ONLINE DATA PROCESSING AGREEMENT

This Data Processing Agreement (“**DPA**”) is made and entered into as of the date of acceptance by You and forms part of the OpsRamp Master Subscription Agreement (the “**Agreement**”). You acknowledge that you, on behalf of the entity You list when accepting this DPA (“**Organization**”) (collectively, **“You”, "Your”, “Partner”, or “Data Controller”**) have read and understood and agree to comply with this DPA, and are entering into a binding legal agreement with **OpsRamp** as defined below (**“OpsRamp”**, **“Us”**, **“We”, “Our”, “Service Provider” or “Data Processor”**) to reflect the parties’ agreement with regard to the Processing of Personal Data (as such terms are defined below) of GDPR-protected individuals. Both parties shall be referred to as the “Parties” and each, a “Party”.

WHEREAS, OpsRamp shall provide the services set forth in the Agreement (collectively, the “**Services**”) for Partner, as described in the Agreement; and

WHEREAS, In the course of providing the Services pursuant to the Agreement, OpsRamp may process Personal Data on your behalf, in the capacity of a “Data Processor”; and the Parties wish to set forth the arrangements concerning the processing of Personal Data (defined below) within the context of the Services and agree to comply with the following provisions with respect to any Personal Data, each acting reasonably and in good faith.

NOW THEREFORE, in consideration of the mutual promises set forth herein and other good and valuable consideration, the receipt and sufficiency of which are hereby acknowledged by the Parties, the parties, intending to be legally bound, agree as follows:

1. INTERPRETATION AND DEFINITIONS

1.1 The headings contained in this DPA are for convenience only and shall not be interpreted to limit or otherwise affect the provisions of this DPA.

1.2 References to clauses or sections are references to the clauses or sections of this DPA unless otherwise stated.

1.3 Words used in the singular include the plural and vice versa, as the context may require.

1.4 Capitalized terms not defined herein shall have the meanings assigned to such terms in the Agreement.

1.5 Definitions:

(a) **“Affiliate”** means any entity that directly or indirectly controls, is controlled by, or is under common control with the subject entity. “**Control**”, for purposes of this definition, means direct or indirect ownership or control of more than 50% of the voting interests of the subject entity.

(b) “**Authorized Affiliate**” means any of Partner's Affiliate(s) which (a) is subject to the Data Protection Laws And Regulations of the European Union, the European Economic Area and/or their member states, Switzerland and/or the United Kingdom, and (b) is permitted to use the Services pursuant to the Agreement between Partner and OpsRamp, but has not signed its own agreement with OpsRamp and is not a "Partner" as defined under the Agreement.

(c) **“Controller” or “Data Controller”** means the entity which determines the purposes and means of the Processing of Personal Data. For the purposes of this DPA only, and except where indicated otherwise, the term "Data Controller" shall include yourself, the Organization and/or the Organization’s Authorized Affiliates.

(d) **“Data Protection Laws and Regulations”** means all laws and regulations, including, without limitation, laws and regulations of the European Union, the European Economic Area and their Member States, Switzerland and the United Kingdom, applicable to the Processing of Personal Data under the Agreement.

(e) **“Data Subject”** means the identified or identifiable person to whom the Personal Data relates.

(f) “**GDPR**” means the Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

(g) **“Member State”** means a country that belongs to the European Union and/or the European Economic Area. “Union” means the European Union.

(h) “**OpsRamp**” means the relevant OpsRamp entity of the following OpsRamp legal entities: OpsRamp Inc.

(i) “**OpsRamp Group**” means OpsRamp and its Affiliates engaged in the Processing of Personal Data.

(j) **"Personal Data"** means any information relating to an identified or identifiable natural person; an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

(k) **"Process(ing)"** means any operation or set of operations which is performed upon Personal Data, whether or not by automatic means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

(l) **"Processor" or "Data Processor"** means the entity which Processes Personal Data on behalf of the Controller.

(m) **"Security Documentation"** means the Security Documentation applicable to the specific Services purchased by Partner, or as shall be made available by OpsRamp. To receive a copy, please send a request to DPOoffice@opsramp.com

(n) **"Sub-processor"** means any Processor engaged by OpsRamp and/or OpsRamp.

(o) "**Supervisory Authority**" means an independent public authority which is established by an EU Member State pursuant to the GDPR.

2. PROCESSING OF PERSONAL DATA

2.1 **Roles of the Parties.** The Parties acknowledge and agree that with regard to the Processing of Personal Data, (i) Partner is the Data Controller, (ii) OpsRamp is the Data Processor and that (iii) OpsRamp or members of the OpsRamp Group may engage Sub-processors pursuant to the requirements set forth in Section 5 "Sub-processors" below.

2.1.1 This DPA is applicable in the following cases:

- If the Partner entity executing this DPA is a party to the Agreement, this DPA is an addendum to and forms part of the Agreement. In such case, the OpsRamp entity which is party to the Agreement is party to this DPA.
- If the Partner entity executing this DPA has executed an Order Form with OpsRamp or its Affiliate pursuant to the Agreement is not itself a party to the Agreement, this DPA is an addendum to that Order Form and applicable renewal Order Forms, and OpsRamp which is party to such Order Form is party to this DPA.
- If the Partner entity executing this DPA is neither a party to an Order Form nor the Agreement, this DPA is not valid and is not legally binding. Such entity should request that the Partner entity who is a party to the Agreement execute this DPA.
- If the Partner entity executing the DPA is not a party to an Order Form nor a Master Subscription Agreement directly with OpsRamp but is instead a customer indirectly via an authorized reseller and/or services partner of OpsRamp services, this DPA is not valid and is not legally binding. Such entity should contact the authorized reseller to discuss whether any amendment to its agreement with that reseller may be required. This DPA shall not replace any comparable or additional rights relating to Processing of Partner Data contained in Partner's Agreement (including any existing data processing addendum to the Agreement).

2.2 **Partner's Processing of Personal Data.** Partner shall, in its use of the Services, Process Personal Data in accordance with the requirements of Data Protection Laws and Regulations and always comply with the obligations applicable to data controllers. For the avoidance of doubt, Partner's instructions for the Processing of Personal Data shall comply with Data Protection Laws and Regulations. Partner shall have sole responsibility for the means by which Partner acquired Personal Data. Without limitation, Partner shall comply with any and all transparency-related obligations (including, without limitation, displaying any and all relevant and required privacy notices or policies) and shall have any and all required legal bases in order to collect, Process and transfer to OpsRamp the Personal Data and to authorize the Processing by OpsRamp of the Personal Data which is authorized in this DPA. Partner shall defend, hold harmless and indemnify OpsRamp, its Affiliates and subsidiaries (including without limitation their directors, officers, agents, subcontractors and/or employees) from and against any liability of any kind related to any breach, violation or infringement by Partner and/or its authorized users of any Data Protection Laws and Regulations and/or this DPA and/or this Section.

2.3 **OpsRamp's Processing of Personal Data.**

2.3.1 Subject to the Agreement, OpsRamp shall Process Personal Data in accordance with Partner's documented instructions for the following purposes: (i) Processing in accordance with the Agreement and this DPA and to provide the Services; (ii) Processing for Partner to be able to use the Services; (iii) Processing to comply with other documented reasonable instructions provided by Partner (e.g., via email) where such instructions are consistent with the terms of the Agreement; (iv) Processing as required by Union or Member State law to which OpsRamp is subject; in such a case, OpsRamp shall inform the Partner of the legal requirement before processing, unless that law prohibits such information on important grounds of public interest.

2.3.2 To the extent that OpsRamp cannot comply with a request from Partner and/or its authorized users relating to Processing of Personal Data (including, without limitation, any instruction, direction, code of conduct, certification, or change of any kind), OpsRamp (i) shall inform Partner, providing relevant details of the problem, (ii) OpsRamp may, without any kind of liability towards Partner, temporarily cease all Processing of the affected Personal Data (other than securely storing those data), and (iii) if the Parties do not agree on a resolution to the issue in question and the costs thereof, each Party may, as its sole remedy, terminate the Agreement and this DPA with respect to the affected Processing, and Partner shall pay to OpsRamp all the amounts owed to OpsRamp or due before the date of termination. Partner will have no further claims against OpsRamp (including, without limitation, requesting refunds for Services) due to the termination of the Agreement and/or the DPA in the situation described in this paragraph (excluding the obligations relating to the termination of this DPA set forth below).

2.3.3 OpsRamp will not be liable in the event of any claim brought by a third party, including, without limitation, a Data Subject, arising from any act or omission of OpsRamp, to the extent that such is a result of Partner’s instructions.

2.3.4 If Partner provides OpsRamp or any of the entities of the OpsRamp Group with instructions, requests, suggestions, comments or feedback (whether orally or in writing) with respect to the Services, Partner acknowledges that any and all rights, including intellectual property rights, therein shall belong exclusively to OpsRamp and that such shall be considered OpsRamp's intellectual property without restrictions or limitations of any kind, and Partner hereby irrevocably and fully transfers and assigns to OpsRamp any and all intellectual property rights therein and waives any and all moral rights that Partner may have in respect thereto.

2.4 **Details of the Processing.** The subject-matter of Processing of Personal Data by OpsRamp is the performance of the Services pursuant to the Agreement. The duration of the Processing, the nature and purpose of the Processing, as well as the types of Personal Data Processed and categories of Data Subjects under this DPA are further specified in Schedule 1 (Details of the Processing) to this DPA.

3. RIGHTS OF DATA SUBJECTS

3.1 **Data Subject Request.** OpsRamp shall, to the extent legally permitted, promptly notify Partner if OpsRamp receives a request from a Data Subject to exercise the Data Subject's right of access, right to rectification, erasure (“right to be forgotten”), restriction of Processing, data portability, right to object, or its right not to be subject to automated individual decision making (“Data Subject Request”). Taking into account the nature of the Processing, OpsRamp shall assist Partner by appropriate technical and organizational measures, insofar as this is possible, for the fulfilment of Partner’s obligation to respond to a Data Subject Request under Data Protection Laws and Regulations. In addition, to the extent Partner, in its use of the Services, does not have the ability to address a Data Subject Request, OpsRamp shall upon Partner’s request provide commercially reasonable efforts to assist Partner in responding to such Data Subject Request, to the extent OpsRamp is legally permitted to do so and the response to such Data Subject Request is required under Data Protection Laws and Regulations. To the extent legally permitted, Partner shall be responsible for any costs arising from OpsRamp's provision of such assistance.

4. OPSRAMP PERSONNEL

4.1 **Confidentiality.** OpsRamp shall ensure that its personnel engaged in the Processing of Personal Data have committed themselves to confidentiality and non-disclosure.

4.2 OpsRamp may disclose and Process the Personal Data (a) as permitted hereunder (b) to the extent required by a court of competent jurisdiction or other Supervisory Authority and/or otherwise as required by applicable laws or applicable Data Protection Laws and Regulations (in such a case, OpsRamp shall inform the Partner of the legal requirement before the disclosure, unless that law prohibits such information on important grounds of public interest), or (c) on a “need-to-know” basis under an obligation of confidentiality to its legal counsel(s), data protection advisor(s) and accountant(s).

5. AUTHORIZATION REGARDING SUB-PROCESSORS

5.1 **Appointment of Sub-processors.** Partner acknowledges and agrees that (a) OpsRamp's Affiliates may be used as Sub-processors; and (b) OpsRamp and/or OpsRamp's Affiliates respectively may engage third-party Sub-processors in connection with the provision of the Services.

5.2 **List of Current Sub-processors and Notification of New Sub-processors.**

5.2.1 OpsRamp shall make available to Partner the current list of Sub-processors used by sending a request to OpsRamp to DPOoffice@opsramp.com. Such Sub-processor list shall include the identities and details of those Sub-processors and their country of location (“**Sub-processor List**”). The Sub-processor List as of the date of execution of this DPA, or as of the date of publication (as applicable), is hereby, or shall be (as applicable), authorized by Partner. In any event, any intended change to the Sub-processor List shall be deemed authorized by Partner unless it provides a written reasonable objection for reasons related to the

GDPR within three (3) business days following the publication of changes to the Sub-processor List. In the event Partner reasonably objects to an intended new Sub-processor, as permitted in the preceding sentence, and the parties do not find a solution in good faith to the issue in question within a reasonable time period (not to exceed thirty (30) days), then Partner may, as its sole remedy, terminate the applicable Agreement and this DPA with respect only to those Services which cannot be provided by OpsRamp without the use of the objected-to new Sub-processor by providing written notice to OpsRamp provided that all amounts due under the Agreement before the termination date with respect to the Processing at issue shall be duly paid to OpsRamp. Until a decision is made regarding the new Sub-processor, OpsRamp may temporarily suspend the Processing of the affected Personal Data. Partner will have no further claims against OpsRamp due to (i) past use of approved Sub-processors prior to the date of objection or (ii) the termination of the Agreement (including, without limitation, requesting refunds) and the DPA in the situation described in this paragraph.

5.2.2 OpsRamp will send an email with the notification of any new Sub-processor(s) to Partner, before authorize such new Sub-processor(s) to Process Personal Data in connection with the provision of the Services.

5.3 **Agreements with Sub-processors**. OpsRamp shall respect the conditions referred to in Articles 28.2 and 28.4 of the GDPR when engaging another processor for Processing Personal Data provided by Partner. In accordance with Articles 28.7 and 28.8 of the GDPR, if and when the European Commission lays down the standard contractual clauses referred to in such Article, the Parties may revise this DPA in good faith to adjust it to such standard contractual clauses.

6. SECURITY

6.1 **Controls for the Protection of Personal Data.** OpsRamp shall maintain all industry-standard technical and organizational measures, and OpsRamp shall maintain the Personal Data secure throughout the data life cycle, required pursuant to Article 32 of the GDPR for protection of the security (including protection against unauthorized or unlawful Processing and against accidental or unlawful destruction, loss or alteration or damage, unauthorized disclosure of, or access to, Personal Data), confidentiality and integrity of Personal Data, as set forth in the Security Documentation which are hereby approved by Partner. OpsRamp regularly monitors compliance with these measures. Upon the Partner’s request, OpsRamp will assist Partner, at Partner’s cost, in ensuring compliance with the obligations pursuant to Articles 32 to 36 of the GDPR taking into account the nature of the processing and the information available to OpsRamp.

6.2 **Third-Party Certifications and Audits**. Upon Partner’s written request at reasonable intervals, and subject to the confidentiality obligations set forth in the Agreement and this DPA, OpsRamp shall make available to Partner that is not a competitor of OpsRamp (or Partner’s independent, third-party auditor that is not a competitor of OpsRamp) a copy of OpsRamp's then most recent third-party audits or certifications, as applicable (provided, however, that such audits, certifications and the results therefrom, including the documents reflecting the outcome of the audit and/or the certifications, shall only be used by Partner to assess compliance with this DPA and/or with applicable Data Protection Laws and Regulations, and shall not be used for any other purpose or disclosed to any third party without OpsRamp's prior written approval and, upon OpsRamp's first request, Partner shall return all records or documentation in Partner's possession or control provided by OpsRamp in the context of the audit and/or the certification). At Partner’s cost and expense, OpsRamp shall allow for and contribute to audits, including inspections, conducted by the controller or another auditor mandated by the controller (who is not a direct or indirect competitor of OpsRamp) provided that the parties shall agree on the scope, timing and conditions of such audits and inspections.

7. PERSONAL DATA INCIDENT MANAGEMENT AND NOTIFICATION

OpsRamp maintains security incident management policies and procedures specified in Security Documentation and, to the extent required under applicable Data Protection Laws and Regulations, shall notify Partner without undue delay after becoming aware of the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Personal Data, including Personal Data, transmitted, stored or otherwise Processed by OpsRamp or its Sub-processors of which OpsRamp becomes aware (a “**Personal Data Incident**”). OpsRamp shall make reasonable efforts to identify the cause of such Personal Data Incident and take those steps as OpsRamp deems necessary and reasonable in order to remediate the cause of such a Personal Data Incident to the extent the remediation is within OpsRamp's reasonable control. The obligations herein shall not apply to incidents that are caused by Partner or Partner’s users. In any event, Partner will be the party responsible for notifying supervisory authorities and/or concerned data subjects (where required by Data Protection Laws and Regulations).

8. RETURN AND DELETION OF PERSONAL DATA

Subject to the Agreement, OpsRamp shall, at the choice of Partner, delete or return the Personal Data to Partner (which is currently enabled via a download mechanism) after the end of the provision of the Services relating to processing, and shall delete existing copies unless applicable law requires storage of the Personal Data. In any event, to the extent required or allowed by applicable law, OpsRamp may retain one copy of the Personal Data for evidence purposes and/or for the establishment, exercise or defense of legal claims and/or to comply with applicable laws and regulations.

OpsRamp has made provision for retrieval of Partner data from the platform by authorization, to the extent allowed by applicable law, delete Partner Data in accordance with the procedures and timeframes specified in the Retention Policies.

9. AUTHORIZED AFFILIATES

9.1 **Contractual Relationship.** The Parties acknowledge and agree that, by executing the DPA, the Partner enters into the DPA on behalf of itself and, as applicable, in the name and on behalf of its Authorized Affiliates, thereby establishing a separate DPA between OpsRamp. Each Authorized Affiliate agrees to be bound by the obligations under this DPA. All access to and use of the Services by Authorized Affiliates must comply with the terms and conditions of the Agreement and this DPA and any violation of the terms and conditions therein by an Authorized Affiliate shall be deemed a violation by Partner.

9.2 **Communication.** The Partner shall remain responsible for coordinating all communication with OpsRamp under the Agreement and this DPA and shall be entitled to make and receive any communication in relation to this DPA on behalf of its Authorized Affiliates.

10. TRANSFERS OF DATA

10.1 **Transfers to countries that offer adequate level of data protection**: Personal Data may be transferred from the EU Member States, the three EEA member countries (Norway, Liechtenstein and Iceland) and the United Kingdom (collectively, "**EEA**") to countries that offer an adequate level of data protection under or pursuant to the adequacy decisions published by the relevant data protection authorities of the EEA, the Union, the Member States or the European Commission ("**Adequacy Decisions**"), without any further safeguard being necessary.

10.2 **Transfers to other countries**: If the Processing of Personal Data includes transfers from the EEA to countries which do not offer an adequate level of data protection or which have not been subject to an Adequacy Decision ("**Other Countries**"), the Parties shall comply with Article 46 of the GDPR, including, if necessary, executing the standard data protection clauses adopted by the relevant data protection authorities of the EEA, the Union, the Member States or the European Commission or comply with any of the other mechanisms provided for in the GDPR for transferring Personal Data to such Other Countries.

11. TERMINATION

This DPA shall automatically terminate upon the termination or expiration of the Agreement under which the Services are provided. Sections 2.2, 2.3.3, 2.3.4 and 12 shall survive the termination or expiration of this DPA for any reason.

12. RELATIONSHIP WITH AGREEMENT

In the event of any conflict between the provisions of this DPA and the provisions of the Agreement, the provisions of this DPA shall prevail over the conflicting provisions of the Agreement.

Notwithstanding anything to the contrary in the Agreement and/or in any agreement between the parties: (A) OpsRamp's (including OpsRamp's Affiliates') entire, total and aggregate liability, for any breach of this DPA and/or Data Protection Laws and Regulations, including, if any, any indemnification obligation regarding data protection or privacy, shall be limited to the amounts paid to OpsRamp under the Agreement within twelve (12) months preceding the event that gave rise to the claim. This limitation of liability is cumulative and not per incident; (B) In no event will OpsRamp and/or OpsRamp Affiliates and/or their third-party providers, be liable under, or otherwise in connection with this DPA for: (i) any indirect, exemplary, special, consequential, incidental or punitive damages; (ii) any loss of profits, business, or anticipated savings; (iii) any loss of, or damage to data, reputation, revenue or goodwill; and/or (iv) the cost of procuring any substitute goods or services; and (C) The foregoing exclusions and limitations on liability set forth in this Section shall apply: (i) even if OpsRamp, OpsRamp Affiliates or third-party providers, have been advised, or should have been aware, of the possibility of losses or damages; (ii) even if any remedy in this DPA fails of its essential purpose; and (iii) regardless of the form, theory or basis of liability (such as, but not limited to, breach of contract or tort).

13. AMENDMENTS

This DPA may be amended at any time by a written instrument duly executed by each of the Parties.

14. LEGAL EFFECT

This DPA shall only become legally binding between Partner and OpsRamp when the formalities steps set out in the Section "INSTRUCTIONS ON HOW TO EXECUTE THIS DPA" below have been fully completed.

15. EXECUTION

You will be presented an online form for completing all pertinent information necessary for execution of this DPA. This form will provide a method for accepting and executing this DPA. YOU ACKNOWLEDGE THAT YOUR ELECTRONIC SUBMISSIONS VIA SUCH FORM CONSTITUTE YOUR AGREEMENT AND INTENT TO BE BOUND BY THIS DPA.

The Parties represent and warrant that they each have the power to enter into, execute, perform and be bound by this DPA.

You, as the executing person on behalf of Partner, represent and warrant that you have, or you were granted, full authority to bind the Organization and, as applicable, its Authorized Affiliates to this DPA. If you cannot, or do not have authority to, bind the Organization and/or its Authorized Affiliates, you shall not supply or provide Personal Data to OpsRamp.

By executing this DPA, Partner enters into this DPA on behalf of itself and, to the extent required or permitted under applicable Data Protection Laws and Regulations, in the name and on behalf of its Authorized Affiliates, if and to the extent that OpsRamp processes Personal Data for which such Authorized Affiliates qualify as the/a "data controller".

This DPA has been pre-signed on behalf of OpsRamp.

<u>List of Schedules</u>

- **SCHEDULE 1 - DETAILS OF THE PROCESSING**
- **SCHEDULE 2 - INFORMATION SECURITY OF THE PLATFORM AND OPERATIONS**

OpsRamp's has duly executed this DPA:
OPSRAMP, INC.

Signature: DocuSigned by:
Curtis DiSibio
0ED7C3F5971347E...

Legal Name: Curtis DiSibio
Print Name: Curtis DiSibio
Title: CFO
Date: 7/10/2019

SCHEDULE 1 - DETAILS OF THE PROCESSING

Subject matter

OpsRamp will Process Personal Data as necessary to perform the Services pursuant to the Agreement, as further instructed by Partner in its use of the Services.

Nature and Purpose of Processing

1. Providing the Service(s) to Partner.
2. Setting up profile(s) for users authorized by Partners.
3. For Partner to be able to use the Services.
4. For OpsRamp to comply with documented reasonable instructions provided by Partner where such instructions are consistent with the terms of the Agreement.
5. Performing the Agreement, this DPA and/or other contracts executed by the Parties.
6. Providing support and technical maintenance, if agreed in the Agreement.
7. Resolving disputes.
8. Enforcing the Agreement, this DPA and/or defending OpsRamp's rights.
9. Management of the Agreement, the DPA and/or other contracts executed by the Parties, including fees payment, account administration, accounting, tax, management, litigation; and
10. Complying with applicable laws and regulations, including for cooperating with local and foreign tax authorities, preventing fraud, money laundering and terrorist financing.
11. All tasks related with any of the above.

Duration of Processing

Subject to any Section of the DPA and/or the Agreement dealing with the duration of the Processing and the consequences of the expiration or termination thereof, OpsRamp will Process Personal Data for the duration of the Agreement, unless otherwise agreed upon in writing.

Type of Personal Data

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

- First name
- Last name
- Phone number
- Email address
- Payment information
- Any other Personal Data or information that the Partner decides to provide to the OpsRamp or the Services
- Device IP Address for Authorized devices

The Partner and the Data Subjects shall provide the Personal data to OpsRamp by supplying the Personal data to OpsRamp's Service.

The Partner acknowledge that OpsRamp may use various software tools for storing such Personal Data in its repositories.

In some limited circumstances Personal Data may also come from others sources, for example, in the case of anti-money laundering research, fraud detection or as required by applicable law. For clarity, Partner shall always be deemed the “Data Controller” and OpsRamp shall always be deemed the “Data Processor” (as such terms are defined in the GDPR).

Categories of Data Subjects

Partner may submit Personal Data to the Services, the extent of which is determined and controlled by Partner in its sole discretion, and which may include, but is not limited to Personal Data relating to the following categories of data subjects:

- Partner’s customers and/or clients
- Partner’s users authorized by Partner to use the Services
- Employees, agents, advisors, freelancers of Partner (who are natural persons)

- business partners and vendors of Partner (who are natural persons)
- Employees or contact persons of Partner’s prospects, business partners and vendors

SCHEDULE 2
INFORMATION SECURITY OF THE PLATFORM AND OPERATIONS

OpsRamp currently observes the security practices described in this Schedule 2. Notwithstanding any provision to the contrary otherwise agreed to by Partner, OpsRamp may modify or update these practices at its discretion provided that such modification and update does not result in a material degradation in the protection offered by these practices. All capitalized terms not otherwise defined herein shall have the meanings as set forth in the Agreement.

1. **Access Control**

i) Preventing Unauthorized Product Access:

A. Outsourced processing: OpsRamp hosts its Service in a colocation and outsourced cloud infrastructure providers. OpsRamp maintains contractual relationships with vendors and, if applicable, Sub-processors in order to provide the Service in accordance with our DPA.

B. OpsRamp relies on contractual agreements, privacy policies, and vendor compliance programs to protect data processed or stored by these vendors.

C. Physical and environmental security: OpsRamp hosts its product infrastructure with multi-tenant, outsourced infrastructure providers. The physical and environmental security controls are audited for SOC1, SOC2 Type II and ISO 27001 compliance, among other certifications.

D. Authentication: OpsRamp implemented a unified password policy for its Platform.

E. Partner who interact with the platform via the user interface must authenticate before accessing their data. OpsRamp also has a provision for integrating with various single sign on tools or use OpsRamp's two-factor authentication mechanisms.

F. Authorization: Partner data is stored in multi-tenant storage systems accessible to Partner via only application user interfaces and application programming interfaces. Partner are not allowed direct access to the underlying application infrastructure. The authorization model in each of OpsRamp'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 role-based access policies defined by the Partner.

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

ii) Preventing Unauthorized Product Use:

OpsRamp implements standard access controls and detection capabilities for the internal networks that support its products.

A. Access controls: Network access control mechanisms are designed to prevent network traffic using unauthorized protocols from reaching the product infrastructure. The control measures are implemented by security group assignment, and traditional firewall rules.

B. Intrusion detection and prevention: OpsRamp implemented Firewalls designed to identify and prevent attacks against publicly available network services. A regular VA and PT assessment is carried on to proactively identify any threats and remediate as required.

C. Static code analysis: Security reviews of code stored in OpsRamp's source code repositories are performed which include checking for coding best practices and identifying software flaws.

iii) Limitations of Privilege & Authorization Requirements:

A. Product access: An authorized group of OpsRamp's employees have access to the Platform and to Partner data via controlled interfaces. The intent of providing access to an authorized employee is to provide effective customer support, to troubleshoot potential problems, to detect and respond to security incidents and implement data security. Access is enabled through a Service request process for all requests for access. Employees are granted access by role and responsibility. Employee roles are reviewed at least once every six months as part of Internal Security Audit.

B. Background checks: All OpsRamp's employees undergo a third-party background check prior to being extended an employment offer, in accordance with the applicable laws. All employees are required to conduct themselves in a manner consistent with company guidelines, non-disclosure requirements, and ethical standards.

2. Data Transfer Controls

I. In-transit: OpsRamp makes HTTPS encryption (also referred to as SSL or TLS) available on every one of its logins. Data is transmitted between POD's in same geographical regions.

II. At-rest: OpsRamp stores user passwords following policies that follow industry standard practices for security. OpsRamp has implemented technologies to ensure that stored data is encrypted at rest.

3. Data Input

I. Detection: OpsRamp has designed an internal monitoring and management systems to log information about the system behaviour, traffic received, system authentication, and other application requests. Internal systems alert appropriate Platform Support Groups of malicious, unintended, or anomalous activities. OpsRamp has established support process and personnel for security, operations to respond to various incidents.

II. Response and tracking: OpsRamp maintains a record of known security incidents that includes description, dates and times, priority and remediation process. 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, OpsRamp will take appropriate steps to minimize Product and Partner damage or unauthorized disclosure.

III. Communication: If OpsRamp becomes aware of unlawful access to Partner data stored within its products, OpsRamp will 1) notify the affected Partner of the incident; 2) provide a description of the steps taken to resolve the incident; and 3) provide status updates to the Partner contact, as OpsRamp deems necessary. Notification(s) of incidents, if any, will be delivered to one or more of the Partner's contacts in a form OpsRamp selects, which may include via email through Partner Support.

4. Availability Control

A. Infrastructure availability: OpsRamp is obligated to provide a minimum of 99.90% uptime for the Platform. The providers maintain a minimum of N+1 redundancy to power, network, and other Services in the Colocation.

B. Fault tolerance: Backup and replication strategies are designed to ensure redundancy and failover protections during a significant processing failure. Partner data is backed up to multiple durable data stores and replicated across multiple PODS. OpsRamp maintains an Active-Active set-up for disaster recovery 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 OpsRamp operations in maintaining and updating the product applications and backend while limiting downtime.

5. Audits and Certification

OpsRamp is SOC2 Type 2 Compliant.