Medallia

MASTER SUBSCRIPTION AGREEMENT

This Medallia Master Subscription Agreement (the "**Agreement**") is effective as of the last day of signature on an Order (the "**Effective Date**") and is between Medallia, Inc. ("**Medallia**") and the other signatory to an Order ("**Customer**"). Medallia provides experience management products (the "**Medallia Products**"). This Agreement establishes the terms and conditions for the purchase and provision of subscriptions to Medallia Products ("**Software Subscriptions**") and related professional services provided by Medallia ("**Professional Services**").

1. ORDERS

a. General

This Agreement does not itself obligate the parties to purchase or provide Software Subscriptions or Professional Services. Such obligations will be documented in ordering documents that describe the Software Subscription or Professional Services scope and the related fees (an "**Order**"). An explicit conflict between these agreements will be resolved according to the following order of precedence: (1) an Order; and (2) this Agreement.

2. PROVISION OF MEDALLIA PRODUCTS

Medallia will make Medallia Products available to Customer through the web browsers and mobile applications specified on the Order and will maintain the hardware and software necessary to do so. Medallia's service level agreements will be as set forth in the applicable product and services descriptions (the "**Documentation**"). Medallia will provide Customer with access to every product improvement consistent with the scope established in the Order, when and if generally available.

3. MEDALLIA PRODUCTS AND PROFESSIONAL SERVICES WARRANTY

a. Express Warranties

Medallia Products will perform in a manner consistent with the Documentation, this Agreement and Order(s) (the "**Solution Warranty**"). Professional Services will be provided in a true and workmanlike manner, consistent with this Agreement and the Order (the "**Services Warranty**").

b. Remedy for Failure of the Solution Warranty

Upon receipt of written notice of a Solution Warranty breach, Medallia will provide a correction at no charge. If Medallia cannot correct the breach within forty-five days from receipt of the warranty notice, then Customer may terminate the affected Order at any time within the next thirty days and receive: (i) if the breach notice was received fewer than ninety days after the Effective Date, a refund of all subscription fees paid; or (ii) if the notice was received at any other time, a prorated refund of subscription fees from the date of the warranty notice. This is Customer's sole and exclusive remedy for a breach of the Solution Warranty.

c. Remedy for Failure of the Professional Services Warranty

Upon receipt of written notice of a Services Warranty breach, Medallia will re-perform the Professional Services as necessary to correct the breach. If Medallia cannot correct the breach within forty-five days from receipt of the warranty notice, then Customer may terminate the affected portion of the Order at any time within the next thirty days and receive a refund of Professional Services fees paid for nonconforming or unperformed Professional

Services. This is Customer's sole and exclusive remedy for a breach of the Professional Services Warranty.

d. Disclaimer of Other Warranties

EXCEPT AS EXPRESSLY PROVIDED HEREIN, AND TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, MEDALLIA PROVIDES MEDALLIA PRODUCTS AND PROFESSIONAL SERVICES "AS IS," MAKES NO WARRANTY OF ANY KIND EXPRESS OR IMPLIED WITH REGARD TO MEDALLIA PRODUCTS OR PROFESSIONAL SERVICES, AND DISCLAIMS ALL OTHER WARRANTIES, SUCH AS: (I) WITHOUT PREJUDICE TO CUSTOMER'S RIGHT TO SERVICE CREDITS FOR A FAILURE TO MEET MEDALLIA'S UPTIME COMMITMENTS, ANY WARRANTY THAT MEDALLIA PRODUCTS AND PROFESSIONAL SERVICES WILL BE ERROR FREE OR UNINTERRUPTED; AND (II) THE IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, TITLE, AND NON-INFRINGEMENT.

e. Beta Services

From time to time, Customer may have the option to participate in early access programs to use alpha or beta services, products, features and documentation ("**Beta Services**") offered by Medallia. These Beta Services are not generally available and may contain bugs, errors, or defects. Accordingly, Medallia provides the Beta Services to Customer "as is" and makes no warranties of any kind with respect to the Beta Services, nor does any Medallia service level agreement apply to the Beta Services. Medallia may discontinue Beta Services at any time in its sole discretion and may never make them generally available.

4. USE OF MEDALLIA PRODUCTS

a. General Obligations

Other than using Medallia Products and its functionalities under an Order, Customer may not copy, modify, distribute, sell, or lease any part of Medallia Products or included software, or reverse engineer or attempt to extract the source code of that software, unless laws prohibit those restrictions. Customer may not use Medallia Products functionality to infringe upon the intellectual property rights of others, or to commit an unlawful activity.

b. Compliance Obligations

Customer will access Medallia Products only for its internal business purposes and will use industry standard practices to restrict the unauthorized use of Medallia Products credentials. If Customer delivers data to Medallia (e.g., names and contact information for consumers), Customer will be responsible for ensuring that such use is allowed under the laws, regulations, and agreements applicable to Customer. This responsibility includes for example: (i) complying with Customer's obligations as a data controller; (ii) ensuring that Customer's privacy policy allows for the delivery of such data to Medallia and its use as disclosed to Customer by Medallia; (ii) securing and maintaining any required consents; (iii) ensuring the validity of any customer contact information provided to Medallia; and (iv) timely informing Medallia of opt out requests received after delivery of the data. Customer shall not configure Medallia Products to collect bank account numbers, payment card or credit card information, bank transaction information, government identification numbers including (but not limited to) social security numbers, state identification numbers, and passport numbers, and sensitive personal information including (but not limited to) religious beliefs, health, sexual orientation, race, and union membership and Medallia will not be liable for non-compliance under laws and regulations that applies to the processing of the foregoing categories of data.

c. Third Party Services

If Customer integrates, or directs Medallia to integrate, Medallia Products with any third party service (e.g., another Customer-managed software solution) Customer acknowledges that such third party service might access or use Customer Data and Customer permits the third party service provider to access or use Customer Data. Customer is solely responsible for the use of such third party services and any data loss or other losses it may suffer as a result of using any such services. If Customer uses any third party service or uses Medallia Products to link or direct online traffic to third-party websites, Customer

shall ensure that such use complies with the terms of use of those third party services.

5. Ownership and Use Rights

a. Customer Data

Customer owns all data delivered to Medallia by Customer or collected by Medallia on behalf of Customer (the "**Customer Data**"). Customer grants Medallia a non-exclusive, worldwide, limited license to the Customer Data for the purposes of: (i) providing and improving Medallia Products and Professional Services; and (ii) developing and publishing broadly applicable experience management insights (such as industry experience management benchmarks, if applicable, provided that only aggregated or de-identified Customer Data is used).

b. Medallia Products

Medallia owns Medallia Products, including all features, functionalities, configurations, designs, templates, and other proprietary elements contained therein and all modifications, improvements, and derivative works thereof. Medallia will provide Customer with access to Medallia Products as described in the Order during the term of a Software Subscription for its internal business purposes. If Customer uses a Medallia API or software developer kit ("**SDK**"), Medallia grants Customer a non-exclusive, worldwide, limited license for use of such API or SDK for the purpose of enabling Customer to use Medallia Products. Customer will not remove, obscure, or alter Medallia's copyright notice, or other proprietary rights notices affixed to or contained within Medallia Products or any related documentation.

c. Documentation

Medallia owns the Documentation and all derivative works thereof. Medallia grants Customer a non-exclusive, worldwide limited license to use, copy, and make derivative works of the Documentation for internal business purposes during the term of a Software Subscription.

d. Trademarks

Customer grants Medallia a limited, non-exclusive license to mark Customer surveys and reports and Customer's instance of Medallia Products with Customer's trademarks, when requested by Customer and subject to Customer approval for consistency with its branding guidelines.

e. Reserved Rights

Customer and Medallia each reserve all intellectual property rights not explicitly granted herein.

6. Payments

a. Invoicing

Fees due for Software Subscriptions and Professional Services will be stated on the Order. Fees are non-cancelable and non-refundable other than as explicitly stated in this Agreement.

b. Taxes

Invoiced amounts are payable in full, without reduction for transaction taxes (e.g., value added taxes, consumption taxes, goods and services taxes, GST/HST, excise, sales, use or similar taxes, and withholding taxes). Customer is required to pay all such transaction taxes, either directly or by increasing payments to Medallia to offset taxes that Customer is required to deduct from payments. If Medallia has a legal obligation to pay or collect such transaction taxes, the appropriate amount will be invoiced to and paid by Customer, unless Customer provides Medallia with a valid tax exemption certificate.

7. Term and Termination

a. Term

The term of this Agreement is from the Effective Date through the last to expire Order.

b. Termination for Cause

Either party may terminate this Agreement or Order within thirty (30) days upon the occurrence of either of the following: (a) in the event the other party fails to cure any material breach of this Agreement or the relevant Order within thirty (30) days after receipt of written notice; or (b) if the other party files or has filed against it any bankruptcy or similar proceeding or enters into any form of arrangement with its creditors that is

not removed within 60 days of filing.

c. Transfer of Customer Data Upon Termination

Upon termination of this Agreement or an Order, Medallia will make customer feedback collected through and, at the time of termination, stored within Medallia Products available for secure download by Customer in a standard flat file format for at least thirty (30) days (the "**Data Transfer Period**"). Within sixty (60) days of the end of the Data Transfer Period, Medallia will remove all Customer Data from Medallia Products.

8. INSURANCE

Medallia will maintain insurance policies providing at least the following coverage and will provide a certificate of insurance upon request:

(i) Technology Errors & Omissions / Professional liability with a limit of at least $5 Million;

(ii) Cyber/Network and Information Security liability with a limit of at least $5 Million;

(iii) Commercial General liability with a limit of at least $1 Million;

(iv) Automobile liability with a limit of at least $1 Million;

(v) Workers Compensation and Employer's liability with a limit of at least $1 Million;

(vi) Umbrella liability with a limit of at least $10 million.

9. PRIVACY, SECURITY, AND AUDITS

a. Compliance with Data Protection Laws

In providing Medallia Products and Professional Services to Customer, Medallia shall comply with applicable legal requirements for privacy, data protection and confidentiality of communications. Such applicable legal requirements include the Standards for the Protection of Personal Information of Residents of the Commonwealth of Massachusetts (201 CMR 17.00), the California Consumer Privacy Act of 2018, and other applicable United States data protection laws at the state level, and implementing national legislation, and Regulation 2016/679 (also known as GDPR), if applicable.

Medallia is certified under the Privacy Shield to cover the transfer of data collected in the European Economic Area and Switzerland to the United States.

b. Data Protection Agreement

Medallia offers a data processing agreement that defines Medallia's and Customer's obligations under GDPR, and includes the EU's approved Standard Contractual Clauses for the handling of data collected in the European Economic Area and Switzerland outside of those areas. If Customer has a need for this agreement, Customer should please request it from Customer's Medallia account representative.

c. Product Specific Privacy and Security Obligations

The parties' product-specific privacy and security obligations are subject to the terms set forth in the applicable privacy and security addendum (and any DPA between the parties).

d. Security Incident Response

Upon becoming aware of any confirmed unauthorized or unlawful breach of security that leads to the destruction, loss, alteration, or unauthorized disclosure of or access to Customer Data (a "Security Incident"), Medallia shall notify Customer without undue delay. Medallia shall provide timely information relating to any Security Incident as it becomes known or as is reasonably requested by Customer. Medallia shall promptly take reasonable steps to mitigate and, where possible, to remedy the effects of any Security Incident.

e. General Performance Audits

Customer may, no more than once per year, audit Medallia's performance under this Agreement and each Order, and Medallia will maintain records sufficient for such audits, including service hours provided, uptime, and the results of security and disaster recovery tests.

f. Security Audits

As described in the applicable privacy and security attachment, Medallia is regularly audited by independent third parties and/or internal auditors. Upon request, Medallia shall supply (on a confidential basis) a summary copy of its audit report(s), if applicable, as well as written responses (on a confidential basis), not more than once per year, to all reasonable security and audit questionnaires that are necessary to confirm Medallia's compliance with this Agreement. Medallia shall permit Customer (or its appointed third party auditors) to carry out an audit of Medallia's processing of Customer Data under this Agreement following: (i) a confirmed Security Incident; or (ii) upon the instruction of a data protection authority.

g. Audit Procedure

Each audit requires at least thirty days' prior notice, except in the event of a Security Incident or upon instruction of a data protection authority. Audits will take place on a mutually agreed date during Medallia's normal business hours, and Customer will cause its representative or agent to employ such reasonable procedures and methods as are necessary and appropriate in the circumstances to minimize interference with Medallia's normal business operations. Onsite audits are limited to two business days.

10. CONFIDENTIALITY

a. Controlling Statement of Obligations

The terms of this Confidentiality provision supersede any non-disclosure or confidentiality agreement entered into by the parties prior to the Effective Date of this Agreement.

b. Confidential Information

Confidential Information means all information provided by a disclosing party to a receiving party that a reasonable industry participant would deem to be confidential, including for example: (i) all information that is marked confidential; (ii) the terms of this Agreement and each Order; (iii) features and functionality of Medallia Products and related documentation; and (iv) Customer Data.

Confidential Information does not include information that is independently developed, that becomes public knowledge through no fault of the receiving party, or that is received from a third party under circumstances that do not create a reasonable suspicion that it has been misappropriated or improperly disclosed.

c. Use and Disclosure Restrictions

A receiving party will use commercially reasonable efforts to protect Confidential Information it receives and will use Confidential Information only as necessary to perform its obligations and exercise its rights under this Agreement and each Order. A receiving party will not disclose Confidential Information to third parties other than as permitted under this Agreement or as compelled by a court or regulator of competent authority (and then while taking all reasonable steps to inform the disclosing party prior to disclosure and to limit the scope of the disclosure).

11. INDEMNIFICATION

a. Intellectual Property Indemnification by Medallia

Medallia will defend Customer against claims, causes of action, and investigations by third parties or government agencies and will pay the resulting judgments, fines, settlements, court costs, and attorneys fees (to "**Indemnify**") for third party claims alleging that Medallia Products infringe a third-party patent, copyright, or trademark or misappropriate a third-party trade secret, subject to the following limitations: (i) if the alleged infringement arises from a modification by Customer or the unauthorized use of Medallia Products; (ii) if the alleged infringement arises from a violation of Customer's obligations under Section 4 ("Use of Medallia Products"); or (iii) if the alleged infringement arises from the combination of Medallia Products with any product or process not provided by Medallia, and if Medallia would not be liable for inducement or contribution for such infringement, then Medallia will have no obligation to Indemnify.

If Customer establishes a reasonable belief that

use of Medallia Products will be enjoined, then Medallia will use commercially reasonable efforts to substitute the affected functionality with a non-infringing alternative or to procure a license to allow for the continued use of the affected functionality. If use of Medallia Products is enjoined and if Medallia has not provided a non-infringing alternative, then Customer may, within 30 days of the date of the injunction, terminate the affected Order immediately upon written notice and receive a refund of the unused portion of prepaid fees.

b. Data Breach Indemnification by Medallia

Medallia will Indemnify Customer for third party claims arising from the improper access, use, or disclosure of personally identifiable Customer Data caused by: (i) Medallia's breach of its obligations under this Agreement; or (ii) the willful misconduct or gross negligence of Medallia personnel or any third party under Medallia's control.

c. Indemnification by Customer

Customer shall Indemnify Medallia from third-party claims arising out of: (i) Customer's or any of its employees and agents use of Medallia Products in violation of Section 4 of this Agreement; and (ii) alleged infringement of a third-party patent, copyright, or trademark or misappropriation of a third-party trade secret arising out of (A) an unauthorized modification by Customer of Medallia Products; or (B) an unauthorized combination of Medallia Products with any product or process not provided or authorized by Medallia.

d. Indemnification Requirements and Procedure

The party seeking indemnification (the "**Indemnified Party**") will provide timely notice to the party from which it seeks indemnification (the "**Indemnifying Party**") (although untimely notice will relieve the Indemnifying Party of its indemnification obligations only commensurate with actual prejudice suffered as a result) and will provide reasonable assistance to Indemnifying Party at the Indemnifying Party's expense. The Indemnifying Party will have sole control over the defense, but the Indemnified Party will have the right to participate at its own cost.

12. LIMITATION OF DAMAGES AND LIABILITY

a. Limitation of Damages

NEITHER PARTY WILL BE LIABLE TO THE OTHER FOR CONSEQUENTIAL, SPECIAL, INCIDENTAL, PUNITIVE, EXEMPLARY, OR INDIRECT DAMAGES OR FOR LOST PROFITS, LOST REVENUES, HARM TO GOODWILL, OR THE COSTS OF PROCURING REPLACEMENT SERVICES, REGARDLESS OF WHETHER SUCH DAMAGE WAS FORESEEABLE. THIS LIMITATION WILL APPLY TO ALL CLAIMS UNDER ALL THEORIES OF LAW AND EQUITY, EXCEPT WHERE PROHIBITED BY LAW.

b. Limitation of Liability

EXCEPT IN THE EVENT OF GROSS NEGLIGENCE; WILLFUL MISCONDUCT; CLAIMS FOR INDEMNIFICATION UNDER THIS AGREEMENT; FOR FEES OWED IN EXCESS OF THE BELOW LIMIT; AND WHERE PROHIBITED BY LAW, THE CUMULATIVE LIABILITY OF EITHER PARTY TO THE OTHER WILL BE LIMITED TO:

(I) TWO TIMES THE FEES PAID OR PAYABLE UNDER THIS AGREEMENT FOR THE 12 MONTHS PRECEDING THE FILING OF THE CLAIM, FOR CLAIMS ARISING FROM A BREACH OF THE CONFIDENTIALITY AND PRIVACY AND SECURITY PROVISIONS OF THIS AGREEMENT; AND

(II) THE FEES PAID OR PAYABLE UNDER THIS AGREEMENT FOR THE 12 MONTHS PRECEDING THE FILING OF THE CLAIM, FOR ALL OTHER CLAIMS.

13. MARKETING

Medallia may include Customer's name and logo on Medallia's public customer list. Customer agrees to partner with Medallia on co-marketing and public relations activities to demonstrate the launch and success of Customer's program (e.g., press release, case study, testimonial, video). Customer grants Medallia a limited, non-exclusive, worldwide license to use its trademark for these purposes.

14. GENERAL TERMS

a. Authority

Each party warrants that it has the authority to enter into this Agreement and each Order.

b. Assignment

Neither this Agreement nor any Order may be assigned without written consent (such consent not to be unreasonably withheld) and any such attempted assignment will be void.

c. Survival

All terms that must survive termination in order to have their customary effect, including terms related to confidentiality, indemnification, limitation of damages and liability, and post-termination data transfer will survive termination or expiration of this Agreement.

d. Force Majeure

No party will be deemed to have breached this Agreement or any Order if its failure to perform was caused by events beyond that party's reasonable control, such as mass failure of internet infrastructure, civil unrest, and natural disasters.

e. Independent Contractors

The parties are independent contractors. Neither party has the right to bind the other, and neither party will make any contrary representation to a third party.

f. Export Compliance

Customer will comply with the export control and economic sanctions laws and regulations of the United States, United Kingdom, and other applicable jurisdictions. Consistent with that obligation, Customer will not make Medallia Products available to any person or entity that is: (i) located in a country that is subject to an embargo by the United States, United Kingdom, or other applicable government, (ii) listed on any United States, United Kingdom, or European Union government list of prohibited or restricted parties, or (iii) engaged in activities directly or indirectly related to the proliferation of weapons of mass destruction.

g. Arbitration, Governing Law and Forum

This Agreement and any dispute or claim arising out of or in connection with its subject matter or formation (including non-contractual disputes or claims) shall be governed by English law.

All disputes arising out of or in connection with this Agreement will be settled by arbitration administered by the International Chamber of Commerce under its procedural Rules of Arbitration and the substantive law of England and Wales, and judgment on the award rendered by the arbitrator(s) may be entered in any court with jurisdiction. The arbitration shall be conducted in London, United Kingdom in the English language. This provision will not impair either party's ability to receive injunctive or other equitable relief from any court with jurisdiction. The United Nations Convention on Contracts for the International Sale of Goods does not apply to this Agreement.

h. No Waiver

The failure of a party to timely enforce an obligation under this Agreement or Order will only be construed as a waiver if given in writing and will not act to waive any other obligation, including any future occurrence of the waived obligation.

i. Complete Agreement

Documentation that accompanies the Order constitute part of this Agreement. This Agreement and each Order contains the full agreement of the parties (superseding all prior or contemporaneous agreements) and may only be amended by a writing signed by both parties. Notwithstanding anything to the contrary therein, terms or conditions stated in Customer order documentation (e.g., a Customer purchase order) will be null and void. Neither party enters into this Agreement or Orders based on representations not stated in these documents, and there will be no presumption against either party as the drafter thereof.

a. Rights of Third Parties

A person who is not a party to this Agreement has no right under the Contracts (Rights of Third Parties) Act 1999 to enforce or to enjoy the benefit of any term of this Agreement.

j. Subcontractors

Medallia may utilize subcontractors as described in Attachment B to provide services, provided

that: (i) Medallia has bound the subcontractor to agreements requiring it to conform to law, regulation, industry standards, and the quality, confidentiality, and privacy standards reflected in this Agreement; and (ii) Medallia remains responsible for delivery of the scope established in the Order.

k. Notices

Notifications required under this Agreement or an Order in relation to breach, disputed payments, audit, or indemnification will be provided in writing to the legal departments of the parties to the addresses identified in an order. Other notifications can be submitted via email. Notifications will be effective as of the date of delivery.

ATTACHMENT A

Privacy and Security

Core Platform and Medallia for Digital

Medallia's core platform for feedback collection and reporting (the "**Core Platform**"), and its platform for feedback collection across digital channels ("**Medallia for Digital**"), together referred to as the "Medallia Experience Cloud", are subject to the following privacy and data security terms:

1. **Security Program and Standards**. Medallia maintains a written information security program that contains appropriate administrative, technical and physical safeguards to protect Customer data, and that comply with SaaS industry standards for security controls. The Core Platform has been certified by an independent third party auditor as aligning with ISO 27001 and SOC 2 Type 2. Medallia for Digital has been certified by an independent third party auditor as aligning with the ISO 27001 standard. The Core Platform and Medallia for Digital also comply with HIPAA standards.

Certifications can be provided to Customer upon written request.

2. **Data Security**. Customer Data for the Core Platform will be stored on Medallia controlled hardware, collocated in data centers that are certified and audited to a SaaS industry standard for security controls (such asSOC 2 Type 2 or ISO 27001). Medallia provides encryption at rest through encrypting hard drives in Medallia's data centers. Data Customer collects with Medallia for Digital will be stored on an Amazon S3 instance in Oregon, USA; Ireland, European Union; Sydney, Australia; Montreal, Canada, or a Medallia co-location facility, depending on Customer's choice. More information about Amazon Web Services security can be found at https://aws.amazon.com/security/.

3. **Network Security.** Medallia shall use industry standard firewall and encryption technologies to protect the public gateways through which Customer's data travels. Medallia will use commercially reasonable efforts for protection against and detection of common network attacks. Medallia will monitor its network for attacks and will deploy appropriate processes to manage vulnerabilities.

4. **Host/Access Management**. User access to the Medallia Experience Cloud will be controlled through a username and password combination managed by Medallia, or through Single Sign-On integration with customer's identity systems using industry standards.

5. **Application Security**. The software development for the Medallia Experience Cloud follows a secure lifecycle, including source code management and appropriate reviews. Application penetration testing will be subject to reasonable fees and requires the execution of a separate agreement.

7. **Data Collection**. The Core Platform enables Customer to send survey invitations to its customers, typically through email, based on touchpoints Customer's customers have with its business. The types of data that are collected via questions in these survey programs are within Customer's control, and will be specified during implementation. Typically, in order for the Medallia Experience Cloud to send surveys, Customer's business initially sends data to Medallia about survey takers in an "invitation file" that includes information such as names, emails, information about the survey taker's interaction with Customer, and other information that enables Customer to segment the survey takers into groups. Medallia for Digital collects customer feedback through surveys deployed on Customer's digital channels. Customer can configure the types of data requested from visitors to such surveys. If surveys are configured to not ask for personal information such as name and email, then no such data will be collected except for analytics information (such as the visitor's IP address).

MEDALLIA JOURNEY ANALYTICS

Medallia's platform for analyzing customer journeys ("Medallia Journey Analytics") is subject to the following privacy and data security terms:

1. **Security Program and Standards.** Medallia maintains a written information security program that contains appropriate administrative, technical and physical safeguards to protect Customer Data, and that comply with SaaS industry standards for security controls. In Medallia Journey Analytics, Customer Data is processed and stored in Google Cloud Platform, whose services are regularly audited against SOC 1, SOC 2, ISO 27001, ISO 27018, and HIPAA.

Such certifications can be downloaded at https://cloud.google.com/security/compliance

2. **Physical and Infrastructure Security**. Customer Data that is at rest is encrypted using Google Cloud Platform's 'encryption by default'. More details can be found at https://cloud.google.com/security/encryption-at-rest/

At a minimum, Customer Data is assigned to a project in Google BigQuery that is unique to Customer, which provides logical separation of data.

Customer Data that is at rest is stored in the region specific by Customer during implementation. Available regions are listed at https://cloud.google.com/storage/docs/locations.

3. **Network Security**. Medallia shall use industry standard firewall and encryption technologies to protect the public gateways through which Customer data travels. Medallia will use commercially reasonable efforts for protection against and detection of common network attacks. Medallia will monitor its network for attacks and will deploy appropriate processes to manage vulnerabilities.

4. **Host/Access Management**. User access to the Medallia Experience Cloud will be controlled through a username and password combination, managed by Medallia.

5. **Application Security**. The software development for the Medallia Experience Cloud follows a secure lifecycle, including source code management and appropriate reviews.

6. **Data Collection**. Medallia Journey Analytics enables Customer to import and collect a wide range of information about Customer's customers or end users. The types of data that are imported and collected in Medallia Journey Analytics will be entirely within Customer's control, and will be specified during implementation and use of the platform. Unless approved by Medallia's data protection attorneys, Customer shall not configure the Medallia Experience Cloud to collect bank account numbers, payment card or credit card information, bank transaction information, government identification numbers including (but not limited to) social security numbers, state identification numbers, and passport numbers, and sensitive personal information including (but not limited to) religious beliefs, health, sexual orientation, race, and union membership and Medallia will not be liable for non-compliance under laws and regulations that applies to the processing of the foregoing categories of data.

STRIKEDECK

Medallia's customer success platform ("**Strikedeck**") is subject to the following privacy and data security terms:

1. **Access Control**

i) Preventing Unauthorized Product Access

Physical and Environmental Security: Strikedeck hosts its product infrastructure with multi-tenant, outsourced data center providers. The physical and environmental security controls of these data center providers are audited for SOC 2 Type II and/or ISO 27001 compliance, and other applicable certifications.

Authentication: Strikedeck implements a uniform password policy for its customer products. Customers who interact with the products via the user interface must authenticate before accessing non-public Customer Data.

Authorization: Customer Data is stored in multi-tenant storage systems accessible to Customers via only application user interfaces and application programming interfaces. Customers are not allowed direct access to the underlying application infrastructure. The authorization model in each of Strikedeck's products is designed to ensure that only the appropriately assigned individuals can access relevant features, views, and customization options. Authorization to data sets is performed through validating the user's permissions against the attributes associated with each data set.

Application Programming Interface (API) Access: Public product APIs may be accessed using an API key or through Oauth authorization.

ii) Preventing Unauthorized Product Use

Access Controls: Network access control mechanisms are designed to prevent network traffic using unauthorized protocols from reaching the product infrastructure. The technical measures implemented differ between data center providers and include Virtual Private Cloud (VPC) implementations and security group assignment, along with traditional enterprise firewall and Virtual Local Area Network (VLAN) assignment.

Intrusion Detection and Prevention: Strikedeck implements intrusion detection systems to protect all hosted sites. These systems are designed to identify and prevent attacks against publicly available network services.

Code Analysis: Security reviews of code stored in Strikedeck's source code repositories is performed, checking for coding best practices and identifiable software flaws.

Penetration Testing: Strikedeck maintains relationships with industry recognized penetration testing service providers for penetration tests. The intent of the penetration tests is to identify and resolve foreseeable attack vectors and potential abuse scenarios.

iii) Limitations of Privilege & Authorization Requirements

Product Access: A subset of Strikedeck's employees have access to Customer Data via controlled interfaces. The intent of providing access to a subset of employees is to provide effective customer support, to troubleshoot potential problems, and to detect and respond to security incidents. Access is enabled through "just in time" requests for access; all such requests are logged. Employees are granted access by role, and reviews of high risk privilege grants are initiated daily. Employee roles are reviewed at least once every six months. All Strikedeck employees undergo a 3rd party background check prior to being extended an employment offer. All employees are required to conduct themselves in a manner consistent with Strikedeck company guidelines, non-disclosure requirements, and ethical standards.

2. **Transmission Control**

In-transit: Strikedeck makes HTTPS encryption (also referred to as SSL or TLS) available on

every one of its login interfaces. Strikedeck's HTTPS implementation uses industry standard algorithms and certificates.

At-rest: Strikedeck stores user passwords as one-way hashes.

3. **Input Control**

Security Incident Detection: Strikedeck designed its infrastructure to log information about the system behavior, traffic received, system authentication, and other application requests. Internal systems aggregated log data and alert appropriate employees of malicious, unintended, or anomalous activities. Strikedeck personnel, including security, operations, and support personnel, are responsive to known incidents.

4. **Job Control**

Strikedeck never sells personal data to any third party.

Terminating Customers: Customer Data is purged per section 7 of the agreement.

5. **Availability Control**

Infrastructure Availability: The data center providers use commercially reasonable efforts to ensure a minimum of 99.95% uptime. The providers maintain a minimum of N+1 redundancy to power, network, and HVAC services.

Fault Tolerance: Backup and replication strategies are designed to ensure redundancy and fail-over protections during a significant processing failure. Customer Data is backed up to multiple durable data stores and replicated across multiple data centers and availability zone.

ATTACHMENT B

Subcontractors and Medallia Subsidiaries

The security and data handling practices of each third party subcontractor is evaluated by Medallia's vendor risk management program. In addition, each third party subcontractor agrees to security and data processing agreements that restrict their access, use and disclosure of personal data in compliance with applicable laws, and Medallia's security and privacy certifications.

For more information on Medallia's security program, visit https://www.medallia.com/security/.

An up-to-date version of this list and a form to sign up for updates is available in Medallia's product documentation at https://docs.medallia.com.

Servicing and Technical Support

The subcontractors listed provide servicing and technical support for Medallia Products.

Subcontractor Name	Corporate Location	Processing Description
Effective Teleservices Pvt Ltd	India	Implementation, servicing, and technical support.
CX Software Solutions SA de CV	Mexico	Implementation, servicing, and topic building for text analytics.
Infinit Outsourcing, Inc.	Philippines	Technical support.
Experis US, Inc.	USA	Topic building for text analytics.
Gemseek Consulting Limited	Bulgaria	Implementation and servicing.
SM Technologies Limited	Brazil	Implementation and servicing.

Technology Providers

The subcontractors listed provide technology for Medallia Products.

Subcontractor Name	Corporate Location	Processing Description
Sumo Logic, Inc.	USA	Manages system logs for diagnosis and resolution of technical issues.
Salesforce.com, Inc.	USA	Tracks technical support tickets.
Amazon Web Services, Inc.	USA	Archives security logs for security incident monitoring and detection.

		Hosts and processes data for Medallia for Digital and Strikedeck. Renders front-end html and reports for Journey Analytics. Hosts content for Rich Media feedback functionality, if enabled.
Google Inc.	USA	Data storage and processing for Journey Analytics. Translates feedback text, if enabled in Customer's Medallia implementation.
AppDynamics, Inc.	USA	Analyzes performance and usage of survey pages and reporting applications.
Usersnap GmbH	Austria	Provides screen capture functionality, if enabled in Customer's Medallia Digital implementation.
Twilio	USA	Provides SMS routing and delivery services. Sendgrid is used to send emails to users in Journey Analytics.
Pendo.io	USA	Analyzes performance and usage of Strikedeck applications.
GFN DSelva Infotech Pvt Ltd	India	Performs development and quality assurance for Strikedeck applications.
Palo Alto Databases, Inc.	USA	Supports Strikedeck Enterprise's ETL tool.
Redis Labs Ltd.	USA	Redis for Caching service maintains state for cookies in Journey Analytics.

Changing Technology Providers

Medallia shall notify Customer if it adds or removes a technology provider at least fifteen (15) days prior to any such changes. Medallia shall provide Customer with automatic updates to Medallia's technology provider list through its administrative portal. Customer may object to Medallia's appointment of a new technology provider by sending an email to privacy@medallia.com within ten (10) calendar days of such notice, provided that such objection is based on reasonable grounds relating to data protection. In such event, the parties will discuss such concerns in good faith with a view towards achieving resolution.

Medallia Subsidiaries

In addition to access from the United States, Medallia employees at its subsidiaries may access Customer's program instance to provide technical support, cloud operations, product troubleshooting, and infrastructure maintenance. Medallia shall maintain agreements with these subsidiaries that obligate them to data privacy and security requirements no less stringent than those set forth in this agreement.

Subsidiary Name	Location
Medallia Canada, Inc.	Canada
Medallia S.A.	Argentina
Medallia Limited	United Kingdom
Medallia Australia PTY Ltd	Australia
Medallia Digital Ltd	Israel
Medallia GmbH	Germany