Salesmate Data Processing Addendum

This Data Processing Addendum ("DPA") is made as of the Effective Date by and between RapidOps Inc (“Salesmate”), and Customer, pursuant to the Master SaaS Subscription Agreement or the Subscription Terms of Service, as applicable ("Agreement ").

The Parties have agreed to the Terms of Service posted at https://www.salesmate.io/tos according to which Salesmate has agreed to provide certain services to Customer (hereinafter the “Services”).

When providing the Services, Salesmate may collect, process and gain access to personal data of individuals or behalf of the Customer. From a data protection perspective, Customer will be the data controller and Salesmate will be the data processor.

This DPA amends the Agreement and sets out the terms that apply when Personal Data is processed by Salesmate under the Agreement. The purpose of the DPA is to ensure such processing is conducted in accordance with applicable laws and with due respect for the rights and freedoms of individuals whose Personal Data are processed. Other capitalized terms used but not defined in this DPA have the same meanings as set out in the Agreement.

1. Definitions

For the purposes of this DPA:

a) “California Personal Information” means Personal Data that is subject to the protection of the CCPA.

b) "CCPA" means California Civil Code Sec. 1798.100 et seq. (also known as the California Consumer Privacy Act of 2018, as amended by the California Privacy Rights Act of 2020 or "CPRA").

c) “EEA" means the European Economic Area, which constitutes the member states of the European Union, the United Kingdom, Norway, Iceland and Liechtenstein.

d) "Data Protection Laws" shall mean the data protection laws of the country in which Controller is established, including the GDPR, CCPA, CPRA and any data protection laws applicable to Controller in connection with the Service Agreement.

e) “Controller” shall mean the entity which, alone or jointly with others, determines the purposes and means of the processing of Personal Data;

f) "Europe" means the European Union, the European Economic Area and/or their member states, Switzerland and the United Kingdom.

g) “European Data” means Personal Data that is subject to the protection of European Data Protection Laws.

h) "European Data Protection Laws" means data protection laws applicable in Europe, including: (i) Regulation 2016/679 of the European Parliament and of the Council on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) ("GDPR"); (ii) Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector; and (iii) applicable national implementations of (i) and (ii); or (iii) GDPR as it forms parts of the United Kingdom domestic law by virtue of Section 3 of the European Union (Withdrawal) Act 2018 ("UK GDPR"); and (iv) Swiss Federal Data Protection Act on 19 June 1992 and its Ordinance ("Swiss DPA"); in each case, as may be amended, superseded or replaced.

i) “Processing” means any operation or set of operations which is performed on Personal Data, encompassing the collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction or erasure of Personal Data. The terms “Process”, “Processes” and “Processed” will be construed accordingly.

j) “Processor” shall mean an entity which processes Personal Data on behalf of the Controller; and

k) “Personal Data” means any information relating to an identified or identifiable natural person.

l) “Personal Data Breach” means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Personal Data transmitted, stored or otherwise Processed by us and/or our Sub-Processors in connection with the provision of the Subscription Services. "Personal Data Breach" will not include unsuccessful attempts or activities that do not compromise the security of Personal Data, including unsuccessful log-in attempts, pings, port scans, denial of service attacks, and other network attacks on firewalls or networked systems.

m) “Sensitive Data” means Personal Data that is protected under special legislation and requires unique treatment, such as “special categories of data”, “sensitive data” or other materially similar terms under applicable Data Protection Laws, which may include any of the following: (a) social security number, tax file number, passport number, driver’s license number, or similar identifier (or any portion thereof); (b) credit or debit card number; (c) financial, credit, genetic, biometric or health information; (d) information revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data or biometric data for the purpose of uniquely identifying a natural person, data concerning health or a person’s sex life or sexual orientation, or data relating to criminal convictions and offenses; and/or (e) account

passwords in unhashed form.

n) "Data Subject" means the individual to whom Personal Data relates.

o) "Instructions" means the written, documented instructions issued by a Controller to a Processor, and directing the same to perform a specific or general action with regard to Personal Data (including, but not limited to, depersonalizing, blocking, deletion, making available).

p) "Sub-Processor" means any Processor engaged by us or our Affiliates to assist in fulfilling our obligations with respect to the provision of the Subscription Services under the Agreement. Sub-Processors may include third parties or our Affiliates but will exclude any Salesmate employee or consultant.

2. Customer's Obligations

a) Compliance with Laws. Within the scope of the Agreement and in its use of the services, Customer shall be responsible for complying with all requirements that apply to it under applicable Data Protection Laws with respect to its Processing of Personal Data and the Instructions it issues to Salesmate.

b) In particular but without prejudice to the generality of the foregoing, Customer acknowledges and agrees that they will be solely responsible for:

   a. The accuracy, quality, and legality of Customer Data and the means by which it acquired Personal Data.
   b. Complying with all necessary transparency and lawfulness requirements under applicable Data Protection Laws for the collection and use of the Personal Data, including obtaining any necessary consents and authorizations (particularly for use by customer for marketing purposes);
   c. Ensuring customer has the right to transfer, or provide access to, the Personal Data to Salesmate for Processing in accordance with the terms of the Agreement.
   d. Ensuring that Customer's Instructions to Salesmate regarding the Processing of Personal Data comply with applicable laws, including Data Protection Laws; and
   e. Complying with all laws (including Data Protection Laws) applicable to any emails or other content created, sent or managed through the Services, including those relating to obtaining consents (where required) to send emails, the content of the emails and its email deployment practices. Customer will inform Salesmate without undue delay if Customer is not able to comply with its responsibilities under sub-section (2.a) or applicable Data Protection Laws.

c) Controller Instructions. The parties agree that the Agreement (including this DPA), together with your use of the Subscription Service in accordance with the Agreement, constitute customer's complete Instructions to us in relation to the Processing of Personal Data, so long as you may provide additional instructions during the subscription term that

are consistent with the Agreement, the nature and lawful use of the Subscription Service.

d) Security. You are responsible for independently determining whether the data security provided for in the Subscription Service adequately meets your obligations under applicable Data Protection Laws. You are also responsible for your secure use of the Subscription Service, including protecting the security of Personal Data in transit to and from the Subscription Service (including to securely backup or encrypt any such Personal Data).

3. Salesmate Obligations

a) Compliance with Instructions. Salesmate shall only Process Personal Data for the purposes described in this DPA or as otherwise agreed within the scope of Customer's lawful Instructions, except where and to the extent otherwise required by applicable law. Salesmate is not responsible for compliance with any Data Protection Laws applicable to Customer or Customer's industry that are not generally applicable to Salesmate.

b) Conflict of Laws. If Salesmate becomes aware that we cannot Process Personal Data in accordance with Customer's Instructions due to a legal requirement under any applicable law, Salesmate will (i) promptly notify Customer of that legal requirement to the extent permitted by the applicable law; and (ii) where necessary, cease all Processing (other than merely storing and maintaining the security of the affected Personal Data) until such time as Customer issues new Instructions with which Salesmate is able to comply. If this provision is invoked, Salesmate will not be liable to Customer under the Agreement for any failure to perform the applicable Subscription Services until such time as Customer issues new lawful Instructions with regard to the Processing.

c) Confidentiality. Salesmate will ensure that any personnel whom Salesmate authorizes to Process Personal Data on our behalf is subject to appropriate confidentiality obligations (whether a contractual or statutory duty) with respect to that Personal Data.

d) Security. Salesmate will have in place and maintain throughout the term of this Agreement appropriate technical and organizational measures to protect the Personal Data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access, and against all other unlawful forms of processing (a "Security Incident").

e) Incidents and Reporting. We will notify you without undue delay after we become aware of any Personal Data Breach and will provide timely information relating to the Personal Data Breach as it becomes known or reasonably requested by you. At your request, we will promptly provide you with such reasonable assistance as necessary to enable you to notify relevant Personal Data Breaches to competent authorities and/or affected Data Subjects, if you are required to do so under Data Protection Laws.

f) Deletion or Return of Personal Data. Upon termination or expiration of the Agreement, Salesmate shall (at Customer's election) delete or return to Customer all Customer Data (including copies) in its possession or control, except that this requirement shall not apply to the extent Salesmate is required by applicable law to retain some or all of the Customer Data, or to Customer Data it has archived on back-up systems, which Customer Data Salesmate shall securely isolate, protect from any further processing and eventually delete in accordance with Salesmate's deletion policies, except to the extent required by applicable law. We strongly recommend retrieving your Customer Data prior to the end of your Subscription Term using our data export tools or APIs.

4. Data Subject Requests

The Salesmate Service provides Customer with a number of controls that Customer can use to retrieve, correct, delete or restrict Personal Data, which Customer may use to assist it in connection with its obligations under Data Protection Laws, including your obligations relating to responding to requests from Data Subjects to exercise their rights under applicable Data Protection Laws ("Data Subject Requests").

To the extent that Customer is unable to independently address a Data Subject Request through the Subscription Service, then upon Customer's written request Salesmate will provide reasonable assistance to Customer to respond to any Data Subject Requests or requests from data protection authorities relating to the Processing of Personal Data under the Agreement. Customer will reimburse Salesmate for the commercially reasonable costs arising from this assistance.

If a Data Subject Request or other communication regarding the Processing of Personal Data under the Agreement is made directly to Salesmate, Salesmate will promptly inform Customer and will advise the Data Subject to submit their request to Customer. Customer will be solely responsible for responding substantively to any such Data Subject Requests or communications involving Personal Data.

5. Sub-Processor

Customer agrees that (a) Salesmate may engage Sub-processors as listed at https://www.salesmate.io/sub-processors/ (the "Sub-processor Page") which may be updated from time to time and Salesmate Affiliates; and (b) such Affiliates and Sub-processors respectively may engage third party processors to process Customer Data on Salesmate's behalf. Customer provides a general authorization for Salesmate to engage onward sub-processors that is conditioned on the following requirements: (a) Salesmate will restrict the onward sub-processor's access to Customer Data only to what is strictly necessary to provide the Services, and Salesmate will prohibit the sub-processor from processing the Personal Data for any other purpose. (b) Salesmate agrees to impose contractual data protection obligations, including appropriate technical and organizational measures to protect personal data, on any sub-processor it appoints that require such sub-processor to protect Customer Data to the standard required by Applicable Data Protection Legislation; and (c) Salesmate

will remain liable and accountable for any breach of this DPA that is caused by an act or omission of its sub-processors.

Salesmate shall provide customer notification, prior to the appointment of any new Sub-Processor (irrespective of whether such new Sub-Processor is appointed for carrying out an existing processing function or a new processing function). Upon notification regarding Salesmate's intention to engage a new Sub-Processor, you may object to such engagement by notifying Salesmate promptly in writing via email at support@salesmate.com, within ten (10) business days after receipt of Salesmate's notice. If Customer objects to the appointment of an additional Sub-processor within thirty (30) calendar days of such notice on reasonable grounds relating to the protection of the Personal Data, then Salesmate will work in good faith with Customer to find an alternative solution. In the event that the parties are unable to find such a solution, Customer may terminate the Agreement at no additional cost.

6. Data Transfers

Customers acknowledge and agree that we may access and Process Personal Data on a global basis as necessary to provide the Subscription Service in accordance with the Agreement, and that Personal Data may be transferred to and processed by Salesmate in the United States and to other jurisdictions where Salesmate Affiliates and Sub-Processors have operations. Wherever Personal Data is transferred outside its country of origin, each party will ensure such transfers are made in compliance with the requirements of Data Protection Laws.

7. Transfer Mechanism

a) Salesmate will not transfer European Data to any country or recipient not recognized as providing an adequate level of protection for Personal Data (within the meaning of applicable European Data Protection Laws), unless it first takes all such measures as are necessary to ensure the transfer is in compliance with applicable European Data Protection Laws. Such measures may include (without limitation) transferring such data to a recipient that is covered by a suitable framework or other legally adequate transfer mechanism recognized by the relevant authorities or courts as providing an adequate level of protection for Personal Data, to a recipient that has achieved binding corporate rules authorization in accordance with European Data Protection Laws, or to a recipient that has executed appropriate standard contractual clauses in each case as adopted or approved in accordance with applicable European Data Protection Laws.

b) You acknowledge that in connection with the performance of the Subscription Services, Salesmate is a recipient of European Data in the United States. Subject to sub-sections (c) and (d), the parties agree that the Standard Contractual Clauses will be incorporated by reference and form part of the Agreement as follows:

   i) EEA Transfers. In relation to European Data that is subject to the GDPR (i) Customer is the "data exporter" and Salesmate is the "data importer"; (ii) the Module Two terms apply to the extent the Customer is a Controller of European

Data and the Module Three terms apply to the extent the Customer is a Processor of European Data; (iii) in Clause 7, the optional docking clause applies; (iv) in Clause 9, Option 2 applies and changes to Sub-Processors will be notified in accordance with the 'Sub-Processors' section of this DPA; (v) in Clause 11, the optional language is deleted; (vi) in Clauses 17 and 18, the parties agree that the governing law and forum for disputes for the Standard Contractual Clauses will be determined in accordance with the 'Contracting Entity; Applicable Law; Notice' section of the Jurisdiction Specific Terms or, if such section does not specify an EU Member State, the Republic of Ireland (without reference to conflicts of law principles); (vii) the Annexes of the Standard Contractual Clauses will be deemed completed with the information set out in the Annexes of this DPA; and (viii) if and to the extent the Standard Contractual Clauses conflict with any provision of this DPA the Standard Contractual Clauses will prevail to the extent of such conflict.

ii) UK Transfers. In relation to European Data that is subject to the UK GDPR, the Standard Contractual Clauses will apply in accordance with sub-section (a) and the following modifications (i) the Standard Contractual Clauses will be modified and interpreted in accordance with the UK Addendum, which will be incorporated by reference and form an integral part of the Agreement; (ii) Tables 1, 2 and 3 of the UK Addendum will be deemed completed with the information set out in the Annexes of this DPA and Table 4 will be deemed completed by selecting "neither party"; and (iii) any conflict between the terms of the Standard Contractual Clauses and the UK Addendum will be resolved in accordance with Section 10 and Section 11 of the UK Addendum.

iii) Swiss Transfers. In relation to European Data that is subject to the Swiss DPA, the Standard Contractual Clauses will apply in accordance with sub-section (a) and the following modifications (i) references to "Regulation (EU) 2016/679" will be interpreted as references to the Swiss DPA; (ii) references to "EU", "Union" and "Member State law" will be interpreted as references to Swiss law; and (iii) references to the "competent supervisory authority" and "competent courts" will be replaced with the "the Swiss Federal Data Protection and Information Commissioner " and the "relevant courts in Switzerland".

c) If for any reason Salesmate cannot comply with its obligations under the Standard Contractual Clauses or is in breach of any warranties under the Standard Contractual Clauses, and Customer intends to suspend the transfer of European Client Data to Salesmate or terminate the Standard Contractual Clauses, Customer agrees to provide Salesmate with reasonable notice to enable Salesmate to cure such non-compliance and reasonably cooperate with Salesmate to identify what additional safeguards, if any, may be implemented to remedy such noncompliance. If Salesmate has not or cannot cure the non-compliance, Customer may suspend or terminate the affected part of the Service in accordance with the Terms of Service without liability to either party (but without prejudice to any fees you have incurred prior to such suspension or termination).

d) Although Salesmate does not currently rely on the EU-US Privacy Shield as a legal basis for transfers of European Data in light of the judgment of the Court of Justice of the EU in Case C-311/18, for as long as Salesmate is self-certified to the Privacy Shield Salesmate will process European Data in compliance with the Privacy Shield Principles and let you know if it is unable to comply with this requirement. In the event that Salesmate adopts an alternative transfer mechanism (including any new or successor version of the EU-US Privacy Shield) for transfers of European Data to Salesmate, such alternative transfer mechanism will apply automatically instead of the Standard Contractual Clauses described in this DPA (but only to the extent such alternative transfer mechanism complies with European Data Protection Laws), and you agree to execute such other documents or take such action as may be reasonably necessary to give legal effect such alternative transfer mechanism.

8. Demonstration of Compliance or Audits

a) The parties acknowledge that when Salesmate is acting as a processor on behalf of Customer, Customer must be able to assess Salesmate's compliance with its obligations under Applicable Data Protection Legislation and this DPA.

b) Salesmate will make available to Customer all information reasonably necessary to demonstrate compliance with this DPA and the obligations under Article 28 of the GDPR. While it is the parties' intention ordinarily to rely on the provision of the documentation to demonstrate Salesmate's compliance with this DPA and the provisions of Article 28 of the GDPR, Salesmate will permit Customer (or its appointed third party auditors) to carry out an audit at Customer's cost and expense (including without limitation the costs and expenses of Salesmate) of Salesmate's processing of Customer Data under the Agreement following a Security Breach suffered by Salesmate, or upon the instruction of a data protection authority acting pursuant to Applicable Data Protection Legislation. Customer must give Salesmate reasonable prior notice of such intention to audit, conduct its audit during normal business hours, and take all reasonable measures to prevent unnecessary disruption to Salesmate's operations. Any such audit shall be subject to Salesmate's security and confidentiality terms and guidelines and may only be performed a maximum of once annually. If Salesmate declines to follow any instruction requested by Customer regarding audits, Customer is entitled to terminate the Agreement.

9. Term and Termination

a) Term. The "Effective Date" of this DPA is the date which is the earlier of (a) Customer's initial access to any Service through any online provisioning, registration or order process or (b) the effective date of the first Service Order Form, as applicable, referencing this DPA. It shall continue to be in full force and effect as long as Processor is processing Personal Data according to Annex I and shall cease automatically thereafter.

b) Amends. From time to time, Salesmate may modify this Data Processing Addendum Unless otherwise specified by Salesmate, changes become effective for Customer upon renewal of the then-current Subscription Term or entry into a new Service Order Form after the updated version of this DPA goes into effect. Salesmate will use reasonable efforts to notify Customer of the changes through communications via Customer's Account, email or other means.

c) Termination. If the Processor is in material breach of the terms of this Data Processing Agreement, then the Customer may terminate the Data Processing Agreement as well as the Service Agreement for cause, at any time upon reasonable notice or without notice.

10. Miscellaneous

a) Conflict. If there is a conflict between the Agreement and this DPA, the terms of this DPA will prevail. The order of precedence will be: (a) this DPA; (a) the Agreement; and (c) the Privacy Policy. To the extent there is any conflict between the Standard Contractual Clauses, and any other terms in this DPA, the Agreement, or the Privacy Policy, the provisions of the Standard Contractual Clauses will prevail.

b) Governing Law. This DPA shall be governed by and construed in accordance with the governing law and jurisdiction provisions in the Agreement, unless required otherwise by Data Protection Laws.

This DPA has been entered into on the date stated at the beginning of it.

Executed for and behalf of Data Exporter by:

…….. (Signature)

……. (Print name)

……. (Position)

……. (Date)

Executed for and behalf of Salesmate by:

D. M. Patel …….. (Signature)

Dipesh Patel ……. (Print name)

Founder & CTO ……. (Position)

12th Aug 2023 ……. (Date)

Annex 1 – Details of processing

1) List of Parties

Data exporter:

Name: The Customer, as defined in Terms of Service (on behalf of itself and Permitted Affiliates)

Address: The Customer's address, as set out in the Order Form

Contact person's name, position and contact details: The Customer's contact details, as set out in the invoice and/or as set out in the Customer's Salesmate account.

Activities relevant to the data transferred under these Clauses: Processing of Personal Data in connection with Customer's use of the Salesmate Subscription Services under the Salesmate Customer Terms of Service

Role: Controller

Data importer:

Name: Rapidops Inc ("Salesmate")

Address: 525, North Tryon Street, Suite 1600, Charlotte, NC 28202-0213

Contact person's name, position and contact details: Dipesh Patel; DPO;

dpo@salesmate.io

Activities relevant to the data transferred under these Clauses: Processing of Personal Data in connection with Customer's use of the Salesmate Subscription Services under the Salesmate Customer Terms of Service

Role: Processor

2) Description of Transfer

a) Categories of Data Subjects whose Personal Data is Transferred

You may submit Personal Data in the course of using the Subscription Service, the extent

of which is determined and controlled by you in your sole discretion, and which may include, but is not limited to Personal Data relating to the following categories of Data Subjects:

Your Contacts and other end users including your employees, contractors, collaborators, customers, prospects, suppliers and subcontractors. Data Subjects may also include individuals attempting to communicate with or transfer Personal Data to your end users.

b) Categories of Personal Data Transferred

You may submit Personal Data to the Subscription Services, the extent of which is determined and controlled by you in your sole discretion, and which may include but is not limited to the following categories of Personal Data:

i) Name, title, street address, email address, phone number, other contact information;
ii) Customer history;
iii) Contract billing and bank data;
iv) IP Addresses;
v) References, meeting notes; and
vi) Any other Personal Data submitted by, sent to, or received by you, or your end users, via the Subscription Service.

c) Sensitive Data transferred and applied restrictions or safeguards

The parties do not anticipate the transfer of sensitive data.

d) Frequency of the transfer

The frequency of the transfer is on a continuous basis for the duration of the Service Agreement.

e) Nature of the Processing

Personal Data will be Processed in accordance with the Agreement (including this DPA) and may be subject to the following Processing activities:

1. Storage and other Processing necessary to provide, maintain and improve the Subscription Services provided to you; and/or

2. Disclosure in accordance with the Agreement (including this DPA) and/or as compelled by applicable laws.

f) Purpose of the transfer and further processing

We will Process Personal Data as necessary to provide the Subscription Services pursuant to the Agreement, as further specified in the Order Form, and as further instructed by you

in your use of the Subscription Services.

g) Period for which Personal Data will be retained

Subject to the 'Deletion or Return of Personal Data' section of this DPA, we will Process Personal Data for the duration of the Agreement, unless otherwise agreed in writing

3) Competent Supervisory Authority

For the purposes of the Standard Contractual Clauses, the supervisory authority that will act as competent supervisory authority will be determined in accordance with GDPR.

Annex 2 – Security Measures

Salesmate as a data processor uses the technical and organisational measures (listed below), to assist in providing services as described in our Terms of Service.

1. Access Control

   a) Preventing Unauthorized Product Access

      Outsourced processing: We host our Service with outsourced cloud infrastructure providers. Additionally, we maintain contractual relationships with vendors in order to provide the Service in accordance with our DPA. We rely on contractual agreements, privacy policies, and vendor compliance programs in order to protect data processed or stored by these vendors.

      Physical and environmental security: We host our product infrastructure with multi-tenant, outsourced infrastructure providers. We do not own or maintain hardware located at the outsourced infrastructure providers' data centers. Production servers and client-facing applications are logically and physically secured from our internal corporate information systems.

      Authentication: We implement a uniform password policy for our 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 our 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.

   b) Preventing Unauthorized Product Use

      We implement industry standard access controls and detection capabilities for the internal networks that support its products.

      i) 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 infrastructure providers and include Virtual Private Cloud (VPC) implementations,

security group assignment, and traditional firewall rules.

ii) Intrusion detection and prevention: We implement a Web Application Firewall (WAF) solution to protect hosted customer websites and other internet-accessible applications. The WAF is designed to identify and prevent attacks against publicly available network services.

iii) Penetration testing: We maintain relationships with industry-recognized penetration testing service providers for penetration testing of both the Salesmate web application and internal corporate network infrastructure at least annually. The intent of these penetration tests is to identify security vulnerabilities and mitigate the risk and business impact they pose to the in-scope systems.

iv) Bug bounty: A bug bounty program invites and incentivizes independent security researchers to ethically discover and disclose security flaws. We implement a bug bounty program in an effort to widen the available opportunities to engage with the security community and improve the product defences against sophisticated attacks.

c) Limitations of Privilege & Authorization Requirements

i) Product access: A subset of our employees have access to the products and to customer data via controlled interfaces. The intent of providing access to a subset of employees is to provide effective customer support, product development and research, to troubleshoot potential problems, to detect and respond to security incidents and implement data security. All such access requests are logged and reviewed.

ii) Background checks: Where permitted by applicable law, Salesmate employees undergo a third-party background or reference checks. All Salesmate employees are required to conduct themselves in a manner consistent with company guidelines, non-disclosure requirements, and ethical standards.

2. Transmission Control

a) In-transit: We use HTTPS encryption for the data transitions. Our HTTPS implementation uses industry standard algorithms and certificates.

b) At-rest: We store user passwords following policies that follow industry standard practices for security. We have implemented technologies to ensure that stored data is encrypted at rest.

3. Input Control

a) Detection: We designed our infrastructure to log extensive information about the system behaviour, traffic received, system authentication, and other application requests. Internal systems aggregate log data and alert appropriate employees of malicious, unintended, or anomalous activities. Our personnel, including security, operations, and support personnel, are responsive to known incidents.

b) Response and tracking: We maintain a record of known security incidents that includes description, dates and times of relevant activities, and incident disposition. Suspected and confirmed security incidents are investigated by security, operations, or support personnel; and appropriate resolution steps are identified and documented. For any confirmed incidents, we will take appropriate steps to minimize product and Customer damage or unauthorized disclosure. Notification to you will be in accordance with the terms of the Agreement.

4. Availability Control

Salesmate implements suitable measures to ensure that Personal Data is protected from accidental destruction or loss. This will be accomplished by:

a) Infrastructure Redundancy. We use two clustered servers for storing the data.

b) Fault tolerance: Backup and replication strategies are designed to ensure redundancy and fail-over protections during a significant processing failure.

c) Online replicas and backups: Where feasible, production databases are designed to replicate data between no less than 1 primary and 1 secondary database. All databases are backed up and maintained using at least industry standard methods.

Our products are designed to ensure redundancy and seamless failover. The server instances that support the products are also architected with a goal to prevent single points of failure. This design assists our operations in maintaining and updating the product applications and backend while limiting downtime. You can read more details here: https://www.salesmate.io/security-reliability/