

## **MASTER SERVICES AGREEMENT**

This Salt Security Master Services Agreement (“**Agreement**”) is made by and between Salt Security, Inc., a Delaware corporation with its principal place of business at 3921 Fabian Way, Palo Alto, California 94303 (“**Salt Security**”) and Customer (defined below) and governs Customer’s use of the Salt Security Platform (each as defined below).

“**Customer**” means a person or entity that accepts and agrees to the terms of this Agreement as of the earlier date (“**Effective Date**”) where such person or entity either clicks a box indicating acceptance of this Agreement or uses the Salt Security Platform. Salt Security reserves the right to modify or update this Agreement in its sole discretion, the effective date of such updates and/or modifications will be the earlier of: (i) 30 days from the date of such update or modification; or (ii) Customer’s continued use of the Salt Security Platform.

IF YOU DO NOT ACCEPT THIS AGREEMENT, YOU MAY NOT ACCESS OR USE THE SALT SECURITY PLATFORM. THE SALT SECURITY PLATFORM IS INTENDED FOR CUSTOMER AND ITS AUTHORIZED USERS ONLY AND ARE NOT FOR USE BY CHILDREN UNDER 13 YEARS OF AGE. IF AN INDIVIDUAL IS ENTERING INTO THIS AGREEMENT ON BEHALF OF A LEGAL ENTITY, SUCH PERSON REPRESENTS AND WARRANTS THAT IT HAS THE LEGAL AUTHORITY TO BIND SUCH LEGAL ENTITY TO THIS AGREEMENT AND THIS AGREEMENT APPLIES TO SUCH ENTITY WHICH IS DEEMED THE CUSTOMER.

If Customer and Salt Security have executed a written agreement governing Customer’s access to and use of the Salt Security Platform as a Salt Security customer, then the terms of such signed agreement will govern and supersede this Agreement.

The parties agree as follows:

1. **Definitions.** The definitions of certain capitalized terms used in this Agreement are set forth below. Others are defined in the body of the Agreement, an Order, in Salt Security’s DPA, or BAA.
  - a. “**Affiliate**” means any entity that Controls, is Controlled by, or is under common Control with the Customer.
  - b. “**Business Associate Agreement**” or “**BAA**” means Salt Security’s Business Associate Agreement, available at: <https://salt.security/business-associate-agreement>, unless the parties have executed a separate BAA in writing and in such case such other BAA applies.
  - c. “**Beta Features**” means any Salt Security Platform features, functionality, or services which Salt Security may make available to Customer to try at no additional cost, and which is designated as beta, trial, non-production or another similar designation.
  - d. “**Confidential Information**” means any information of a confidential or proprietary nature provided by a party to the other party, which includes any information that should be reasonably understood as confidential under the circumstances, including the terms of this Agreement and each Order, and: (i) with respect to Salt Security, the Salt Security Platform and Usage Data; and (ii) with respect to Customer, the Customer Data. Confidential Information does not include information that: (A) is or becomes public knowledge without any action by, or involvement of, the party to which the Confidential Information is disclosed; (B) is documented as being known to the Receiving Party prior to its disclosure by the Disclosing Party; (C) is independently developed by Receiving Party without reference or access to the Confidential Information of the Disclosing Party and is so documented; or (D) is obtained by Receiving Party without restrictions on use or disclosure from a third party.
  - e. “**Control**” means ownership, directly or indirectly, of 50% or more of the voting interest with the power to direct or cause the direction of the management and policies of such entity.
  - f. “**Customer Data**” means all data provided by, or on behalf of, Customer in connection with or by means of the Salt Security Platform, including any Personal Data as that term is defined under the DPA or as otherwise set under applicable laws. Notwithstanding anything to the contrary in this Agreement, Customer Data does not include Usage Data.
  - g. “**Customer Environment**” means equipment, systems and servers owned or managed solely by Customer.

- h. **“Data Processing Agreement”** or **“DPA”** means Salt Security’s Data Processing Addendum, available at: <https://salt.security/data-processing-addendum>, unless the parties have executed a separate DPA in writing and in such case such other DPA applies.
- i. **“Documentation”** means the user guides, operating manuals and all other materials provided by Salt Security that describe the installation, operation, use or technical specifications of the Salt Security Platform.
- j. **“Hosted Service”** means the cloud-based components of Salt Security’s proprietary API protection and cybersecurity platform.
- k. **“Implementation Services”** means services identified and performed by Salt Security but solely as necessary to implement the Salt Security Platform within the Customer Environment as required under the applicable order.
- l. **“Installed Software”** means any proprietary software provided by Salt Security to be installed by Customer solely for use with the Hosted Service.
- m. **“Malicious Code”** means viruses, worms, time bombs, Trojan horses and other harmful or malicious code, files, scripts, agents, or programs designed to intentionally disrupt or disable any systems, software, applications, files, or other data.
- n. **“Order”** means an ordering document for a subscription to access and use the Salt Security Platform: (i) signed in writing by Customer and Salt Security; (ii) purchased through the Salt Security Platform (e.g., by means of the Service dashboard); or (iii) via any third-party marketplace (e.g., via Amazon AWS Marketplace, Microsoft Azure).
- o. **“Prohibited Content”** means content that: (i) is illegal under any applicable law; (ii) violates any third-party rights including, but not limited to, privacy, intellectual property rights and trade secrets; (iii) contains false, misleading, or deceptive statements, depictions, or practices; or (iv) contains Malicious Code.
- p. **“Reseller”** means a third party authorized by Salt Security to sell subscriptions to access and use the Salt Security Platform.
- q. **“Salt Security Platform”** means the Hosted Service, Installed Software, Documentation, as well as all modifications, enhancements, updates, upgrades, patches, workarounds, and fixes, and any derivative works thereof, to each of the foregoing.
- r. **“Service Level Agreement”** is Salt Security’s standard service level agreement that applies to the Salt Security Platform located in Exhibit A attached hereto.
- s. **“Subscription Term”** is the length of the subscription specified in the applicable Order.
- t. **“Support Services”** has the meaning specified in Section 3(c) below.
- u. **“Taxes”** means any and all customs, duties, sales, use, value added, withholding, or other taxes, federal, state or otherwise, however designated, which are levied or imposed because of the transactions contemplated by this Agreement.
- v. **“Usage Data”** means data collected, anonymized and aggregated by Salt Security pertaining to Customer’s use and interaction with the Salt Security Platform, which includes, but is not limited to, Customer’s API environment, performance of the Salt Security Platform, metrics and other measures of Customer’s use and operation of the Salt Security Platform. Usage Data is not Customer Data and does not consist of Personal Data (as defined in the DPA).
- w. **“User”** means any individual employee, contractor or agent of Customer authorized by Customer to use the Salt Security Platform.

2. **Grant of License to the Salt Security Platform; Restrictions.**

a. **Grant of License to the Salt Security Platform & Installed Software.** Subject to the terms of this Agreement and the applicable Order, Salt Security grants Customer (and its Affiliates) a limited, non-exclusive, non-sublicensable, non-transferable (except as otherwise provided herein) license during the Subscription Term, solely for Customer's internal business operations: (i) to access and use the Salt Security Platform; and (ii) only if indicated in the applicable Order, to install and use the Installed Software within the Customer Environment solely in object code form.

b. **Salt Security Platform Restrictions.** Customer will not (and will not authorize or permit any third party to): (i) allow anyone other than Users to access and use the Salt Security Platform; (ii) share any Salt Security issued access credentials with any third party; (iii) sublicense, resell, lease, rent, loan, distribute, publish or otherwise make available or transfer rights or usage to all or any portion of the Salt Security Platform, or provide the Salt Security Platform on a timesharing, service bureau or other similar basis; (iv) access the Salt Security Platform in order to benchmark, or monitor the availability, security, performance, or functionality of the Salt Security Platform, for any competitive purposes without Salt Security's express written consent; (v) reverse engineer, decompile, disassemble, or otherwise attempt to discern the source code or interface protocols of the Salt Security Platform or any part thereof; (vi) modify, adapt, or translate the Salt Security Platform (whether in whole or in part) or remove or modify any proprietary markings or restrictive legends placed on or within the Salt Security Platform; (vii) make copies, store, or archive, any portion of the Salt Security Platform without the prior written permission of Salt Security except with respect to Installed Software subject to the terms of this Agreement; (viii) use the Salt Security Platform in violation of any applicable law; (ix) introduce, any Malicious Code into the Salt Security Platform or any part thereof; or (x) exploit the Salt Security Platform in any unauthorized manner including by circumventing any process Salt Security has put in place to safeguard the Salt Security Platform (e.g., those limiting certain Personal Data from being stored), or by deploying spiders, web-bots, screen-scrapers, or web crawlers, that may damage or adversely affect server or network capacity or Salt Security Platform infrastructure (together, (i) through (x) the "**Restrictions**"). The foregoing Restrictions will be inapplicable to the extent prohibited by applicable law.

c. **Trial Period.** Subject to the terms of the Agreement and Order, including payment of all Trial Period fees (if any), commencing on the Effective Date and for the period set forth on the Order, Customer will have the right to use the Salt Security Platform for evaluation purposes ("**Trial Period**"). Prior to the end of the Trial Period, Customer may terminate this Agreement without further obligation upon written notice to Salt Security ("**Trial Termination Notice**"). If Salt Security does not receive a Trial Termination Notice prior to the end of the Trial Period, the Subscription Term commences upon the expiration of the Trial Period, and Salt Security will invoice Customer in accordance with Section 7.

d. **Beta Features.** Beta Features made available by Salt Security are provided to Customer for testing purposes only. Salt Security makes no commitments to provide Beta Features in any future versions of the Salt Security Platform or otherwise. Customer is not obligated to use Beta Features. Salt Security may immediately and without notice remove Beta Features for any reason without liability to Customer. Notwithstanding anything to the contrary in this Agreement, Salt Security does not provide support for Beta Features. For clarity, all Beta Features are provided "AS IS" without warranty of any kind.

e. **Customer Affiliates.** Customer Affiliates may access and use the Salt Security Platform pursuant to this Agreement subject to the terms and conditions of this Agreement and as specified in the Order. Customer shall ensure that each such Affiliate complies with the terms and conditions of this Agreement and Customer shall be responsible and liable for any breach of this Agreement by any such Affiliate.

f. **Third-Party Applications.** The Salt Security Platform integrates with third party products, services, tools, or applications that are not owned or controlled by Salt Security ("**Third-Party Application(s)**"). Salt Security neither licenses Third Party Applications for Customer's benefit nor endorses any Third-Party Applications. This Agreement does not apply to such Third-Party Applications including Customer's use thereof. SALT SECURITY HAS NO LIABILITY OR OBLIGATION OF ANY KIND RELATED TO ANY THIRD-PARTY APPLICATIONS USED BY CUSTOMER.

3. **Salt Security Obligations for the Salt Security Platform.**

- a. **Salt Security Platform.** Salt Security will provide the Salt Security Platform in conformance with this Agreement, the Order and applicable Documentation. Salt Security will be responsible for hosting the Salt Security Platform as specified in the Order.
- b. **Updates.** Salt Security may update the Salt Security Platform from time to time during the Subscription Term. For clarity, Salt Security may enhance or modify the Salt Security Platform in its sole discretion, provided it does not materially reduce the core functionality of the Salt Security Platform.
- c. **Support Services.** Salt Security will provide Customer with Salt Security's standard level of support and uptime as set forth in the Salt Security Service Level Agreement (**Exhibit A**) at no additional charge ("**Support Services**"). Unless otherwise stated in an Order, the fee for Support Services is included in the cost of the subscription set forth in the applicable Order.
- d. **Implementation Services.** Unless otherwise stated in an Order, Salt Security will perform all Implementation Services subject to the fees specified in the Order.

4. **Customer Obligations.**

- a. **Internet Connections.** Customer will be responsible for obtaining Internet connections necessary for Customer to access the Salt Security Platform.
- b. **Access to the Customer Environment.** Customer will make available to Salt Security all reasonable access to the Customer Environment necessary for Salt Security to complete the Implementation Services and in relation to Support Services, including updating, maintaining, troubleshooting or similar activities necessary for Salt Security to deliver the Salt Security Platform. Salt Security will abide by Customer's written policies, provided to Salt Security in advance, with respect to access to and use of the Customer's Environment for performance of the Implementation Services and Support Services.
- c. **Installed Software & Updates.** Except where Implementation Services are specified to the contrary, Customer will be responsible for: (i) installing the Installed Software as provided for in the Documentation; and (ii) implementing Installed Software updates within the Customer Environment. Customer will implement such updates in a timely fashion. If Customer fails to do so, performance of the Salt Security Platform may be impacted.
- d. **Export.** The Salt Security Platform is subject to export control laws and regulations. Customer may not access or use the Salt Security Platform or any underlying information or technology except in full compliance with all applicable United States export control laws. Neither the Salt Security Platform nor any underlying information or technology may be accessed or used: (i) by any individual or entity in any country to which the United States has embargoed goods; or (ii) by anyone on the U.S. Treasury Department's list of specially designated nationals or the U.S. Commerce Department's list of prohibited countries or debarred or denied persons or entities.
- e. **User Accounts & Passwords.** Customer will safeguard and ensure that all Users safeguard User accounts and passwords. Customer will notify Salt Security immediately if it learns of any unauthorized use of any User accounts or passwords or any other known or suspected breach of security.

5. **Data License & Protections.**

- a. **Data License.** In connection with its use of the Salt Security Platform, Customer (including its Users) may transfer Customer Data to Salt Security. Salt Security uses and processes Customer Data to provide the Salt Security Platform and to create and develop Usage Data (i.e., that Salt Security uses to develop and improve the Salt Security Platform). Customer grants Salt Security a limited license during each Subscription Term to use Customer Data as provided for in this Section 5(a) and in accordance with this Agreement and the DPA.
- b. **DPA.** Salt Security will process all Customer Data for the purposes set forth in this Agreement and in accordance with the DPA.

c. BAA. Salt Security will process all Customer Data that is PHI (as defined in the BAA) for the purposes set forth in this Agreement and in accordance with the BAA but only to the extent indicated in an Order and when Customer is a Covered Entity as defined in the BAA or under applicable law.

d. Security & Privacy. Salt Security maintains industry-standard physical, technical, and administrative safeguards to protect Customer Data in accordance with the Salt Security's "**Security Protocols**" set forth in the DPA.

6. Fees.

a. Payments. Salt Security will invoice Customer for all fees and any applicable taxes as provided in the applicable Order and subsequent invoice. Unless otherwise provided for in an Order: (i) all amounts are due and payable to Salt Security within thirty (30) days from the date of Salt Security's invoice; and (ii) all fees are based on the Salt Security Platform purchased, not on actual use and are non-refundable.

b. Taxes. Customer will pay all applicable Taxes excluding only those based on Salt Security's net income. If Customer is compelled to make a deduction or set-off for any such Taxes, Customer will pay Salt Security such additional amounts as necessary to ensure receipt by Salt Security of the full amount Salt Security would have received but for the deduction. Any applicable direct pay permits or valid Tax-exempt certificates must be provided to Salt Security prior to the execution of this Agreement. If Salt Security is required to collect and remit Taxes on Customer's behalf, Salt Security will invoice Customer for such Taxes, and Customer will pay Salt Security for such Taxes in accordance with Section 6(a).

c. Late Payments. In the event that Salt Security does not receive any invoiced amount by the due date as set forth in Section 6(a), without limiting its rights and remedies, Salt Security may: (i) charge interest on the outstanding balance (at a rate not to exceed the lesser of one and one half percent (1.5%) per month or the maximum rate permitted by law); (ii) condition future Salt Security Platform renewals and additional Orders on payment terms shorter than those specified in Section 6(a); and/or (iii) suspend and terminate for failure to pay (if applicable) the Salt Security Platform pursuant to Section 7(b).

d. Additional Capacity. If Customer exceeds any capacity set forth in the Order, whichever party first discovers such overage must contact the other party ("**Overage Notice Date**") to discuss the overage and determine a plan to either reduce such capacity in future months or purchase additional capacity. If the parties cannot agree upon an increased capacity plan for Customer within 60 days of the API Overage Notice Date, Salt Security (or Reseller, if applicable) is hereby authorized to invoice Customer (and Customer shall pay, no later than thirty (30) days after the invoice date, unless otherwise provided in the Order) for such increased capacity at the rates applicable during Customer's current subscription term, prorated for the remainder of the Term. Any such additional capacity, and corresponding fees, shall apply for the remainder of the Subscription Term.

7. Term & Termination.

a. Term. The "**Term**" of the Agreement commences on the Effective Date and will continue in effect thereafter so long as there is an active Subscription Term under an Order, or until terminated earlier in accordance with Section 7(b). For clarity, each Subscription Term will be set forth in the applicable Order.

b. Suspension & Termination for Non-Payment. Salt Security may suspend Customer's access to, or use of, the Salt Security Platform upon written notice to Customer if any amount due to Salt Security under any invoice is past due. If Customer fails to pay within 30 days of receipt of Salt Security's notice of suspension for late payment, Salt Security may terminate this Agreement and/or the applicable Order immediately upon written notice to Customer.

c. Termination. Either party may terminate this Agreement and/or any Order: (i) upon thirty (30) days' notice to the other party if the other party materially breaches this Agreement and such breach remains uncured at the expiration of such thirty (30) day period; or (ii) immediately, if the other party becomes the subject of a petition in bankruptcy or any other proceeding relating to insolvency, liquidation, or assignment for the benefit of creditors.

d. Effect of Termination. If Customer terminates this Agreement in accordance with Section 7(c)(i), Salt Security will reimburse Customer on a pro-rata basis for any pre-paid fees allocable to the remaining Subscription

Term as of the date of such termination. Upon termination or expiration of this Agreement for any reason, Salt Security will, upon written request and within 30 days of such request, delete all Customer Data processed on behalf of Customer during the Subscription Term as specified in the DPA.

e. Survival. The following provisions will survive any expiration or termination of the Agreement: Sections 8 (Confidentiality), 9 (Ownership), 11 (Indemnification), 12 (Limitation on Liability), and 17 (Miscellaneous, as applicable).

8. **Confidentiality**.

a. Each party that receives (“**Receiving Party**”) Confidential Information of the other party (“**Disclosing Party**”) will protect and preserve such Confidential Information as confidential, using no less care than that with which it protects and preserves its own confidential and proprietary information (but in no event less than a reasonable degree of care), and will not use or disclose the Confidential Information for any purpose except to perform its obligations and exercise its rights under this Agreement and applicable Order(s).

b. Receiving Party may disclose, distribute, or disseminate Disclosing Party’s Confidential Information to any of its officers, directors, members, managers, partners, employees, contractors, or agents (its “**Representatives**”), provided Receiving Party reasonably believes that its Representatives have a need to know, and such Representatives are bound by confidentiality obligations at least as restrictive as those contained herein. The Receiving Party will at all times remain responsible for any violations of this Agreement by any of its Representatives.

c. A Receiving Party will not violate its confidentiality obligations if it discloses Disclosing Party’s Confidential Information if required by applicable laws, including by court subpoena or similar instrument so long as the Receiving Party provides the Disclosing Party with written notice of the required disclosure to allow the Disclosing Party to contest or seek to limit the disclosure or obtain a protective order. If no protective order or other remedy is obtained, the Receiving Party will furnish only that portion of the Confidential Information that is legally required and agrees to exercise reasonable efforts to ensure that confidential treatment will be accorded to the Confidential Information so disclosed.

d. Each party acknowledges that any violation or threatened violation of this Section 8 may cause irreparable injury to the other party, entitling the other party to seek injunctive relief in addition to all legal remedies.

9. **Ownership**.

a. Salt Security Property. Salt Security owns and retains all right, title, and interest in and to the Salt Security Platform (including for clarity any part thereof). Except for the limited license granted to Customer in Sections 2(a) and 2(b), Salt Security does not by means of this Agreement or otherwise transfer any other rights to Customer.

b. Customer Property. Customer owns and retains all right, title, and interest in and to the Customer Data. Except for the licenses granted to Salt Security in Section 5(a), Customer does not by means of this Agreement or otherwise transfer any other rights to Salt Security.

c. Feedback. Customer may provide comments, suggestions, and recommendations to Salt Security with respect to the Salt Security Platform and aspects thereof (including, without limitation, comments, suggestions, and recommendations with respect to modifications, enhancements, improvements and other changes to each of the foregoing) (collectively, “**Feedback**”). Salt Security may freely use and exploit any such Feedback without any obligation to Customer, unless otherwise agreed upon by the parties in writing.

10. **Representations & Warranties; Disclaimer**.

a. Mutual Representations and Warranties. Each party represents and warrants it has validly entered into this Agreement and has the legal power to do so.

b. Customer Representations and Warranties. Customer represents and warrants it: (i) is entitled to transfer, or enable the transfer of, all Customer Data to Salt Security; (ii) has all licenses, permissions, consents and rights necessary to grant Salt Security the licenses set forth in this Agreement and enable the Implementation Services; and

(iii) will not transmit any Prohibited Content to Salt Security whether by means of the Salt Security Platform or as required for Salt Security's provision of Support Services hereunder.

c. Disclaimer. WITH THE EXCEPTION OF THE LIMITED WARRANTIES SET FORTH IN THIS SECTION 10, THE IMPLEMENTATION SERVICES, SALT SECURITY PLATFORM AND BETA FEATURES ARE PROVIDED "AS IS" TO THE FULLEST EXTENT PERMITTED BY LAW. SALT SECURITY AND ITS LICENSORS EXPRESSLY DISCLAIM ALL OTHER WARRANTIES, EXPRESS OR IMPLIED, INCLUDING WARRANTIES OF PERFORMANCE, MERCHANTABILITY, FITNESS FOR ANY PARTICULAR PURPOSES, AND NON-INFRINGEMENT. SALT SECURITY DOES NOT WARRANT THAT THE IMPLEMENTATION SERVICES, SALT SECURITY PLATFORM OR BETA FEATURES: (I) ARE ERROR-FREE; (II) WILL PERFORM UNINTERRUPTED; OR (III) WILL MEET CUSTOMER'S REQUIREMENTS.

11. **Indemnification.**

a. By Salt Security.

- i. Salt Security will defend Customer, and its Affiliates, including each of the foregoing's officers, directors, employees and agents (collectively, "**Customer Indemnified Parties**"), from any third-party claim, demand, dispute, suit or proceeding, and Salt Security will indemnify Customer Indemnified Parties from and against any related losses, liabilities, damages, costs or expenses (including, without limitation, reasonable attorneys' fees), finally awarded against the Customer Indemnified Parties to such third party, by a court of competent jurisdiction or agreed to in settlement, alleging that the Salt Security Platform, including Customer's permitted use thereof, infringes any registered United States patent, trademark, copyright or misappropriates a trade secret of such third party.
- ii. If Salt Security becomes, or in Salt Security opinion is likely to become, the subject of an infringement or misappropriation claim, Salt Security may, at its option and expense: (a) procure for Customer the right to continue using the Salt Security Platform (or the component thereof subject of such infringement); (b) replace the Salt Security Platform (including any component part) with a non-infringing substitute subject to Customer's prior written approval; or (c) modify the Salt Security Platform so that it becomes non-infringing. If none of the foregoing alternatives are available, Salt Security shall notify Customer, and Customer may elect to terminate the license immediately pursuant to Section 7(c) and refund Customer the pro-rata, unused portion of any prepaid fees.
- iii. Salt Security will not be obligated to defend or be liable for costs or damages solely to the extent the infringement or misappropriation is attributable to: (a) Third-Party Applications; (b) Customer Data; (c) modifications to the Salt Security Platform made other than by Salt Security, but only to the extent such claim would not have arisen but for such modification; (d) combination of the Salt Security Platform with a non-Salt Security application, product, data or business process, but only to the extent such claim would not have arisen but for such combination; (e) continued use of the Salt Security Platform after Customer has been notified of modifications or substitutes to the extent use of such modifications or substitutes would have prevented the claim; (f) any use of the Salt Security Platform other than the most current version made available to Customer; or (g) use of the Salt Security Platform that violates the terms of this Agreement to the extent such claim would not have arisen but for such violation.
- iv. Customer's sole and exclusive remedy and the entire liability of Salt Security, its officers, directors, employees, shareholders, contractors, and representatives, with respect to any and all claims relating to alleged infringement of a third-party's intellectual property rights, will be pursuant to the indemnification provisions set forth in this Section 11(a).

b. By Customer. Customer will defend Salt Security, and its Affiliates, including each of the foregoing's officers, directors, employees and agents (collectively, "**Salt Security Indemnified Parties**"), from any third-party claim, demand, dispute, suit or proceeding, and Customer will indemnify the Salt Security Indemnified Parties from and against any related losses, liabilities, damages, costs or expenses (including, without limitation, attorneys' fees), finally awarded against the Salt Security Indemnified Parties related to: (i) Customer or a User violating a Restriction; (ii) Customer's breach of Section 10(b) (Customer Representations & Warranties); or (iii) any allegation by a governmental body that use of Customer Data, as permitted by Salt Security under this Agreement or at Customer's request or direction, has violated any applicable law.

c. **Indemnification Process.** The indemnified parties will: (i) give the indemnifying party prompt written notice of any claim, action or demand for which indemnity is claimed; (ii) give the indemnifying party sole control over the defense and settlement of the claim, provided that the indemnifying party will not settle any claim that involves the payment of money or acknowledgement of wrongdoing on the part of the indemnified parties without indemnified parties' prior written approval such approval not to be unreasonably withheld, conditioned or delayed; and (iii) provide the indemnifying party with reasonable cooperation, at the indemnified parties' expense, in connection with the defense and settlement of the claim.

12. **Limitation on Liability.**

a. NEITHER PARTY, NOR ITS AFFILIATES, NOR THE OFFICERS, DIRECTORS, EMPLOYEES, SHAREHOLDERS, OR REPRESENTATIVES OF ANY OF THEM, WILL BE LIABLE TO THE OTHER PARTY FOR ANY INCIDENTAL, INDIRECT, SPECIAL, EXEMPLARY OR CONSEQUENTIAL DAMAGES, THAT MAY ARISE OUT OF THIS AGREEMENT, EVEN IF THE OTHER PARTY HAS BEEN NOTIFIED OF THE POSSIBILITY OR LIKELIHOOD AND WHETHER BASED ON CONTRACT, TORT, NEGLIGENCE, STRICT LIABILITY, SERVICES LIABILITY OR OTHERWISE.

b. EXCEPT WITH RESPECT TO UNCAPPED CLAIMS (DEFINED BELOW), IN NO EVENT WILL THE COLLECTIVE LIABILITY OF EITHER PARTY, OR THEIR RESPECTIVE AFFILIATES, OFFICERS, DIRECTORS, EMPLOYEES, SHAREHOLDERS, AGENTS AND REPRESENTATIVES, TO THE OTHER PARTY FOR ANY AND ALL DAMAGES, INJURIES, AND LOSSES ARISING FROM ANY AND ALL CLAIMS AND CAUSES OF ACTION ARISING OUT OF, BASED ON, RESULTING FROM, OR IN ANY WAY RELATED TO THIS AGREEMENT, EXCEED THE TOTAL AMOUNT OF FEES PAID BY CUSTOMER FOR USE OF THE SALT SECURITY PLATFORM DURING THE PERIOD TWELVE (12) MONTHS PRIOR TO THE EVENT GIVING RISE TO THE CLAIM.

THE EXISTENCE OF MULTIPLE CLAIMS OR SUITS UNDER OR RELATED TO THIS AGREEMENT WILL NOT ENLARGE OR EXTEND THE LIMITATION OF MONEY DAMAGES WHICH WILL BE THE CLAIMANT'S SOLE AND EXCLUSIVE REMEDY.

c. **"Uncapped Claims"** means any claim or liability associated with: (i) either party's breach of Section 8 (Confidentiality) but not relating to any liability associated with Salt Security's privacy and/or security obligations with respect to Customer Data which remains subject to the Excluded Claims cap; (ii) either party's respective indemnification obligations under Section 11; or (iii) any liability of a party which cannot be limited under applicable law, including gross negligence, recklessness, or intentional misconduct.

13. **Insurance.** Salt Security will maintain in full force and effect during the Term:

a. Commercial general liability insurance on an occurrence basis for bodily injury, death, property damage, and personal injury, with coverage limits of not less than \$1,000,000 per occurrence and \$2,000,000 general aggregate for bodily injury and property damage;

b. Worker's compensation insurance as required by applicable law; and

c. Technology Errors & Omissions and Cyber-risk on an occurrence or claims-made form, for limits of not less than \$5,000,000 annual aggregate covering liabilities for financial loss resulting or arising from acts, errors or omissions in the rendering of the Salt Security Platform, or from data damage, destruction, or corruption, including without limitation, unauthorized access, unauthorized use, virus transmission, denial of service, and violation of privacy from network security failures in connection with the Salt Security Platform.

Insurance carriers will be rated A-VII or better by A.M. Best Provider. Salt Security's coverage will be considered primary without right of contribution of Customer's insurance policies. In no event will the foregoing coverage limits affect or limit in any manner Salt Security's contractual liability for indemnification or any other liability of Salt Security under this Agreement.

14. **United States Government Users.** The Salt Security Platform is commercial computer software, as such term is defined in 48 C.F.R. §2.101. Accordingly, if Customer is the U.S. Government or any contractor therefor,



Customer shall receive only those rights with respect to the Salt Security Platform as are granted to all other end users under license, in accordance with (a) 48 C.F.R. §227.7201 through 48 C.F.R. §227.7204, with respect to the Department of Defense and their contractors, or (b) 48 C.F.R. §12.212, with respect to all other U.S. Government licensees and their contractors.

15. **Force Majeure.** Except for Customer's payment obligations hereunder, neither Salt Security nor Customer will be liable by reason of any failure or delay in the performance of its obligations on account of events beyond the reasonable control of a party, which may include denial-of-service attacks, a failure by a third-party hosting provider or utility provider, strikes, shortages, riots, fires, acts of God, war, terrorism, pandemics and governmental action (each, a "**Force Majeure Event**"). For clarification, events caused by a party's own action are not Force Majeure Events. If a Force Majeure Event prevents Salt Security from providing the Salt Security Platform for at least thirty (30) consecutive days, either of the parties may immediately terminate this Agreement and any Order, by providing written notice to the other.

16. **Marketing Logo Rights.** Customer grants Salt Security the right to use Customer's name and logo on Salt Security's website, and in its portfolio for sales, promotional or marketing purposes, for the sole purpose of identifying Customer as a customer.

17. **Miscellaneous.** This Agreement is the entire agreement between the parties and supersedes all prior agreements and understandings concerning the subject matter hereof. The parties are independent contractors, and this Agreement will not establish any relationship of partnership, joint venture, or agency between the parties. Failure to exercise any right under this Agreement will not constitute a waiver. There are no third-party beneficiaries to this Agreement. This Agreement is governed by the laws of California without reference to conflicts of law rules. For any dispute relating to this Agreement, the parties consent to personal jurisdiction and the exclusive venue of the courts in Santa Clara County, California. Any notice provided by one party to the other under this Agreement will be in writing and sent by overnight courier or certified mail (receipt requested) to the address above. If any provision of this Agreement is found unenforceable, this Agreement will be construed as if it had not been included. Neither party may assign this Agreement without the prior, written consent of the other party, except that either party may assign this Agreement without such consent: (i) to an Affiliate of the assigning party; and/or (ii) in connection with an acquisition of a party or a sale of all or substantially all of its assets. This Agreement may be executed in two or more counterparts, each of which will be deemed an original, but all of which together will constitute one and the same instrument. Facsimile or other electronic copies of such signed copies will be deemed to be binding originals. To the extent there is an inconsistency between the terms of the Agreement, Order, and DPA, such documents and their terms will be controlled in the following order of precedence: (i) Order; (ii) Agreement; (iii) DPA; and (iv) BAA (if applicable).

## **Exhibit A**

### **Service Level Agreement & Support Services**

#### **Monthly Uptime Percentage:**

The Salt Security Platform will achieve a Monthly Uptime Percentage of at least 99.9% of the time in any calendar month. Customer may obtain real-time metrics regarding Salt Security's performance against the Monthly Uptime Percentage on the self-service Salt Security Status Page (<https://saltsecurity.statuspage.io/#>).

**"Downtime"** means the Salt Security Platform is not operating in material accordance with the Documentation.

**"Monthly Uptime Percentage"** means the total number of minutes in a calendar month minus the number of minutes of Downtime suffered in a calendar month, divided by the total number of minutes in a calendar month.

Downtime caused by any of the following will be excluded from the calculation of the Monthly Uptime Percentage: (a) an act or omission by Customer that does not strictly comply with this Agreement; (b) Customer's Internet connectivity; (c) factors described in Section 15 of the Agreement ("Force Majeure"); (d) failure, interruption, outage or other problem with any Third-Party Application; (e) scheduled outages of the Salt Security Platform; or (f) disabling, suspension or termination of the Salt Security Platform in accordance with Section 7 of the Agreement ("Term and Termination").

#### **Support Services:**

Live support: 2am-10pm (Eastern Time)

Customer will appoint a single support liaison (and one backup) to communicate with Salt Security's support personnel. Salt Security will not be obligated to answer support inquiries from any other contact.

Support requests can be submitted via the Salt console, via the Salt Security Support Portal at <https://support.salt.security/hc/en-us>, or emailed to [support@salt.security](mailto:support@salt.security) anytime (24x7) and will be handled during live support hours.

Salt Security will not be obligated to provide support to the extent arising from: (i) Customer's failure to implement any update or enhancement made available to Customer by Salt Security at no charge for addressing such error; (ii) changes by Customer or third parties to the operating system, network configuration or environment; (iii) any customization of the Salt Security Platform for Customer, whether or not performed by Salt Security, Customer or a third party; (iv) use of the Salt Security Platform in a manner for which it is not designed or other than as specified in the applicable Documentation; or (v) the combination, use or interconnection of the Salt Security Platform with other software or hardware not supplied and not approved by Salt Security.