This Data Security Exhibit ("**Exhibit**") applies in addition to any existing Master Services Agreement, similar subscription agreement, or End User License Agreement (collectively, the "**Agreement**") between Apttus Corporation ("**Conga**") 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.

Conga 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 Conga 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 Subscription Services purchased under the Agreement 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 Conga 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**" means 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.

Conga agrees to maintain a data security program that includes 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 Conga for the Subscription Services will be subject to annual certification of compliance with ISO 27001 and SOC 2 Type 2 standards.

2.1 Risk Assessment and Treatment.

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

2.2 Access Controls.

(a) Conga Personnel's access to data processing systems is only granted to authenticated users based on a role-based authorization concept using the following measures: Data encryption, individualized password assignment (at least 8 characters, regular automatic expiration), employee ID cards, password-protected screen savers in case of inactivity, intrusion detection systems and intrusion-prevention systems, and regularly updated antivirus and spyware filters in the network and on the individual PCs and mobile devices.

(b) Conga's provisioning process requires Conga Personnel to change the authentication method upon initial login. Access revocation for Conga Personnel is conducted upon termination or role change. Conga Personnel role changes resulting in additional access require VP or above approval. Conga uses the least privilege model to ensure access is granted on an approved need to perform job functions. Conga reviews access quarterly.

(c) Conga employs managed firewalls to control access and allow only authorized traffic to Conga infrastructure. In addition, Conga employs security controls to manage ingress and egress of data based upon protocol, port, source and destination within the environment. Any traffic not adhering to these strict access controls is discarded at the Internet boundary. Internally at Conga, host-based intrusion detection and monitoring systems are deployed at the server and network layers, respectively.

(d) Customer has the ability to limit access to the Subscription Services to authorized Customer Personnel to prevent unauthorized access to Customer Data, including through the use of multifactor authentication.

(e) Subscription Service access logs are maintained.

2.3 Encryption. All Customer Data, including Personal Data, is encrypted at rest and, in transit, using TLS encryption technology. TLS connections are negotiated for at least 256-bit encryption or stronger.

2.4 Conga Restrictions. Conga 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 Customer Data, to any person.

2.5 Backups. Conga performs daily backups of Customer Data and retains such data for thirty (30) days. However, for Subscription Services hosted on the Salesforce Platform, Conga does not backup Customer Data due to the nature of such Subscription Services and the Salesforce Platform, provided Customer may extract Customer Data from the Salesforce Platform to perform its own backups.

2.6 Physical Security of Data Centers. Buildings are protected with appropriate access control systems, based on a security classification and an appropriately defined access authorization concept. Buildings are secured by access control measures using a card reader system. Depending on the security category, property, buildings or individual areas are secured by additional measures such as special access profiles, separation locks, video surveillance and security personnel. Access rights for authorized persons are granted individually according to defined criteria. This also applies to external persons.

3. Compliance with Laws.

3.1 Regulatory Cooperation. If Conga 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, Conga agrees to assist and cooperate to meet any obligation to the relevant regulatory authority.

3.2 Right of Access. Conga 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 Conga is required by any Law to disclose any Customer Data, Conga 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.

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

(i) training on how to implement and comply with its information security program; and

(ii) promoting a culture of security awareness through periodic communications from senior management with employees.

(b) All Conga employees are required to complete security and privacy awareness training as part of onboarding and on an ongoing annual basis and must agree to Conga's privacy and confidentiality requirements.

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. Conga utilizes external service providers to perform an application vulnerability assessment biannually and application penetration test annually.

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

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

7. Security incidents and response. Conga has a rigorous incident management process for security events that may affect the confidentiality, integrity, or availability of systems or data. If an incident occurs, the security team logs and prioritizes it according to its severity. Events that directly impact customers are assigned the highest priority. This process specifies courses of action, procedures for notification, escalation, mitigation, and documentation. Key staff are trained in forensics and handling evidence in preparation for a Security Incident, including third-party and proprietary tools. To help ensure the swift resolution of Security Incidents, the Conga security team is available 24/7 to all Conga employees. Conga has a response plan that includes procedures to be followed in the event of a Security Incident, including 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.

(a) **Notification**. Internal reporting as well as Customer notification in the event of unauthorized disclosure of Customer Data in accordance with the Agreement. Conga will coordinate communication between Conga technical support and the Customer points of contact Conga has on record.

(b) **Recordkeeping**. Customer Data is managed according to the Agreement (including this Data Security Exhibit).

(c) **Audit**. Conducting and documenting root cause analysis and remediation plans.

8. Contingency Planning / Disaster Recovery.

(a) Excluding components of the Subscription Services operated by Salesforce.com, Inc., Conga infrastructure and, where applicable, Customer Data, are maintained and stored for the purposes of assuring availability or recoverability in the event of a disaster are maintained on redundant systems with the same data security standards as in production environments. Availability and resilience of systems and services are ensured by isolating critical IT and network components, by providing adequate backup and redundancy systems, using power redundancy systems, and regularly testing of systems and services. Test and live systems are kept completely separated.

(b) The availability of and access to Personal Data in the event of a physical or technical incident shall be restored by taking the following measures: Personal data is stored in RAID systems and integrates redundant systems according to security marking. Systems for uninterruptible power supplies (e. g. UPS, batteries, generators) are used to secure the power supply in the used data centers. Additionally, databases or data centers are mirrored in different physical locations.

(c) Recovery Time Objective (“**RTO**”) is Conga’s objective for the maximum period of time between Conga’s 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 twenty-four (24) hours.

(d) Recovery Point Objective (“**RPO**”) is the objective for the maximum period of data loss measured as the time from which the first transaction is lost until Conga’s declaration of the disaster. The RPO is one (1) hour. There is no RPO associated with the Subscription Services. However, for Subscription Services hosted on the Salesforce Platform, there is no RPO due to the Subscription Services and the Salesforce Platform.

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.

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

12. Testing. Conga 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.

Conga 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 auditing; and

(b) reviewing User and privileged (e.g. administrator) access to Conga production systems.

14. Change and Configuration Management.

Conga has a well-defined System Development Life Cycle (SDLC) methodology that governs the application development and change management process. Conga enforces that the SDLC policies and procedures are reviewed annually and are updated on an as-needed basis to reflect changes in the operating environment. Further, Conga 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.

Conga 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 Conga 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, Conga 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.