you.com

SECURITY ADDENDUM

This Security Addendum ("Addendum") is provided to customer ("Customer") by SuSea, Inc. ("Provider") with respect to Provider's products and services. This Addendum is incorporated by reference into the Master Services Agreement ("MSA") for any Order Form by and between Customer and Provider. Terms defined in the MSA shall have the same meaning when used in this Addendum.

A. Commitment to Security

Provider is committed to achieving and preserving the trust of its customers by providing a comprehensive security and privacy program that carefully considers data protection matters across its suite of products and services. For information on Data Protection specifically please see our Data Protection Agreement ("DPA") found at www.you.com/dpa. This Addendum is incorporated by reference into the DPA.

B. Architecture

Provider offers the following architecture options for its services:

Managed Service - Provider's platform runs in the Provider's AWS account, with all Customer Data stored within the account(s) or services, unless otherwise agreed between the parties.

C. Security Controls

Provider implements the following security and operational controls in its environment:

1. **SOC2 Type 2 Audit -** Provider has completed a SOC2 Type 2 audit and can provide the report upon request.

2. **Employment Practices -** The following steps are in place for all Provider resources:

- Background checks are performed on all employees before hiring.
- Employees and Contractors are trained on, and acknowledge in writing their compliance with, security controls and commitment to protecting company and Customer data at the time of hire. Ongoing security awareness training is provided throughout employment and contracting term.
- Access to all Provider environments is revoked upon employee or contractor departure, and all assets are securely wiped before being re-issued or disposed of.

3. **Data Encryption -** The following protocols are in place for data protection:

- **At Rest:** Provider uses industry-standard encryption methods to protect stored Customer Data, which is stored on servers not accessible from the Internet.

○ **In Transit:** Communications between servers and Customer browsers, as well as between servers and Customer Data source servers, are encrypted using industry-standard methods.

4. **Infrastructure -** Provider uses Amazon Web Services (AWS) for its infrastructure, ensuring security and compliance according to industry standards.

5. **Employee Security Practices -** The following steps are implemented as standard for all Providers employees and contractors who have access to Customer Data: Multi-factor authentication and single sign-on (SSO) for all critical applications are mandatory; encryption is enabled on all employee devices, and anti-virus protection is active on all employee laptops; and a clean desk policy and screen savers that lock after inactivity are enforced.

6. **Development Lifecycle -** Security controls are integrated throughout the software development lifecycle, with mandatory code reviews and various testing types, including security tests.

7. **Change Management Policy -** A documented process manages changes to production systems, including security patching and assessments.

8. **Access Controls -** Access to information systems is limited to authorized personnel, ensuring that access is removed promptly when job responsibilities change. Access reviews occur quarterly.

9. **Incident Management -** A security incident response plan is in place, detailing roles, investigation procedures, communication protocols, recordkeeping, and audits. This plan is tested on an annual basis. The plan includes provisions to notify the Customer of any defined security incidents no later than: (i) seventy-two (72) hours after discovery of an incident; or (ii) in accordance with applicable data protection laws and regulations, whichever is shorter. Provider shall provide all reasonable assistance to Customer in Customer meeting its obligations under relevant law.

10. **Logging -** Mechanisms are in place to record and examine activity for all critical applications, services, and infrastructure systems, with measures to protect logs from unauthorized changes. Customers may request log entry records to assist in forensic analysis when Customer Data may be impacted.

11. **Data Retention Policy -** Provider complies with applicable privacy regulations by ensuring Customer data is not retained in violation of deletion requests, or otherwise in violation of data disposal requirements when it is no longer needed per privacy laws. Customer Data is securely deleted upon request and/or when no longer needed. Provider will keep and maintain complete and accurate records in connection with its performance of the Services and will retain these records for at least three (3) years following termination or expiration of the applicable MSA, except that such retention shall not include Protected Confidential Information (as defined therein).

12. **Data Access Policy -** Provider engineers do not have default access to Customer Data and must obtain management approval for access. Access is granted based solely on a need-to-know

basis, with strong authentication measures in place.

13. **Subcontracting** - As further set forth in the DPA, Provider utilizes a Security Trust Portal (e.g. https://trust.you.com) where all subcontracting and subprocessing relationships are defined and disclosed, which is updated from time to time.

D. Responsibilities of the Customer

1. Customer agrees to provide the Provider with all necessary access and support to facilitate the security measures outlined in this Addendum.

2. It is Customer's responsibility to ensure that its use of the Services complies with relevant legal and regulatory obligations.

3. Customer is responsible for managing and securing its methods to access the Services (for example, password, SSO connections, email inboxes for email-code-authentication, etc.).

4. Customer is responsible for keeping its relevant IT systems (such as the browser(s) used to access the Services) up-to-date and appropriately patched.

E. Term and Termination

This Addendum will commence on the Effective Date of the MSA and shall continue until terminated by either party with a written notice of thirty (30) days. This Addendum shall automatically terminate upon the expiration or any earlier termination of the MSA. In addition, if and to the extent Customer terminates its business relationship with Provider, this Addendum and any related DPAs shall likewise automatically terminate.

F. Governing Law

This Addendum and its terms and conditions shall be governed by the laws of the State of California.

G. Amendments

After incorporation by reference into the MSA and the Data Protection Agreement, any later amendments or modifications to this Addendum must be in writing and signed by both parties. Notwithstanding anything to the contrary in this Addendum or otherwise, Provider may modify this Addendum to the extent a governmental, regulatory, or other similar entity or agency requests, or, if Provider determines in the exercise of its reasonable business judgment that it is necessary or advisable, to address compliance-related requirements or certain other legal or contractual obligations ("**Modifications**"), the Parties shall confer and cooperate in good faith to enter into an amendment to this Addendum to implement such Modifications with respect to the provision of services by Provider to Customer.