

SECURITY ADDENDUM

This is a customizable starting template, not a finished legal document. Replace every [BRACKETED] field with your specifics, delete or adapt any clause that does not fit your arrangement, and have a licensed attorney in the governing jurisdiction review it before you or anyone else signs. CyberSygn is not a law firm and this template is not legal advice.

This Security Addendum (this "**Addendum**") is entered into as of [EFFECTIVE DATE] (the "**Effective Date**") by and between:

[CUSTOMER LEGAL NAME], a [STATE] [ENTITY TYPE, e.g. limited liability company] with its principal place of business at [CUSTOMER ADDRESS] ("**Customer**"); and

[VENDOR LEGAL NAME], a [STATE] [ENTITY TYPE] with its principal place of business at [VENDOR ADDRESS] ("**Vendor**").

Customer and Vendor are each a "**Party**" and together the "**Parties**."

Recitals. The Parties have entered into, or will enter into, an underlying agreement under which Vendor provides products or services to Customer (the "**Principal Agreement**"). This Addendum sets out the security commitments that apply to Vendor's handling of Customer's data and systems. In consideration of the mutual promises below, and as a condition of the Principal Agreement, the Parties agree as follows.

1. Definitions and Scope

1.1 Defined terms. "**Customer Data**" means data that Customer or its users provide to, or that Vendor processes on behalf of Customer under, the Principal Agreement. "**Security Incident**" means a confirmed unauthorized access to, acquisition of, disclosure of, alteration of, loss of, or destruction of Customer Data, or a confirmed compromise of a system holding Customer Data. "**Services**" means the products or services Vendor provides under the Principal Agreement.

1.2 Scope. This Addendum applies to all Customer Data and to all systems, networks, facilities, and personnel that Vendor uses to provide the Services.

1.3 Order of precedence. If a conflict exists between this Addendum and the body of the Principal Agreement on a matter of information security, this Addendum controls.

2. Security Program

2.1 Written program. Vendor will maintain a written information security program that includes administrative, technical, and physical safeguards designed to protect the confidentiality, integrity, and availability of Customer Data, and that is appropriate to the nature of the Services and the sensitivity of the Customer Data.

2.2 Industry alignment. Vendor will align its program with a recognized security framework, such as [FRAMEWORK, e.g. ISO/IEC 27001, SOC 2, NIST CSF], and will not materially weaken its safeguards during the term.

2.3 Ownership. Vendor will assign responsibility for its security program to a qualified individual or team and will review the program at least [FREQUENCY, e.g. annually].

3. Access Control

3.1 Least privilege. Vendor will grant access to Customer Data only to personnel who need it to provide the Services, and only at the minimum level of access required.

3.2 Authentication. Vendor will require unique credentials for each user, enforce strong authentication, and require multi-factor authentication for administrative and remote access to systems holding Customer Data.

3.3 Provisioning and deprovisioning. Vendor will promptly revoke access when a person no longer needs it, and within **[NUMBER, e.g. 24]** hours of a change in that person's role or separation from Vendor.

3.4 Review. Vendor will review access rights to systems holding Customer Data at least **[FREQUENCY, e.g. quarterly]**.

4. Data Protection Measures

4.1 Encryption in transit. Vendor will encrypt Customer Data in transit over public or untrusted networks using current, industry-accepted protocols.

4.2 Encryption at rest. Vendor will encrypt Customer Data at rest where technically feasible, using current, industry-accepted algorithms and sound key management.

4.3 Segregation. Vendor will logically separate Customer Data from the data of Vendor's other customers and from Vendor's own data, except where commingling is necessary and authorized in writing.

4.4 Data minimization. Vendor will collect, retain, and process only the Customer Data needed to provide the Services and will not use Customer Data for its own purposes except as the Principal Agreement permits.

5. Operational Security

5.1 Vulnerability management. Vendor will scan its systems for vulnerabilities on a regular basis and will remediate vulnerabilities on a risk-prioritized schedule, addressing critical vulnerabilities within **[NUMBER, e.g. 30]** days of identification.

5.2 Patching. Vendor will apply security patches to systems holding Customer Data within a reasonable period based on severity.

5.3 Logging and monitoring. Vendor will log security-relevant events on systems holding Customer Data, retain those logs for at least **[NUMBER, e.g. 90]** days, and monitor for anomalous or unauthorized activity.

5.4 Change management. Vendor will follow a documented change-management process for changes to systems that hold or process Customer Data.

6. Personnel and Subcontractors

6.1 Background checks. Subject to applicable law, Vendor will perform background screening on personnel with access to Customer Data, proportionate to the sensitivity of that data.

6.2 Training. Vendor will provide security and privacy awareness training to personnel with access to Customer Data at least **[FREQUENCY, e.g. annually]**.

6.3 Subcontractors. Vendor will impose security obligations no less protective than this Addendum on any subcontractor that handles Customer Data and remains responsible for each subcontractor's performance.

7. Security Incident Response

7.1 Notification. Vendor will notify Customer without undue delay, and in any event within [NUMBER, e.g. 48] hours, after confirming a Security Incident affecting Customer Data.

7.2 Investigation and remediation. Vendor will promptly investigate each Security Incident, take reasonable steps to contain and remediate it, and keep Customer reasonably informed of material developments.

7.3 Cooperation. Vendor will cooperate with Customer's reasonable requests for information needed to meet Customer's own legal or regulatory obligations and will not make any public statement attributing a Security Incident to Customer without Customer's prior written consent, except as required by law.

8. Audit and Assessment

8.1 Reports. On Customer's reasonable request, no more than [NUMBER, e.g. once] per [PERIOD, e.g. twelve months], Vendor will provide its current third-party audit reports or certifications (such as a SOC 2 Type II report or ISO certificate) covering the Services.

8.2 Audit rights. If the available reports do not reasonably address Customer's concerns, or following a Security Incident, Vendor will support a reasonable audit by Customer or its mandated assessor, on reasonable prior notice and subject to confidentiality, conducted so as to minimize disruption to Vendor's operations.

8.3 Findings. Vendor will remediate material findings that show a breach of this Addendum on a mutually agreed, risk-based schedule.

9. Return, Deletion, and General Provisions

9.1 Return or deletion. On expiration or termination of the Principal Agreement, or on Customer's earlier written request, Vendor will return or securely delete Customer Data in accordance with the Principal Agreement, except for copies retained in routine backups or as required by law, which remain subject to this Addendum.

9.2 Secure disposal. Vendor will dispose of media containing Customer Data using methods designed to prevent recovery.

9.3 Survival. Sections 1, 7, 9, and any others that by their nature should survive, survive termination for as long as Vendor retains any Customer Data.

9.4 Governing law and venue. This Addendum is governed by the laws of the State of [STATE], without regard to its conflict-of-laws rules, and the Parties submit to the exclusive jurisdiction of the state and federal courts located in [COUNTY, STATE].

9.5 Severability and waiver. If any provision is unenforceable, the rest remains in effect. A Party's failure to enforce a provision is not a waiver.

9.6 Counterparts and electronic signature. This Addendum may be signed in counterparts and by electronic signature, each of which is an original and all of which together form one agreement.

IN WITNESS WHEREOF, the Parties have executed this Addendum as of the Effective Date.

CUSTOMER

VENDOR

Signature: _____

Signature: _____

Printed name: [NAME]

Printed name: [NAME]

Title: **[TITLE]**

Title: **[TITLE]**

Date: _____

Date: _____

Template provided by CyberSygn. Not legal advice. CyberSygn is not a law firm. Consult a licensed attorney in your jurisdiction before relying on this document.