm. Vendor shall cooperate fully with such assessments.
- 8.4** Vendor shall conduct application security testing (AST) including static application security testing (SAST) and dynamic application security testing (DAST) as part of its software development lifecycle for all applications used to deliver the Services. Vendor shall not release application updates with unmitigated Critical or High vulnerabilities identified through SAST/DAST.
- 8.5** Vendor shall conduct phishing simulation exercises for all personnel with access to Client Data at least twice annually and shall provide security awareness training within thirty (30) days to all personnel who fail a simulation.

SECTION 9 – SECURITY MONITORING, LOGGING, AND DETECTION

 **GUIDANCE:** *Logging is the primary means of detecting breaches and supporting incident investigation. Many breaches are discovered months after initial compromise; without comprehensive logs retained for a sufficient period, forensic investigation is impossible. SIEM + SOC is the current baseline for Tier 1 enterprise security. NDR (Network Detection and Response) and EDR (Endpoint Detection and Response) together provide comprehensive telemetry. Log retention requirements must align with your forensic investigation needs and regulatory retention obligations.*

- 9.1** Vendor shall implement and maintain a SIEM system that aggregates security events from all systems within the scope of this Addendum in near-real time. The SIEM shall be configured to detect and alert on, at minimum: (a) unauthorized access attempts and authentication failures; (b) privilege escalation; (c) anomalous data access or exfiltration patterns; (d) malware detection; (e) network reconnaissance activity; (f) modifications to security controls or audit configurations; and (g) access to Client Data outside of normal business hours or from unexpected locations.
- 9.2** Vendor shall maintain security logs sufficient to reconstruct security incidents and support forensic investigation. Logs shall be: (a) retained for a minimum of twelve (12) months online (queryable) and an additional twelve (12) months in offline or archive storage; (b) protected from unauthorized modification or deletion (immutable log storage); (c) synchronized to a common time standard (NTP with a trusted source); and (d) inclusive of, at minimum: authentication events, access control changes, data access and modification events, network traffic logs, and system configuration changes.
- 9.3** Vendor shall maintain a SOC capability (internal or contracted) providing twenty-four (24) hour, seven (7) day, three hundred sixty-five (365) day monitoring of security events affecting systems that process Client Data. The SOC shall have documented escalation procedures and mean time to detect (MTTD) and mean time to respond (MTTR) targets reviewed with Client annually.
- 9.4** Vendor shall deploy Endpoint Detection and Response (EDR) agents on all endpoints (workstations, laptops, servers) within the scope of this Addendum. EDR solutions shall provide real-time threat detection, behavioral analysis, and the ability to isolate compromised endpoints. Vendor shall not use signature-only antivirus as a substitute for EDR.
- 9.5** Vendor shall deploy Network Detection and Response (NDR) capabilities to detect lateral movement, command-and-control traffic, and anomalous data flows within the network segments that process Client Data.
- 9.6** User and Entity Behavior Analytics (UEBA) shall be implemented, or SIEM rules shall be configured to equivalent effect, to detect anomalous user behavior including bulk data access, access from unusual geographic locations, and access outside normal patterns, particularly for accounts with access to Client Data.

SECTION 10 – INCIDENT RESPONSE

 **GUIDANCE:** *The incident response requirements here supplement the notification requirements in Article 16 of the MSA. The key additions here are the technical requirements: documented IRP with defined roles, tabletop exercises, and the contractually binding notification timeline of 24 hours. The NIST SP 800-61 lifecycle (Preparation, Detection and Analysis, Containment, Eradication and Recovery, Post-Incident Activity) is the standard framework.*

- 10.1** Vendor shall maintain a documented Incident Response Plan (IRP) that: (a) follows the NIST SP 800-61 or equivalent incident response lifecycle (Preparation, Detection and Analysis, Containment, Eradication and Recovery, Post-Incident Activity); (b) identifies roles and responsibilities for the incident response team; (c) defines incident classification criteria and severity levels; (d) includes notification procedures, including the twenty-four (24) hour notification obligation to Client set forth in Section 16.3 of the MSA; (e) includes evidence preservation and chain of custody procedures; and (f) is reviewed and updated at least annually and after any material Security Incident.
- 10.2** Vendor shall conduct tabletop incident response exercises at least annually, testing at minimum: (a) a ransomware or destructive malware scenario affecting systems that process Client Data; (b) a data exfiltration scenario involving Client Data; and (c) a third-party / supply chain compromise scenario. Vendor shall provide Client with a summary of tabletop exercise results upon request.
- 10.3** Vendor's incident response capability shall include: (a) a dedicated incident response retainer with a qualified forensic firm, or equivalent in-house capability; (b) documented procedures for engaging legal counsel and regulatory counsel in the event of a Data Breach; (c) a communication plan for notifying regulators, law enforcement, and affected individuals; and (d) a post-incident review process to identify root causes and implement systemic improvements.
- 10.4** Vendor shall not destroy, overwrite, or otherwise alter any evidence relevant to a Security Incident without Client's written consent, and shall preserve forensic evidence in a manner suitable for potential litigation and regulatory proceedings.

SECTION 11 – DATA CLASSIFICATION, HANDLING, AND DESTRUCTION

 **GUIDANCE:** *Data classification is a foundational control: you cannot protect what you have not categorized. Client Data should be classified at the highest sensitivity level applicable to its content. Secure media disposal (NIST 800-88 guidelines) is often overlooked at offboarding and is a regulatory focus area. The certificate of destruction requirement is a contractual backstop for the data return/deletion obligation in MSA Article 6.7.*

- 11.1** Vendor shall implement a formal data classification scheme covering all data processed under this Agreement. Client Data shall be classified at the equivalent of “Confidential” or higher in Vendor’s classification scheme and shall receive the highest level of protection required for any data in that classification.
- 11.2** Vendor shall implement data handling procedures specifying how Client Data may be stored, transmitted, accessed, shared, processed, and destroyed at each stage of its lifecycle. Such procedures shall prohibit: (a) storage of Client Data on personal devices; (b) transmission of Client Data via unencrypted channels (including unencrypted email); (c) storage of Client Data in geographies not approved by Client under Section 6.6 of the MSA; (d) printing or physical reproduction of Client Data except as strictly necessary for performance of the Services; and (e) co-mingling of Client Data with data from other clients in a manner that makes data isolation impossible.
- 11.3** Vendor shall implement Data Loss Prevention (DLP) controls on all systems with access to Client Data, including: (a) DLP policies preventing bulk download, exfiltration, or transmission of Client Data; (b) blocking of unauthorized cloud storage, personal email, and USB transfer of Client Data; and (c) monitoring and alerting for policy violations.
- 11.4** Upon expiration or termination of the MSA, or upon Client’s written request at any time, Vendor shall securely destroy all Client Data in accordance with NIST SP 800-88 Guidelines for Media Sanitization (or equivalent) within thirty (30) days and shall provide Client with a certificate of destruction specifying: (a) the types and approximate volume of data destroyed; (b) the destruction method used (e.g., cryptographic erasure, overwriting, physical destruction); (c) the date of destruction; and (d) the systems and media from which destruction was performed.
- 11.5** Vendor shall not transfer Client Data to any backup, archive, or secondary storage system without ensuring equivalent security controls apply in the destination environment and that the transfer is captured in Vendor’s data inventory.

SECTION 12 – PHYSICAL AND ENVIRONMENTAL SECURITY

 **GUIDANCE:** *Physical security is often overlooked in IT security assessments but is directly relevant to data breaches via physical theft, unauthorized physical access, or tailgating into data centers. Data center certifications (SOC 2, ISO 27001) generally cover physical security, but Vendor's primary office environments also handle Client Data through employee workstations and may not be covered by data center certifications.*

- 12.1** Vendor shall maintain physical access controls at all facilities where Client Data is processed or stored, including: (a) multi-factor physical access controls (badge + PIN or badge + biometric) at entry points to areas processing Client Data; (b) visitor management procedures requiring escorts for non-badged visitors; (c) physical access logs reviewed at least monthly; and (d) CCTV monitoring of areas where Client Data is processed or stored, with recordings retained for a minimum of ninety (90) days.
- 12.2** Vendor's data centers (whether operated directly by Vendor or by Vendor's cloud infrastructure providers) shall: (a) implement environmental controls for temperature, humidity, and fire suppression; (b) implement redundant power supply (UPS and generator backup); (c) implement physical intrusion detection systems; (d) be certified or audited under a recognized standard (ISO/IEC 27001, SOC 2, TIA-942, or equivalent) covering physical security; and (e) restrict physical access to authorized data center personnel only.
- 12.3** Vendor shall implement a clean desk policy for all employees and contractors with access to Client Data: (a) physical documents containing Client Data shall be secured when not in use; (b) workstations shall be locked when unattended; and (c) physical document shredders meeting DIN 66399 Level P-4 or equivalent shall be available for destruction of physical documents containing Client Data.

SECTION 13 – PERSONNEL SECURITY AND SECURITY AWARENESS

 **GUIDANCE:** *Insider threats account for a significant proportion of data breaches. Personnel security controls — background checks, training, separation of duties, termination procedures — are the primary mitigations. The scope of background checks should be calibrated to the sensitivity of the data the employee will access. Security awareness training effectiveness should be measured through phishing simulation failure rates, not just training completion rates.*

- 13.1** Prior to providing access to any system that processes Client Data, Vendor shall conduct background screening of all personnel (employees and contractors) including, at minimum: (a) criminal record check for a period of not less than seven (7) years, to the extent permitted by applicable law; (b) identity verification; (c) verification of employment history and highest-level education credential; and (d) for personnel in security-sensitive roles: financial background check and professional reference verification.
- 13.2** Vendor shall require all personnel with access to Client Data or systems that process Client Data to complete: (a) security awareness training covering phishing, social engineering, password hygiene, data handling, and incident reporting — within thirty (30) days of hire and annually thereafter; (b) privacy awareness training covering applicable Privacy Laws, data subject rights, and data handling obligations — within thirty (30) days of hire and annually thereafter; (c) AI acceptable use training — within thirty (30) days of hire and upon material updates to Vendor's AI acceptable use policy; and (d) role-specific security training for personnel in IT, security, and development roles.
- 13.3** Vendor shall implement separation of duties controls to ensure that no single individual has the ability to perform high-risk actions (such as creating user accounts, approving access, and auditing access) without oversight. Critical security functions shall require dual approval.
- 13.4** Vendor shall implement a formal employee termination and offboarding procedure that includes: (a) immediate revocation of all system access upon notice of termination; (b) return of all Client Data, Confidential Information, and equipment; (c) escorted departure from facilities; and (d) post-departure access verification.
- 13.5** Vendor shall maintain a formal security incident reporting program allowing personnel to report security concerns without fear of retaliation, including an anonymous reporting channel.

SECTION 14 – THIRD-PARTY AND SUPPLY CHAIN SECURITY

 **GUIDANCE:** Supply chain security has become a regulatory and Board-level priority following SolarWinds, MOVEit, and similar incidents. Fourth-party risk (Vendor's vendors' vendors) is increasingly recognized as a material risk vector. Require Vendor to extend security obligations to its material Subprocessors and to monitor them continuously, not just at onboarding. Vendor should maintain a complete and current list of all Subprocessors with access to Client Data.

- 14.1** Vendor shall conduct security due diligence on all Subprocessors before granting them access to Client Data, including: (a) completing a standardized security questionnaire; (b) reviewing available audit reports (SOC 2, ISO 27001, or equivalent); and (c) assessing the Subprocessor's vulnerability management practices.
- 14.2** Vendor shall impose contractual security obligations on all Subprocessors that have access to Client Data, requiring compliance with security standards at least as protective as those set forth in this Addendum.
- 14.3** Vendor shall conduct annual security reassessments of all Subprocessors that have ongoing access to Client Data, and shall monitor Subprocessors continuously for security incidents, data breaches, and material adverse security events using a combination of security questionnaires, audit report reviews, and threat intelligence sources.
- 14.4** Vendor shall notify Client within forty-eight (48) hours of becoming aware of any Security Incident affecting a Subprocessor that involves or may involve Client Data.
- 14.5** Vendor shall maintain a complete, current inventory of all Subprocessors with access to Client Data, including: (a) Subprocessor name and legal entity; (b) services provided; (c) geographic location of data processing; (d) data types accessed; and (e) date of last security assessment. This inventory shall be provided to Client upon request and shall be automatically triggered for review whenever a Subprocessor suffers a disclosed security incident.
- 14.6** Vendor's software supply chain shall be protected through: (a) code integrity verification using code signing for all production deployments; (b) software composition analysis (SCA) to identify vulnerable open source components in the software supply chain; (c) a documented secure software development lifecycle (SSDLC); and (d) multi-party approval for deployments to production systems that process Client Data.

SECTION 15 – AI AND MACHINE LEARNING SECURITY

GUIDANCE: AI security requirements are rapidly becoming a standard component of IT security addenda. NIST AI RMF (2023), ISO/IEC 42001 (2023), OWASP LLM Top 10, and the EU AI Act together define the emerging security and governance framework for AI systems. Shadow AI — employees using unauthorized LLMs — is the most common and least-controlled AI risk in enterprise vendor environments today.

- 15.1** Vendor shall maintain an inventory of all AI Systems used in the delivery of Services or that process Client Data, updated at least quarterly. The inventory shall include for each AI System: (a) the AI System name and version; (b) the developer/provider; (c) the Services component it supports; (d) data inputs, including whether Client Data is used; (e) the regulatory risk classification under the EU AI Act; and (f) known limitations, biases, and error rates.
- 15.2** Vendor shall implement a formal AI governance program aligned with at least one recognized framework (NIST AI RMF, ISO/IEC 42001, EU AI Act requirements, or equivalent), including: (a) documented AI risk assessment procedures; (b) human oversight requirements for AI-driven decisions affecting Client or Client's customers; (c) bias detection and remediation procedures; (d) AI model performance monitoring and drift detection; and (e) incident response procedures specific to AI System failures or adversarial attacks.
- 15.3** Vendor shall implement technical controls to prevent Shadow AI use by its personnel, including: (a) a written AI acceptable use policy prohibiting use of unauthorized AI tools for processing Client Data; (b) technical controls (web filtering, DLP policies) blocking or monitoring access to unauthorized generative AI tools from systems with access to Client Data; (c) an approved AI tools list reviewed and updated at least quarterly; and (d) annual awareness training on AI acceptable use.
- GUIDANCE:** Shadow AI represents a significant and growing blind spot for most vendor security programs. A vendor employee copying a client contract or customer data into a free-tier LLM can expose that data to the model provider's training pipeline, third-party access, or data retention beyond the vendor agreement's terms. Technical controls (DLP + web filtering) are more effective than policy alone.
- 15.4** Vendor shall implement security controls to protect AI Systems against: (a) prompt injection attacks (for LLM-based systems); (b) adversarial inputs designed to manipulate model behavior; (c) model inversion attacks; (d) membership inference attacks; and (e) data poisoning through compromised training pipelines. Vendor shall conduct adversarial testing of AI Systems at least annually.
- 15.5** Vendor shall not use Client Data to train, fine-tune, or improve any AI System without Client's prior express written consent, consistent with Section 17.2 of the MSA.
- 15.6** For any AI System used in the Services that makes or materially supports automated decisions affecting Client or Client's customers, Vendor shall: (a) maintain human oversight capable of reviewing and overriding AI-generated decisions; (b) document the basis for AI-generated decisions in sufficient detail to support an explanation to affected individuals; (c) monitor for and remediate AI-generated outcomes that exhibit demographic or other biases; and (d) comply with all applicable obligations under the EU AI Act for deployers of high-risk AI Systems.

SECTION 16 – CLOUD SECURITY

 **GUIDANCE:** *Cloud misconfiguration remains the leading cause of cloud data breaches. The shared responsibility model means Vendor is responsible for securing what runs inside the cloud (applications, data, identities, operating systems) while the cloud provider secures the infrastructure. Cloud Security Posture Management (CSPM) and Cloud Workload Protection Platforms (CWPP) are the primary technical controls. If Vendor uses a specific cloud provider (AWS, Azure, GCP), require alignment with that provider's Well-Architected Framework.*

- 16.1** Where Vendor provides Services using cloud infrastructure (IaaS, PaaS, or SaaS from a third-party cloud provider), Vendor shall: (a) document the shared responsibility model with the cloud provider and Client's data flows within the cloud environment; (b) implement a Cloud Security Posture Management (CSPM) solution to continuously monitor cloud configurations; (c) enable cloud provider security logging and monitoring services (e.g., AWS CloudTrail/GuardDuty, Azure Security Center, GCP Security Command Center) with logs forwarded to Vendor's SIEM; and (d) implement Infrastructure as Code (IaC) security scanning to detect misconfigurations before deployment.
- 16.2** Vendor shall implement cloud identity and access management (IAM) best practices, including: (a) prohibition on use of root/super-admin accounts for day-to-day operations; (b) enforcement of MFA for all cloud console and API access; (c) use of short-lived credentials (temporary tokens) rather than long-lived API keys; (d) regular review and removal of unused IAM roles, policies, and service accounts; and (e) implementation of Service Control Policies (SCPs) or equivalent organization-level guardrails preventing unauthorized data exfiltration.
- 16.3** Client Data stored in cloud environments shall: (a) be encrypted at rest with client-managed keys (BYOK/HYOK) where technically feasible and requested by Client; (b) be stored only in cloud regions approved by Client under Section 6.6 of the MSA; (c) have access logged at the object/record level; and (d) be protected from public internet exposure (no public S3 buckets, no publicly exposed databases or storage accounts).
- 16.4** Vendor shall obtain and maintain relevant cloud security certifications (e.g., ISO/IEC 27017, ISO/IEC 27018, CSA STAR) for cloud services used to deliver the Services, and shall provide evidence of such certifications to Client annually.

SECTION 17 – REMEDIATION TIMELINES AND ESCALATION

GUIDANCE: A consolidated remediation timeline table provides clear, measurable contractual commitments and reduces ambiguity in dispute situations. This table synthesizes the individual remediation requirements from Sections 7, 8, 10, and elsewhere into a single reference. Add a client escalation right (e.g., right to terminate the affected SOW) for repeated failures to meet remediation timelines.

The following table summarizes required remediation timelines. These timelines are contractual commitments and are in addition to any more specific timelines set forth in other sections of this Addendum.

Event / Finding	Notify Client	Contain / Mitigate	Fully Remediate
Critical Vulnerability (CVSS 9+)	24 hours	72 hours	15 days
High Vulnerability (CVSS 7–8.9)	48 hours	7 days	30 days
Medium Vulnerability (CVSS 4–6.9)	5 business days	15 days	60 days
Security Incident (confirmed)	24 hours	24 hours	Per forensic plan
Security Incident (suspected)	24 hours	48 hours	Per forensic plan
Pentest Critical Finding	24 hours of report	30 days	30 days
Pentest High Finding	5 business days of report	45 days	60 days
Subprocessor Incident	48 hours	48 hours	Per forensic plan
Cloud Misconfiguration (Critical)	24 hours	4 hours	24 hours
CISA KEV-listed Vulnerability	24 hours of discovery	72 hours	15 days

17.2 If Vendor fails to meet any remediation timeline set forth in this Section 17 for a Critical or High severity event on two or more occasions within any twelve (12) month period, Client shall have the right to: (a) require Vendor to engage a qualified third-party security firm at Vendor's expense to assess and remediate the failure; (b) impose financial penalties as specified in the applicable SOW or SLA; and/or (c) terminate the affected SOW without penalty upon thirty (30) days' written notice.

SECTION 18 – AUDIT RIGHTS AND COMPLIANCE VERIFICATION

 **GUIDANCE:** *This section operationalizes the audit rights in Article 9 of the MSA at the security-specific level. The annual questionnaire is the lowest-cost, highest-frequency verification mechanism. SOC 2 Type II reports provide the most robust third-party assurance. On-site audits should be reserved for material security concerns. Require Vendor to notify Client of any SOC 2 qualification or significant audit finding immediately.*

- 18.1** Vendor shall respond to Client's annual information security questionnaire (which may be based on SIG, CAIQ, VSAQ, or Client's proprietary template) within thirty (30) business days of receipt.
- 18.2** Vendor shall provide Client with its most recent SOC 2 Type II report (or ISO/IEC 27001 certification and Statement of Applicability, if SOC 2 is not available) within thirty (30) days of each report's issuance, and shall immediately notify Client of: (a) any qualified opinion or material finding in a SOC 2 or audit report; (b) any lapse, suspension, or revocation of a security certification; or (c) any material change to Vendor's security program that may affect compliance with this Addendum.
- 18.3** Client reserves the right to conduct security assessments of Vendor as described in Article 9 of the MSA. Vendor shall cooperate fully and shall provide access to relevant documentation, systems, and personnel as reasonably requested.
- 18.4** Vendor shall implement a continuous compliance monitoring program and shall provide Client with a quarterly attestation letter from Vendor's CISO confirming Vendor's ongoing compliance with the material requirements of this Addendum.

SECTION 19 – CERTIFICATIONS AND STANDARDS ALIGNMENT

GUIDANCE: Required certifications should be calibrated to the risk tier of the vendor. For Tier 1 critical vendors, require SOC 2 Type II + ISO 27001. For regulated data (PHI, PCI data), require sector-specific certifications. PCI-DSS is required for any vendor touching cardholder data. HIPAA does not have a certification scheme but requires a Business Associate Agreement. FedRAMP is required for cloud services sold to U.S. federal agencies.

- 19.1** Unless otherwise agreed in writing, Vendor shall obtain and maintain throughout the Term the following security certifications applicable to the Services:
- (a) SOC 2 Type II (Security and Availability Trust Service Criteria) — annual audit with report issued within ninety (90) days of audit period end;
 - (b) ISO/IEC 27001 — where Vendor's size and scope make certification feasible (otherwise, alignment with ISO 27001 shall be documented);
 - (c) PCI-DSS Level 1 Merchant or Service Provider certification — if Vendor processes, stores, or transmits cardholder data on Client's behalf;
 - (d) HIPAA Business Associate Agreement — if Vendor processes Protected Health Information (PHI) on Client's behalf;
 - (e) ISO/IEC 42001 AI Management System certification — where Vendor operates AI Systems in the delivery of Services (or equivalent AI governance framework attestation where ISO 42001 certification is not yet available).
- 19.2** Vendor shall align its security program with the following frameworks, as evidenced by documentation available to Client upon request:
- (a) NIST Cybersecurity Framework 2.0 — Vendor shall document its CSF profile (current and target) and provide it to Client annually;
 - (b) NIST AI Risk Management Framework — for AI Systems used in the Services;
 - (c) CIS Controls v8 — Vendor shall implement all applicable Implementation Group 2 (IG2) controls for organizations handling sensitive data; and
 - (d) OWASP Application Security Verification Standard (ASVS) Level 2 — for all web applications used to deliver the Services.

SECTION 20 – SECURITY REPORTING AND GOVERNANCE

 **GUIDANCE:** Regular security reporting creates accountability and facilitates Client's ongoing third-party risk monitoring. The CISO-to-CISO (or equivalent) cadence ensures that security issues reach the appropriate level rather than being resolved at the operational level and never escalated. Security scorecards allow Client to trend Vendor's security posture over time and integrate into Client's own TPRM program management.

- 20.1** Vendor shall provide Client with the following security reports on the schedules specified:
- (a) Monthly: (i) patch compliance rate by severity (Critical, High, Medium, Low); (ii) open vulnerability count by severity; (iii) Security Incidents detected and resolved in the prior month; (iv) any Security Incidents in progress.
 - (b) Quarterly: (i) comprehensive vulnerability management summary (Section 7.5); (ii) access control review results (Section 4.1.2); (iii) security awareness training completion rates (Section 13.2); (iv) CISO attestation of compliance with material requirements of this Addendum (Section 18.4); and (v) AI System inventory updates (Section 15.1).
 - (c) Annually: (i) SOC 2 Type II or equivalent audit report (Section 18.2); (ii) penetration test executive summary (Section 8.2); (iii) NIST CSF profile (Section 19.2(a)); (iv) business continuity and disaster recovery test summary (MSA Section 15.3); and (v) updated Subprocessor inventory (Section 14.5).
- 20.2** Vendor shall designate a named security liaison to Client's TPRM or security team, available during business hours to respond to security inquiries within one (1) business day and to urgent security matters within four (4) hours.
- 20.3** Vendor shall participate in an annual security governance review meeting with Client's CISO (or designee) to: (a) review the prior year's security performance; (b) discuss material changes to Vendor's security posture; (c) review the IT Security Addendum and agree on any needed updates; and (d) align on Client's evolving security requirements.

EXECUTION AND ACKNOWLEDGMENT

The Parties acknowledge that this IT Security Addendum is incorporated into and forms part of the Master Services Agreement. Each Party represents that it has read, understood, and agreed to the terms of this Addendum.

[CLIENT LEGAL NAME]

Signature

Printed Name

Title

Date

[VENDOR LEGAL NAME]

Signature

Printed Name

Title (CISO or authorized signatory)

Date
