Vendor Security Addendum

Version: 1.0

Effective Date: April 2025

Purpose
This addendum outlines the minimum security standards and expectations vendors must meet when handling or accessing company data, systems, or services. It supplements the core vendor agreement.

---

1. Information Security Controls
- Vendor must implement and maintain industry-standard security controls, including:
  - Data encryption at rest and in transit
  - Access controls (role-based, MFA)
  - Network segmentation and firewall protections
  - Secure system development practices

---

2. Personnel & Training
- Vendor employees with access to company data must complete annual security awareness training
- Background checks are required for roles with administrative or sensitive data access

---

3. Breach Notification
- Vendor must notify the company of any data breach or suspected compromise within **48 hours**
- Notification must include known details, impact assessment, and mitigation steps

---

4. Subprocessors
- Vendor must disclose all subprocessors handling company data
- Subprocessors must adhere to equal or greater security standards
- Company reserves the right to object to new subprocessors

---

5. Audits & Reporting
- Company may audit vendor's security controls with **30 days' notice**
- Vendor agrees to provide evidence of certifications (e.g., SOC 2, ISO 27001), penetration tests, or security assessments upon request

---

6. Termination
- Company may terminate the agreement immediately if vendor fails to meet these security obligations
- Upon termination, vendor must return or securely destroy all company data

---

7. Survival
- These obligations remain in effect even after termination of the main agreement

---

By signing below, the Vendor agrees to comply with the terms outlined in this Security Addendum.

Vendor Name:
Authorized Representative:
Date: