MEDALLIA MASTER SUBSCRIPTION AGREEMENT - SECURITY MEASURES

Medallia maintains and manages a comprehensive written security program designed to protect: (a) the security and integrity of Client Data; (b) against threats and hazards that may negatively impact Client Data; and (c) against unauthorized access to Client Data. Medallia's security program includes the following:

1. **Risk Management**
   - **a.** Conducting an annual risk assessment designed to identify threats and vulnerabilities in the administrative, physical, legal, regulatory, and technical safeguards used in the Medallia Products.
   - b. Maintaining a documented risk remediation process to assign ownership of identified risks, establish remediation plans and timeframes, and provide for periodic monitoring of progress.

2. **Information Security Program**
   - a. Maintaining a documented comprehensive information security program. This program will include policies and procedures aligning with industry best practices, such as ISO 27001/27002.
   - b. Such information security program shall include, as applicable: (i) adequate physical security of all premises in which Client Data will be processed and/or stored; (ii) reasonable precautions taken with respect to Medallia personnel employment; and (iii) an appropriate network security program.
   - c. These policies will be reviewed and updated by Medallia management annually.

3. **Organization of Information Security**
   - a. Assigning security responsibilities to appropriate Medallia individuals or groups to facilitate protection of the Medallia Products environment and associated assets.
   - b. Establishing information security goals to be met.

4. **Human Resources Security**
   - a. Medallia employees undergo comprehensive screening during the hiring process. Background checks and reference validation will be performed to determine whether candidate qualifications are appropriate for the proposed position. Subject to any restrictions imposed by applicable law and based on jurisdiction, these background checks include criminal background checks, employment validation, and education verification as applicable.
   - b. Ensuring all Medallia employees are subject to confidentiality and non-disclosure commitments before access is provisioned to Medallia Products and/or Client Data.
   - c. Ensuring applicable Medallia employees receive security and privacy awareness training designed to provide such employees with information security knowledge to provide for the security, availability, and confidentiality of Client Data.
   - d. Upon Medallia employee separation or change in roles, Medallia shall ensure any Medallia employee access is revoked in a timely manner and all Medallia assets, both information and physical, are returned.

5. **Asset Management**

a. Maintaining asset and information management policies and procedures. This includes ownership of assets, an inventory of assets, classification guidelines, and handling standards pertaining to Medallia assets.

b. Maintaining media handling procedures to ensure media containing Client Data is encrypted and stored in a secure location subject to strict physical access controls.

c. When a storage device has reached the end of its useful life, procedures include a decommissioning process that is designed to prevent Client Data from being exposed to unauthorized individuals using the techniques recommended by NIST to destroy data as part of the decommissioning process.

d. If a hardware device is unable to be decommissioned using these procedures, the device will be virtually shredded, degaussed, purged/wiped, or physically destroyed in accordance with industry-standard practices. Devices used in the administration of the Medallia Products that have been decommissioned will be subjected to these or equally effective standards.

6. Access Controls

a. Maintaining a logical access policy and corresponding procedures. The logical access procedures will define the request, approval, and access provisioning process for Medallia personnel. The logical access process will restrict Medallia user (local and remote) access based on the principle of least privilege for applications and databases. Medallia user access recertification to determine access and privileges will be performed periodically. Procedures for onboarding and off-boarding Medallia personnel users in a timely manner will be documented. Procedures for Medallia personnel user inactivity threshold leading to account suspension and removal threshold will be documented.

b. Limiting access to Client Data to its personnel who have a need to access Client Data as a condition to Medallia's performance of the services under this Agreement. Medallia shall utilize the principle of "least privilege" and the concept of "minimum necessary" when determining the level of access for all Medallia users to Client Data. Medallia shall require strong passwords subject to complexity requirements and periodic rotation.

7. **System Boundaries**

a. The systems that compose a functioning Medallia cloud platform for the Products are limited to shared components such as network devices, servers, and software that are physically installed and operating within Medallia's Internet-enabled network infrastructure. This system boundary also includes the network connectivity, power, physical security, and environmental services provided by the third-party provider that owns and operates the

b. Medallia is not responsible for any system components that are not within this system boundary, including network devices, network connectivity, workstations, servers, and software owned and operated by the Client or other third parties. Medallia may provide support for these components at its reasonable discretion.

8. Encryption

a. Client maintains ownership of the encryption all Client Data uploaded to their Products through the full lifecycle period. Client Data may be uploaded via SFTP, TLS/SSL, or through an Medallia services API over a TLS/SSL connection to the Medallia cloud platform. Medallia will configure TLS and/or SSL certificates.
b. Client Data shall be encrypted at rest at the storage-level.

9. Physical and Environment Security

a. Medallia products and Client data are hosted at providers who have demonstrated compliance with one or more of the following standards (or a reasonable equivalent): International Organization for Standardization ("ISO") 27001 and/or American Institute of Certified Public Accountants ("AICPA") Service Organization Controls ("SOC") Reports for Services Organizations. These providers provide Internet connectivity, physical security, power, and environmental systems and services for the Medallia cloud platform used for the Products.
b. An N-tiered architecture is used to support presentation, application, processing, and data services. For enhanced security in the Medallia cloud platform, technologies such as firewalls, intrusion detection and prevention, and vulnerability management are used.

10. Operations Security

a. Maintaining documented Medallia cloud operating procedures.
b. Maintaining change and release management controls to ensure changes to products production systems made by Medallia are properly authorized and reviewed prior to implementation.
c. Monitoring usage, security events, and capacity levels within the Medallia cloud to manage availability and proactively plan for future capacity requirements.

d. Utilizing virus and malware protection software a, which are configured to meet common industry standards designed to protect Medallia systems and Client Data from virus infections or similar malicious payloads.
e. Implementing disaster recovery and business continuity procedures. These will include periodic replication of Client Data to a secondary data center in a geographically disparate location from the primary data center.
f. Maintaining a system and security logging process to capture critical system logs. These logs shall be maintained for at least six months and reviewed on a periodic basis.
g. Ensuring systems processing and storing Client data are appropriately configured and hardened.
h. Ensuring servers, operating systems, and supporting software used in the Medallia cloud for Products receive Critical and High security patches within a timely manner, In the event any such security patch would materially adversely affect the Products, then Medallia will use commercially reasonable efforts to implement compensating controls until a security patch is available that would not materially adversely affect the Products.
i. Conducting third-party external application penetration tests periodically.

11. Supplier Relationships

a. Maintaining a Vendor Management Program to evaluate and mitigate risks for any third parties that host or process Client data.

12. Security Incident

a. Employing incident response standards that are based upon applicable industry standards, such as ISO 27001:2013 and National Institute for Standards and Technology ("NIST"), or equivalent in order to maintain the information security components of the Products environment.
b. Responses to these incidents follow the Medallia documented incident response sequence. This sequence includes the incident trigger phase, evaluation phase, escalation phase, response phase, recovery phase, de-escalation phase, and post incident review phase.
c. Medallia will notify Client of a Security Incident as required pursuant to applicable law but in no event later than 72 hours after a Security Incident. A "**Security Incident**" means a determination by Medallia of an actual disclosure of unencrypted Client Data to an unauthorized person or entity.

13. Information Security Aspects of Business Continuity Management

a. Maintaining a business continuity and disaster recovery plan.
b. Reviewing and testing this plan annually.