DATA SECURITY ADDENDUM

Under the Gramm-Leach-Bliley Act and the FTC Safeguards Rule (16 C.F.R. Part 314)

This Data Security Addendum ("Addendum") is entered into by and between **[FIRM LEGAL NAME]** ("Firm") and **SecureLynx, LLC**, a California limited liability company ("Service Provider"), effective as of **[EFFECTIVE DATE]** (the "Effective Date"). Firm and Service Provider may be referred to individually as a "Party" and collectively as the "Parties."

Recitals

A. Service Provider provides **[DESCRIBE SERVICES, e.g., managed IT, security, backup, and support services]** to Firm under a separate services agreement (the "Underlying Agreement"), and in connection with those services may access, receive, maintain, or transmit Customer Information on behalf of Firm.

B. Firm is a "financial institution" subject to the Standards for Safeguarding Customer Information, 16 C.F.R. Part 314 (the "Safeguards Rule"), issued under the Gramm-Leach-Bliley Act ("GLBA"). The Safeguards Rule requires Firm to oversee its service providers and to require them by contract to implement and maintain appropriate safeguards for Customer Information.

C. This Addendum supplements and is incorporated into the Underlying Agreement and sets out the terms governing Service Provider's handling of Customer Information. In the event of a conflict regarding Customer Information, the terms of this Addendum control.

NOW, THEREFORE, in consideration of the mutual promises below, the Parties agree as follows:

1. Definitions

Capitalized terms used but not defined in this Addendum have the meanings given in the Safeguards Rule. For convenience:

- **"Customer Information"** means any record containing nonpublic personal information ("NPI") about a customer of the Firm, in paper, electronic, or other form, that is handled or maintained by or on behalf of the Firm, consistent with 16 C.F.R. § 314.2.
- **"Security Event"** means an event resulting in unauthorized access to, or the disruption or misuse of, an information system, information stored on it, or Customer Information held in physical form.
- **"Authorized User"** means any employee, contractor, agent, or other person authorized by Service Provider to access information systems or Customer Information in connection with the services.
- **"WISP"** means the Firm's written information security program required by the Safeguards Rule.
- **"Qualified Individual"** means the individual designated to oversee, implement, and enforce the WISP under 16 C.F.R. § 314.4(a).

2. Compliance with the Safeguards Rule

Service Provider will implement and maintain administrative, technical, and physical safeguards for Customer Information appropriate to the size and complexity of its operations and the nature and scope of the services, consistent with 16 C.F.R. Part 314. Service Provider will use Customer Information only as necessary to perform the services under the Underlying Agreement, and will limit access to Authorized Users on a need-to-know basis.

3. Safeguards

Service Provider will maintain safeguards that include, at a minimum:

- **Access controls.** Limit access to Customer Information to Authorized Users, apply least-privilege principles, and review access periodically.
- **Encryption.** Encrypt Customer Information at rest and in transit over external networks, consistent with current standards, or apply equivalent compensating controls approved in writing by the Firm.
- **Multi-factor authentication.** Require multi-factor authentication for access to systems that hold Customer Information.
- **Secure disposal.** Securely dispose of Customer Information when it is no longer needed for the services or as the Firm directs, consistent with 16 C.F.R. § 314.4(c).
- **Logging and monitoring.** Maintain logging and monitoring sufficient to detect unauthorized access to or use of Customer Information.
- **Change management.** Follow reasonable change-management procedures for systems that store or transmit Customer Information.

4. Service Provider Personnel and Subcontractors

- Service Provider will train its Authorized Users on the safeguards required by this Addendum.
- Service Provider may engage subcontractors to perform parts of the services, provided it remains responsible for the services and ensures each subcontractor that accesses Customer Information is bound in writing to obligations at least as protective as those in this Addendum.

5. Security Event Notification

- Service Provider will notify the Firm of any Security Event involving Customer Information without unreasonable delay and in no event later than seventy-two (72) hours after discovery.
- The notice will include the information reasonably available about the nature and scope of the Security Event, the Customer Information involved, and the remediation steps taken or planned, and Service Provider will cooperate with the Firm's investigation and response.

- The Parties acknowledge the Firm may be required to report certain Security Events to the Federal Trade Commission within thirty (30) days of discovery, and Service Provider will provide timely assistance to support that obligation.

6. Support for the Firm's Information Security Program (WISP)

- As part of the services, Service Provider will assist the Firm in developing, implementing, and maintaining its WISP, including risk assessments, safeguard implementation, monitoring and testing, and periodic program review.
- **Qualified Individual.** If the Firm designates in writing, Service Provider will make available a qualified person to serve as, or to support, the Firm's Qualified Individual under 16 C.F.R. § 314.4(a).
- **Reporting.** Service Provider will provide periodic reports reasonably sufficient to support the Firm's written reporting to its leadership.
- **Tax preparers.** The Parties acknowledge that tax-return preparers are separately required to maintain a WISP under IRS Publication 4557. Assistance under this Section is intended to support, and not to replace, the Firm's own obligations.
- **Firm responsibility.** The Firm retains ultimate responsibility for its compliance with the Safeguards Rule and for its WISP. Service Provider's role is to support and advise; it does not assume the Firm's legal obligations as a financial institution.

7. Cooperation and Assessment

On the Firm's reasonable written request, and no more than once per year unless a Security Event has occurred, Service Provider will provide information sufficient for the Firm to assess Service Provider's safeguards, such as a summary of its security practices, relevant certifications or audit reports (for example, SOC 2), or responses to a reasonable security questionnaire. This supports the periodic reassessment the Safeguards Rule requires of the Firm.

8. Return or Destruction of Customer Information

On termination of the Underlying Agreement, or at the Firm's earlier written request, Service Provider will return or securely destroy Customer Information in its possession or control, except to the extent retention is required by law or by routine backup cycles, in which case the safeguards in this Addendum continue to apply for as long as the information is retained.

9. Relationship to the Underlying Agreement; Liability

This Addendum is incorporated into and governed by the Underlying Agreement, including its limitation of liability, except where this Addendum expressly states otherwise. Nothing in this Addendum expands Service Provider's liability beyond the limits in the Underlying Agreement.

10. Term

This Addendum is effective as of the Effective Date and continues for as long as Service Provider accesses, receives, maintains, or transmits Customer Information on behalf of the Firm, or until the termination of the Underlying Agreement, whichever is later.

Signatures

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

FIRM

_____

Signature

[FIRM LEGAL NAME]
By (print name): **[NAME]**
Title: **[TITLE]**
Date: **[DATE]**

SERVICE PROVIDER

_____

Signature

SecureLynx, LLC
By (print name):
Title: Founder
Date: **[DATE]**