Security Schedule to the Boomi Master Services Agreement

This Security Schedule ("Schedule") to the Boomi Master Services Agreement ("Agreement") identifies a description of the technical, administrative and organizational security measures (the "Security Practices") employed by Boomi for the protection of Customer data, including Personal Data submitted by Customer to the applicable Boomi Services, as that term is defined in the Agreement. Capitalized terms not defined herein shall have the meaning set for in the Agreement.

1. Security Practices and Procedures.

1.1 Boomi has implemented and maintains Security Practices that are designed to ensure the ongoing confidentiality, integrity, availability, and resilience of information and processing systems. The Security Practices address: (a) information and data security, privacy, and protection; (b) system and asset management; (c) development and maintenance (such as anti-malware, patch/vulnerability management, and network security); (d) production/implementation (such as identification, authentication, authorization, passwords, and remote access); (e) governance (including classification); (f) physical security of people and assets, and (g) information security practices and standards that are designed to protect the confidentiality, integrity, and availability of Boomi's information and computing environment from a wide range of threats, and in order to minimize business impacts. These Security Practices are reviewed and approved by Boomi's chief security officer or his/her delegates on a regular basis. Boomi reserves the right to revise this Schedule, including the policies and procedures set forth herein, from time to time.

1.2 Boomi maintains information Security Practices that (a) leverage guidance from applicable recognized information security frameworks, (b) include administrative, technical and physical safeguards reasonably designed to protect the confidentiality, integrity, and availability of Boomi information, networks, and systems, and (c) are appropriate to the nature, size, and complexity of Boomi's operations.

1.3 Key features of the Security Practices include:

A. Implementing information security controls to address security risks and evaluating information security risks, taking into account the impact of threats and vulnerabilities, and.

B. Various risk management processes designed to ensure information security risks are addressed on an ongoing basis.

C. Audit practices prescribing the frequency, methods, responsibilities, planning requirements and reporting for each of the Boomi Services. As a part of the continual improvement process, Boomi relies on internal and external audit results as a means to measure the design and effectiveness of the information. The types of audits will depend on the applicable Boomi Service and may include SOC1, SOC2, HIPAA, PCI, FedRAMP and other industry assessments and certifications.

1.4 Boomi implements organizational and management controls to ensure the protection of systems processing Personal Data, including ensuring that any person authorized by Boomi to access or process Personal Data is subject to an obligation of confidentiality, screening/background checks on employees who have access to Personal Data in accordance with applicable law and Boomi policies, and mandatory training to employees accessing Personal Data ensure that they understand their obligations and responsibilities in complying with Boomi security policies.

1.5 Boomi participates, from time to time, in industry-accepted security assessments such as the Consensus Assessments Initiative Questionnaire (CAIQ), which offers an industry-accepted means of documenting security controls in IaaS, PaaS, and SaaS service, providing security control transparency. The CAIQ, or other relevant document based on the nature of the applicable Boomi Service, is reviewed periodically for the Boomi AtomSphere™ Platform, mapped to Boomi policies and standards, and updated with relevant and current US and international regulatory and privacy standards, where applicable. The CAIQ, or other relevant document, provides Boomi's customers with an industry standard assessment, using a robust compilation of questions targeted to gathering pertinent information to determine how cybersecurity, IT, operating and data security risks are managed across a broad spectrum of risk control areas within the Boomi environment. Boomi's responses to the CAIQ, or comparable forms of information gathering, are for informational purposes only and are intended to provide more detailed information regarding the controls outlined in this document. The CAIQ, or its equivalent, however is not intended to modify or amend the terms and conditions of the Agreement or this Schedule. Boomi makes no representations or warranties of any kind, written, oral, express, implied or otherwise, with respect to the responses contained therein. Upon prior written request from Customer to Boomi, not more than once per any twelve (12) month period, Boomi agrees to provide Customer with a copy of its then most-recent version of the CAIQ, or comparable document including additional Boomi security & compliance documents, such as AtomSphere Security Standards, SOC, and/or third-party web application penetration testing, provided a current Non-Disclosure Agreement exists between Customer and Boomi.

1.6 With regard to any product purchased or licensed from Boomi, there may be supplemental or additional security assurances that may apply to such product if expressly stated in your contract or signed order documents, provided that in the event of a conflict between this Schedule and any statement in such assurances, this Schedule shall supersede the other assurances. No statements outside of a formal warranty statement on Boomi's web page(s), or a signed writing from an officer of Boomi, shall be binding.

1.7 Certain Boomi Services allow Customers to manage and change aspects of the security configurations and protocols, so that each Customer may control (a) access to its data, (b) where data is hosted, (c) support privileges, and (d) the time within data is stored and/or purged, allowing each Customer to customize the security of the Boomi Services for their unique use case. Boomi will process Customer Data in accordance with Customer's configuration and/or documented instructions.

1.8 Deletion of Personal Data. Upon termination of the Services, if Customer requests in writing, Boomi will as soon as reasonably practicable, delete the Personal Data on Boomi systems, subject to applicable legal requirements and to the extent the data or copies thereof can reasonably and practically be expunged. In all events, each Customer controls the duration of Boomi's temporary retention of logs and certain processed documents and may choose, at their discretion, to reduce the number of days that logs, processed documents, and temporary data is maintained from the default thirty (30) days (or fourteen (14) for Boomi Atom cloud).

1.9 In all events, Customers are responsible for ensuring that their own system configurations, data deletion schedules, access to passwords, contractor and personnel actions and decisions are aligned to the Customer's security needs and policies. Boomi may send data where directed by Customer and may comply with the configuration and data access as implemented by Customer.

2. **Organizational Security, Risk Management and Incident Response.**

2.1 To facilitate corporate adherence to Boomi's Security Practices, Boomi's security organization collaborates with representatives throughout Boomi to provide strategy, support, and guidance for the following non-exhaustive activities and practices:

A. Establishing security policies, practices, standards and regulations, awareness and education, risk assessments and management, contract security requirements management, application and infrastructure consulting, assurance testing and managing the security direction of the company;

B. Development of security testing and design and implementation of security solutions designed to enable security controls adoption across the environment;

C. Managing operations of implemented security solutions, the environment, and incident response; and

D. Overseeing forensic investigations with key stakeholders, including legal, privacy, and human resources.

2.2 Boomi maintains a risk management process to frame, assess, respond to, and monitor risk, consistent with applicable contractual and legal obligations. Boomi performs periodic risk assessments of its environment and systems to understand the risks and apply appropriate controls to manage and mitigate such risks. Threat and vulnerability assessments are periodically reviewed, and remediation actions are taken if material weaknesses are found.

2.3 Boomi assesses risks associated with third-party Subprocessors that host Customer Data through ongoing risk management practices. This process includes a risk-based approach to Subprocessor relationships that accounts, as applicable, for areas such as physical security, data access, network connectivity, and compliance impact.

2.4 Boomi maintains incident detection and response practices, which utilize tools and technologies to help manage and mitigate incidents. Incident response practices exist for security and data protection incidents, which address the measures that Boomi will take in the event of an incident affecting the security of a Boomi facility or Boomi system used by Boomi in connection with the provision of services, and may include procedures for incident analysis, containment, response, remediation, reporting, and the return to normal operations.

3. Communications and Operations Management: Boomi manages changes to its corporate infrastructure, systems, and applications through policies, procedures, and tools to govern such changes, to ensure that they undergo the appropriate reviews, approvals, and to communicate effectively to Boomi personnel and other applicable users. To protect against malicious use of assets and malicious software, additional controls may be implemented, based on risk. Such controls may include information security practices and standards; restrictive access controls; separate development and test environments; malware detection on servers, desktops and notebooks; malware email attachment scanning; system compliance scans; intrusion detection monitoring and response; logging and alerting on key suspicious events; information handling procedures based on data type, application and network security; use of external assets; and system and application vulnerability scanning.

4. Asset and Information Classification and Control.

4.1 Boomi has implemented and maintains policies to assure that assets are provisioned and monitored by Boomi during their lifecycle until depreciated and returned. Assets are accounted for, have a designated owner and are documented through Boomi's asset management policies.

4.2 Any asset security and resiliency requirements are determined based on business criticality and/or data classification sensitivity. Industry guidance for handling critical and sensitive information provides the framework for technical, organizational and physical safeguards. These may include controls such as access management, encryption, logging and monitoring, and data destruction.

5. Access Controls.

5.1 Boomi implements appropriate access controls designed to protect against unauthorized access to Boomi information, networks, and systems. To reduce the risk of misuse, intentional or otherwise, access is controlled following the principles of "least privilege" and "need to know". Access controls Boomi may utilize include access reviews, maintenance of service accounts and privileged access to the applications, system level settings for access, and the generation of access-related reports.

5.2 Boomi utilizes industry standard practices to identify and authenticate Boomi users who attempt to access Boomi information, networks, or systems. Boomi requires the use of strong passwords across all Boomi systems and networks. Boomi Security Practices (a) prohibit Boomi users from sharing, writing down, emailing, IM'ing, or storing passwords unencrypted on any Boomi system, and (b) lock accounts after a series of consecutive incorrect password attempts.

5.3 Boomi utilizes industry standard practices to enhance access controls, which, pending the applicable Boomi Service, may include (a) automatic time-out of user terminal if left idle, identification and password required to reopen, (b) protection against external access by means of accepted industry standard firewall(s) whose connection to the intranet, if applicable, is safeguarded by a VPN connection; (c) masking of passwords when displayed or entered, as appropriate; and (d) appropriate and industry standard password encryption when transmitted.

6. **Infrastructure Development and Maintenance:** Boomi maintains threat and vulnerability management practices to monitor for vulnerabilities on an on-going basis. Vulnerabilities are identified using a variety of sources/methods which, pending the nature of the Boomi Services purchased, may include vulnerability scans, penetration tests, and employee, customer, and external reporting. Publicly released third-party vulnerabilities are reviewed for applicability in the Boomi environment. Vulnerability remediation timeframes are calculated based on risk. Vulnerability scans and assessments are routinely and regularly performed on Boomi's application infrastructure. External-facing applications, and internal assets that are deemed by Boomi to be high-risk are scanned and penetration tested at Boomi's discretion. Code reviews and vulnerability assessments are used in the development environment prior to release to production to proactively detect and remediate vulnerabilities where deemed appropriate by Boomi. These processes are designed to enable proactive identification and remediation of vulnerabilities as well as support Boomi's compliance and regulatory requirements. These practices are in place in support of appropriate reviews and authorizations prior to implementing any new technologies or changes within the production environment of the Boomi Services.

7. **Software Development, Maintenance and Vulnerability Response.**

7.1 Minimizing the risk associated with security vulnerabilities in the Boomi Services is a corporate responsibility and directly aligns with Boomi's core values. Boomi has implemented and maintains practices to define the steps that must be taken to ensure that all Boomi Services have been appropriately assessed and developed. These practices, in concert with Boomi's Security Practices, help to address security throughout the development and maintenance lifecycle of the Boomi Services. Boomi employs a rigorous process to continually evaluate and improve its secure development and vulnerability response practices, and Boomi regularly compares these against industry practices.

7.2 Boomi uses commercially reasonable efforts to design and implement vulnerability response processes to identify and address vulnerabilities, including providing and applying security updates and/or other corrective actions for its products, as applicable. After investigating and validating a reported vulnerability, Boomi will attempt to develop and qualify an appropriate remedy for products that are under active support from Boomi in accordance with Boomi's vulnerability response practices.

7.3 Where applicable, Boomi will remedy a reported vulnerability in one or more of the following forms: (a) a new release of the affected product or service provided by Boomi; (b) a Boomi-provided patch that can be installed on top of the affected product or service; (c) instructions to download and install an update or patch from a third-party vendor that is required for mitigating the vulnerability; or (d) a corrective procedure or workaround published by Boomi that instructs users in adjusting the product or service configuration to mitigate the vulnerability.

7.4 Boomi will communicate remedies to customers where applicable. Boomi will include the following information as applicable: (i) products, services, and versions affected; (ii) vulnerability severity rating leveraging industry standard rating systems; (iii) description of the vulnerability and potential impact; and (iv) remedy details with update and workaround information.

7.5 Boomi strives to provide the remedy or corrective action in a commercially reasonable time. Response timelines will depend on many factors, such as: the severity, the remedy complexity, the component or portion of the product or service affected (for example, some updates require longer validation cycles or can only be updated in a major release), the stage of the product or service within its lifecycle, etc.

8. **Compliance and Trust.**

8.1 Boomi follows a comprehensive set of practices and standards to manage security and resiliency risks, to comply with applicable laws and regulations, and address the protection of customer personal information, and data protection and data handling procedures.

8.2 Mechanisms such as the security and resiliency practices, internal and external audits/assessments, legal counsel and/or privacy consultation, internal controls assessment, internal and third-party penetration testing and vulnerability assessments, contract management, security awareness and compliance training, security consulting, policy exception reviews and risk management all combine to drive compliance with these requirements.

9. Personnel Security.

9.1 As part of the employment process, Boomi employees are required to undergo a screening process subject to and consistent with applicable law. Although Boomi reserves the right to review its policies and implement personnel security within its sole discretion, under current policy and subject to local law and local availability, Boomi conducts one or more of the following screenings for employment: drug screening, Social Security trace, criminal records search, education and employment verification, and employment eligibility verification. Boomi attempts to meet current industry standards for like companies in Boomi's industry, but Boomi cannot map its personnel security or screening process to meet the specific expectation of a particular Customer.

9.2 Third parties or outside contractors are either screened by Boomi, screened as a condition of the contract, or verified as screened by the contractor following a Boomi-approved screening process. Boomi requires its personnel to comply with Boomi Security Practices and maintains a disciplinary process to take action against personnel that do not comply with Boomi Security Practices, including but not limited to, those put in place to meet its security, availability and confidentiality commitments and requirements. Boomi provides security awareness training to all applicable Boomi personnel.

9.3 Boomi ensures that persons authorized to access Customer Personal Data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality, and access the data only upon instructions from Boomi, unless required to do so by applicable law.

10. Corporate and Physical Security: Physical and environmental security controls are in place to guard against unauthorized physical access, damage and interference to Personal Data. Boomi or Boomi's third-party data hosting and cloud IT Subprocessors adhere to various technological and operational approaches in their physical security program in regard to risk mitigation. Physical access of Boomi facilities, for example, is restricted to authorized personnel and physical controls are in place to protect the confidentiality, integrity, and availability of Boomi's data and computing environments from a wide range of threats and to ensure business continuity, minimize business impacts and maximize return on investment and business opportunities. Access controls may include, but are not limited to, security logs, monitoring, alarms, limited access to secure areas, protection of access paths, video surveillance, key cards, and two-factor authentication. Boomi works closely with each of its sites and Subprocessors to determine and confirm that appropriate security measures are in place based on the specific jurisdiction and continually monitors any changes and risks to the physical infrastructure, business, and known threats. Boomi balances its approach towards security by considering elements of control that include architecture, operations, and systems

11. Business Continuity and Disaster Recovery: Boomi maintains business continuity practices designed to enable Boomi to fulfill its obligations under the Agreement specifically in the case of a business interruption caused by the material loss of operational resources due to a natural or man-made event. Boomi will make reasonable attempts, under the circumstances, to timely contact Customer in the event of a business interruption that materially impacts Customer.

12. Compliance: Boomi will, upon written request no more than once per year, certify to its compliance with this Schedule.