

This Data Security Exhibit ("**Exhibit**") applies in addition to any existing Master Subscription Services Agreement or End User License Agreement (collectively, the "**Agreement**") between Apttus Corporation ("**Apttus**") and the customer that is a party to such Agreement ("**Customer**"). In the event of any conflict between this Exhibit and the Agreement, this Exhibit shall prevail to the extent of any inconsistency. In the event of any conflict between this Exhibit and any Order executed hereunder, this Exhibit shall prevail to the extent of any inconsistency, except with regard to any provision of any Order that specifically identifies a conflicting provision of this Exhibit and states that the conflicting provision of this Exhibit does not prevail. All capitalized terms, if not otherwise defined herein, shall have the meaning set forth in the Agreement.

Apttus may amend this Exhibit from time to time by posting an amended version at its website and sending Customer notice thereof (an email to Customer's project sponsor shall be deemed sufficient in this case). Such amendment will be deemed accepted and become effective thirty (30) days after such notice (the "**Proposed Amendment Date**") unless Customer first gives Apttus written notice of rejection of the amendment. In the event of such rejection, this Exhibit will continue under their original provisions, and the amendment will become effective at the start of Customer's next term following the Proposed Amendment Date. Customer's continued use of the services purchased hereunder following the effective date of an amendment will confirm Customer's consent thereto. This Exhibit may not be amended in any other way except through a written agreement by authorized representatives of each party.

1. Definitions.

"**Security Incident**" means the reasonable suspicion of, discovery by, or notice to, Customer or Apttus that:

- (a) Customer Data has been disclosed, accessed or obtained by an unauthorized person;
- (b) systems have been compromised; or
- (c) a person has threatened the unauthorized disclosure, access to or obtaining of any Customer Data.

"**Law(s)**" means all laws, regulations, ordinances, rules and orders of any court or government body.

"**Personnel**" means employees and contractors who perform activities in connection with the handling of Customer Data.

"**Personal Information**" is information that can be used on its own or with other information to identify, contact, or locate a single person, or to identify an individual in context.

2. General Obligations.

Apttus agrees to maintain a comprehensive data security program that contains administrative, technical and logical safeguards designed to protect the confidentiality, integrity, and availability of Customer Data and protect it from disclosure, improper alteration, or destruction. The measures implemented and maintained by Apttus for the Service will be subject to annual certification of compliance with ISO 27001.

2.1 Risk Assessment and Treatment.

As part of an annual ISO 27001 certification, Apttus maintains a risk assessment program pertaining to the treatment and handling of Customer Data that has been approved by management, and has been communicated to all employees.

2.2 Access Controls.

- (a) Customer has the ability to limit access to the Subscription Services to authorized Personnel to prevent unauthorized access to Customer Data.
- (b) Subscription Service access logs are maintained.
- (c) The Subscription Service supports identity verification, including multi-factor authentication.

2.3 Encryption. All Customer Data is encrypted while "in transit".

2.4 Apttus Restrictions. Apttus will not, except as necessary to perform its obligations set forth in the Agreement:

- (a) use or disclose any Customer Data for any purpose other than as is strictly necessary to perform its obligations as set forth in the Agreement;
- (b) copy, use, reproduce, display, perform, modify, destroy or transfer any Customer Data or works derived from Customer Data; nor
- (c) sell any Customer Data, or anything that includes any Data, to any person.

2.5 Backups.

- (a) Daily backups of all Customer Data is performed for production environments only (does not include sandboxes).
- (b) Customer Data backups are retained for thirty (30) days.

2.6 Physical Security of Data Centers shall include:

- (a) restricted access and visitor logs;
- (b) electronic controlled access system; and
- (c) CCTV on sensitive areas, unless prohibited by law.

3. Compliance with Laws.

3.1 Regulatory Cooperation. If Apttus collects, accesses, receives, stores or otherwise handles any Customer Data that becomes subject to a regulatory inquiry, notification or other action required by all applicable Laws, Apttus agrees to assist and cooperate to meet any obligation to the relevant regulatory authority.

3.2 Right of Access. Apttus will cooperate with and assist Customer, as necessary, to enable any individual exercising their right of data access, correction, deletion or blocking of Personal Information under any applicable Law.

4. Disclosure by Law.

If Apttus is required by any Law to disclose any Customer Data, Apttus will:

- (a) to the extent permitted by applicable Law, give Customer prior notice of the obligation as soon as practical after becoming aware; and
- (b) take all steps to enable Customer an opportunity to prevent or limit the disclosure of the Customer Data.

5. Security Awareness and Training.

Apttus has developed a mandatory security awareness and training program for all members of Apttus cloud service operations, which includes:

- (a) training on how to implement and comply with its Information Security Program; and
- (b) promoting a culture of security awareness through periodic communications from senior management with employees.

6. Scans and assessments.

6.1 Scans. In order to maintain the security of the Subscription Services, regular network and system scans are performed, including non-intrusive network scans on customer-facing infrastructure.

6.2 Assessments. Apttus utilizes external service providers to perform an application vulnerability assessment biannually.

6.3 Patching. A software patching process is in place to remedy vulnerabilities in a timely manner based on scans and assessments.

6.4 Summary. A summary of the results of the most recent vulnerability assessments will be made available to Customer upon request.

7. Security incidents and response. Apttus has a response plan that includes procedures to be followed in the event of a Security Incident, including:

- (a) **Formation** of an internal incident response team assessing the risk the incident poses and determining who may be affected, and mitigate additional risk or impact;
- (b) **Notification.** Internal reporting as well as Customer notification in the event of unauthorized disclosure of Customer Data in accordance with the Agreement;
- (c) **Recordkeeping.** Customer Data is managed according to the Agreement (including this Data Security Exhibit).
- (d) **Audit.** Conducting and documenting root cause analysis and remediation plans.

8. Contingency Planning / Disaster Recovery.

Customer Data stored for the purposes of assuring availability or recoverability in the event of a disaster is maintained with the same data security standards as Customer Data in production environments.

Recovery Time Objective ("RTO") is Apttus' objective for the maximum period of time between Apttus' decision to activate the disaster recovery processes to failover the Subscription Services to a secondary site due to a declared disaster, and the point at which our customers can resume production operations at a secondary site. If the decision to failover is made during the period in which an upgrade is in process, the RTO extends to include the time required to complete the upgrade. The RTO is 24 hours.

Recovery Point Objective ("RPO") is APTTUS' objective for the maximum period of data loss measured as the time from which the first transaction is lost until Apttus' declaration of the disaster. The RPO does not apply to any data loads that are underway when the disaster occurs. The RPO is 4 hours.

9. Audit Controls.

Hardware, software and/or procedural mechanisms are maintained to record and examine activity in information systems that contain or use electronic information, including appropriate logs and reports concerning these security requirements.

10. Portable media.

Apttus does not store Customer Data on desktops, laptops or other removable storage devices which are housed outside of a secured data center.

11. Secure Disposal.

Upon Customer request, Apttus will dispose of tangible property containing Customer Data, using available technology, such that Customer Data cannot be practicably read or reconstructed.

12. Testing. Apttus will periodically test and evaluate the key controls and operations against relevant compliance frameworks to validate that they are properly implemented and effective in addressing the threats and risks identified.

13. Monitoring.

Apttus will monitor network and production systems, including error logs on servers, disks and security events for any potential problems, including:

- (a) reviewing changes affecting systems handling authentication, authorization; and
- (b) reviewing User and privileged (e.g. administrator) access to Apttus production systems.

14. Change and Configuration Management.

Apttus will maintain policies and procedures for managing changes to production systems, applications, and databases, including:

- (a) a process for documenting, testing and approving the promotion of changes into production; and
- (b) acceptance testing and approval processes specifically related to standard bug fixes, updates, and upgrades made available for the Subscription Services.

15. Background Checks.

Apttus shall perform background checks for its employees who will have access to Customer Data. Such background checks shall include:

- (a) for all employees, a criminal record search for previous seven years;
- (b) for U.S.-based employees, verification of social security number for previous five years; and
- (c) verification of eligibility to lawfully work in the United States (or applicable country).

16. HIPAA.

If Apttus processes Protected Health Information (“PHI”), as defined in the Health Insurance Portability and Accountability Act (“HIPAA”) and its implementing regulations, as amended, on behalf of Customer, Apttus

shall, in addition to the obligations set forth in this Agreement, (i) enter into a form of Business Associate Agreement; and (ii) make its internal practices, books and records relating to the use and disclosure of PHI available to the U.S. Department of Health and Human Services, as may be required by HIPAA.

17. PCI DSS (Payment Card Industry Data Security Standard).

If Apttus will process any payment card information from or on behalf of Customer, the following terms apply: Apttus shall at all times comply with the then-current PCI DSS and any similar data security standards that may be imposed by federal, state or local law. Apttus will have an annual assessment performed by a qualified security assessor certified by the PCI Security Standards Council. Upon request by Customer, Apttus will provide Customer with a PCI Attestation of Compliance or such other documentation as reasonably requested by Customer to evidence Apttus' continuing compliance.