Menlo Security End User License Agreement

This End User License Agreement ("**EULA**") between You and Menlo Security, Inc. ("**Menlo Security**") sets forth the terms and conditions that govern Your use of the Menlo Security Software and Cloud Services (collectively, the "**Menlo Security Technology**"). Definitions of capitalized terms are set forth in Section 12 (Definitions).

YOU AGREE TO BE BOUND BY THE TERMS OF THIS EULA BY (A) EXECUTING A WRITTEN ORDER FORTHEMENLO SECURITY TECHNOLOGY, OR (B) BY YOUR EXPRESS AGREEMENT. IF YOU DO NOT HAVE THE AUTHORITY TO ENTER INTO THIS EULA OR YOU DO NOT AGREE WITH ITS TERMS, DO NOT USE THE MENLO SECURITY TECHNOLOGY. IF YOU PROCEED WITH DOWNLOAD, INSTALLATION, ACCESS, DEPLOYMENT, OR USE, YOU ARE REPRESENTING AND WARRANTING THAT YOU HAVE AUTHORITY TO ENTER INTO THIS EULA. THIS PARAGRAPH DOES NOT APPLY WHERE YOU HAVE EXPRESSLY AGREED TO SEPARATE END USER LICENSE TERMS WITH MENLO SECURITY EITHER DIRECTLY OR AS PART OF A TRANSACTION WITH AN APPROVED PARTNER.

SECTION 1. USE OF THE MENLO SECURITY TECHNOLOGY

1.1 LICENSE GRANT. Subject to the terms of this Agreement, Menlo Security hereby grants You a limited, non-sub-licensable, non-transferable, non-exclusive, (a) license to use the Software and (b) right to access and use the Cloud Services, both solely for Your internal business purposes, for the duration of the Subscription Term, and in accordance with the Order, this EULA, and any related Documentation (collectively, "**Use Rights**").

1.2 USE BY THIRD PARTY AGENTS. You may permit Your Third Party Agents to exercise the Use Rights on Your behalf solely for Your internal business purposes and provided: (a) You ensure such Third Party Agents comply with this EULA and (b) You are responsible for any breach of this EULA by such Third Party Agents.

1.3 BETA AND EVALUATION USE. If Menlo Security grants You Use Rights of the Menlo Security Technology for trial, evaluation or beta purposes ("**Evaluation Technology**"), the Evaluation Technology is provided "AS-IS" without any express or implied warranty, indemnity, or support of any kind and Menlo Security will have no liability relating to Your use of the Evaluation Technology. Except as agreed in writing by Menlo Security, Your use of the Evaluation Technology is limited to non-production internal use. You may use the Evaluation Technology for a limited period of thirty (30) days, unless otherwise agreed to in writing by Menlo Security ("**Evaluation Term**"). Menlo Security may modify or discontinue Your use of the Evaluation Technology at any time. If you do not discontinue use of and/or return the Evaluation Technology at the end of the Evaluation Term, Menlo Security reserves the right to invoice You for the list price and You agree to pay such invoice.

1.4 INTEROPERABILITY. Notwithstanding the foregoing and solely to the extent required by applicable law to achieve interoperability between Menlo Security's Software and other software, Menlo Security will provide such interoperability information to You, provided You agree to any additional terms reasonably required by Menlo Security and such interoperability information is considered Menlo Security Confidential Information.

SECTION 2. RESTRICTIONS AND OBLIGATIONS

2.1 RESTRICTIONS. You will not and will not allow any third party to: (a) copy, modify, transfer, sell, or distribute the Menlo Security Technology; (b) reverse engineer, decrypt, disassemble, decompile or create derivative works of the Menlo Security Technology; (c) attempt to discover the source code or structure, sequence and organization of the Menlo Security Technology (except where the foregoing is expressly permitted by applicable local law, and then only to the extent so permitted); (d) rent, lease, or use the Menlo Security Technology for timesharing or service bureau purposes, or otherwise use the Menlo Security Technology on behalf of any third party; or (e) use the Menlo Security Technology for performing comparisons or other "benchmarking" activities, either alone or in connection with any software (and You will not publish or disclose any such performance information or comparisons). You shall maintain and not remove or obscure any proprietary notices on the Menlo Security Technology.

2.2 CUSTOMER RESPONSIBILITIES. You agree that You are responsible for: (a) all activity of Your Authorized Users and Third Party Agents; (b) Your Authorized Users' and Third Party Agents' compliance with this EULA; (c)

keeping Your account information up to date and using reasonable means to protect Your account information; and (d) Customer Data. If You become aware of an Authorized User's or Third Party Agent's violation of this EULA, You must promptly suspend such use of the Menlo Security Technology.

2.3 SUPPORT OBLIGATIONS. Menlo Security will provide the level of support set forth on the Order, unless You are receiving support directly from Your Approved Partner. Menlo Security offers standard technical support at no additional fee and upgraded support options for an additional fee.

2.4 MODIFICATIONS. Menlo Security may modify, enhance or refine a Cloud Service, provided that Menlo Security will not materially reduce the core functionality of that Cloud Service. Additionally, Menlo Security may perform scheduled maintenance of the infrastructure and software used to provide a Cloud Service, during which time You may experience some disruption to that Cloud Service, provided that Menlo Security will provide You with advance notice of such maintenance, when reasonably practicable.

SECTION 3. INTELLECTUAL PROPERTY OWNERSHIP

3.1 OWNERSHIP OF MENLO SECURITY TECHNOLOGY. Menlo Security and its licensors own all right, title and interest in and to the Menlo Security Technology, Menlo Security Content and Documentation, as well as any modifications that are derivative works of the Menlo Security Technology, Menlo Security Content and Documentation. Your rights to use the Menlo Security Technology are limited to those expressly granted in this EULA and any applicable Order. No other rights with respect to the Menlo Security Technology or any related intellectual property rights are implied. Menlo Security reserves all rights not expressly granted to You and does not transfer any ownership rights in any Software or Cloud Service.

3.2 OWNERSHIP OF CUSTOMER DATA. You retain all right, title and interest in Customer Data. Menlo Security may use any feedback You provide in connection with Your use of the Menlo Security Technology as part of its business operations.

3.3 OWNERSHIP OF MENLO SECURITY CONTENT. Without limiting the confidentiality obligations set forth in this EULA, Menlo Security retains all right, title and interest in the Menlo Security Content. Nothing herein shall be construed as prohibiting Menlo Security from utilizing the Menlo Security Content for purposes of operating Menlo Security's business, provided that the Menlo Security Content does not include Your Confidential Information, Customer Data or any information that personally identifies a specific individual.

SECTION 4. ORDERS, FEES, AND PAYMENT

4.1 ORDERS. Your Order is subject to this EULA. If You are entitled to a refund under this EULA, such refund will be remitted to You or if purchasing through an Approved Partner, to Your Approved Partner.

4.2 DIRECT ORDERS. Sections 4.2 through 4.4 apply only to Orders placed directly with Menlo Security. If You purchase the Menlo Security Technology through an Approved Partner, all terms regarding invoicing, payment and tax are between You and such Approved Partner.

4.3 FEES AND PAYMENT. The Fees shall be set forth in each Order. Unless otherwise set forth in an Order, all fees are due and payable net thirty (30) days from the receipt date of invoice. Menlo Security is entitled to charge interest on any sum that is not paid when due at the interest rate established by the Secretary of the Treasury as provided in 41 U.S.C. 7109, which is applicable to the period in which the amount becomes due, and then at the rate applicable for each six-month period as fixed by the Secretary until the amount is paid.

4.4 TAXES. Menlo shall state separately on invoices taxes excluded from the fees, and You agree either to pay the amount of the taxes or provide evidence necessary to sustain an exemption, in accordance with FAR 552.212-4(k).

4.5 VERIFICATION. You will maintain for the duration of the Subscription Term and for a period of one (1) year after its termination or expiration, complete and accurate records of Your use of the Menlo Technology to verify compliance with this EULA ("**Records**"). Upon reasonable notice and no more than once per year, Menlo Security and/or its auditors will have the right subject to Government security requirements to access Your applicable books, systems, records, and accounts during Your normal business hours to verify such compliance. If the audit process discloses underpayment of fees, Menlo Security reserves the right to invoice You or Your Authorized Partner for such fees.

SECTION 5. TERM AND TERMINATION

5.1 TERM AND RENEWAL. The initial term of Your subscription to the Menlo Security Technology will begin on the Start Date set forth in an Order and will continue for a period of twelve (12) months, or as otherwise set forth in an Order **("Initial Subscription Term")**. Your subscription to the Menlo Security Technology may be renewed for additional, successive subscription terms of twelve (12) months by executing a written order (each a "**Renewal Subscription Term**") at Menlo Security's then-current applicable price for the Menlo Technology. This EULA will expire or terminate upon the expiration or termination of all Subscription Terms pursuant to an Order hereunder.

5.2 SUSPENSION. Menlo Security may immediately temporarily suspend Your Use Rights if: (a)You breach 11.5 (Export); (b) we reasonably believe Your use of the Menlo Security Technology poses a security risk to the Menlo Security Technology or other users of the Menlo Security Technology; or (c)reserved. If permitted by law, Menlo Security will provide You notice before suspending Your Use Rights and Menlo Security will promptly reinstate your Use Rights once Menlo Security determines the issue causing the suspension is resolved.

5.3 TERMINATION. When the End User is an instrumentality of the U.S., recourse against the United States for any alleged breach of this Agreement must be brought as a dispute under the contract Disputes Clause (Contract Disputes Act). During any dispute under the Disputes Clause, Menlo shall proceed diligently with performance of this Agreement, pending final resolution of any request for relief, claim, appeal, or action arising under the Agreement, and comply with any decision of the Contracting Officer.

5.4 EFFECTS OF TERMINATION. Upon termination or expiration of this EULA, You must stop using and accessing the Menlo Security Technology. Additionally, You must destroy all copies of Software (to the extent applicable) and Menlo Security's Confidential Information in Your control. If this EULA is terminated,, Menlo Security will refund You or your Approved Partner any prepaid fees prorated as of the effective date of the termination.

SECTION 6. CONFIDENTIAL INFORMATION

6.1 CONFIDENTIALITY. Recipient agrees to protect Discloser's Confidential Information using no less than reasonable care and to avoid disclosure of any Confidential Information except to Authorized Recipients. Recipient must ensure that Authorized Recipients are bound to terms no less restrictive than those set forth in this EULA and Recipient is liable for any breach of this Section 6 by its Authorized Recipients.

6.2 EXCLUSIONS. Confidential Information shall not include information that: (a) is or becomes generally known to the public without breach of any obligation owed to the other party; (b) was known to a party prior to its disclosure by the other party without breach of any obligation owed to the other party; (c) was independently developed by a party without breach of any obligation owed to the other party; (d) is received from a third party without breach of any obligation owed to the other party; or (v) is Aggregated Data as defined in Section 12 (Definitions).

6.3 COMPELLED DISCLOSURE. To the extent Recipient is required by law to disclose Confidential Information, Recipient may make such disclosure, provided that Recipient (a) notifies Discloser of such requirement prior to disclosure (to the extent permitted by law) and (b) reasonably cooperates, at Discloser's expense, regarding discloser's efforts to avoid and limit disclosure. Menlo recognizes that Federal agencies are subject to the Freedom of Information Act, 5 U.S.C. 552, which may require that certain information be released, despite being characterized as "confidential" by the vendor.

6.4 RETURN AND DESTRUCTION. Upon the reasonable request of Discloser, Recipient will either return, delete or destroy all Confidential Information of Discloser and certify the same.

SECTION 7. DATA PROTECTION AND SECURITY

7.1 DATA PROTECTION AND PERSONAL DATA. Menlo Security will follow globally recognized data protection and privacy standards and laws applicable to its processing of Personal Data in connection with Your use of the Menlo Security Technology. Menlo Security will comply with the requirements and obligations set forth in Menlo Security's Data Protection Addendum ("DPA"), attached as Exhibit 1, which includes standard terms for the processing of Personal Data. For more details about how Menlo Security handles information not otherwise

covered by the DPA, please visit the Privacy Policy at https://www.menlosecurity.com/privacy-policy/ and attached hereto.

7.2 SECURITY MEASURES. Menlo Security will maintain appropriate technical and organizational safeguards and security measures as set forth in the DPA and designed to protect the security, confidentiality and integrity of Customer Data and Personal Data processed by Menlo Security on Your behalf and to protect such Customer Data and Personal Data against accidental or unlawful destruction, loss, alteration, or disclosure.

7.3 YOUR OBLIGATIONS. Your instructions to Menlo Security for the processing of Personal Data will comply with all applicable data protection and privacy laws. You have sole responsibility for the accuracy, quality, and legality of Personal Data and the means by which You acquired Personal Data. You are responsible for providing notice to, and obtaining consents from, individuals regarding the collection, processing, transfer and storage of their Personal Data through Your use of the Menlo Security Technology.

SECTION 8. INDEMNIFICATION

8.1 INDEMNIFICATION BY MENLO SECURITY. Menlo Security will have the right to intervene to defend any third party claim against You alleging that Your valid use of the Menlo Security Technology under an Order infringes or misappropriates such third party's patent, copyright or registered trademark (the "**IP Claim**"). Nothing contained herein shall be construed in derogation of the U.S. Department of Justice's right to defend any claim or action brought against the U.S., pursuant to its jurisdictional statute 28 U.S.C. §516. Menlo Security will indemnify You against any damages, reasonable attorney fees and costs finally awarded by a court of competent jurisdiction or any settlements arising from an IP Claim, provided You: (a) promptly notify Menlo Security of the IP Claim; (b) grant Menlo Security exclusive control of the defense and settlement of the IP Claim, and (c) fully cooperate with Menlo Security in defense of the IP Claim.

8.2 OTHER REMEDIES. If the Menlo Security Technology becomes, or in Menlo Security's opinion is likely to become the subject of an IP Claim, Menlo Security may, in its sole discretion and at no cost to You: (a) modify or replace the Menlo Security Technology so that it no longer infringes or misappropriates, with equivalent functionality; or (b) procure You the right to continue using the Menlo Security Technology. If neither of the foregoing alternatives are reasonably available, Menlo Security may terminate Your applicable Subscription Term Use Rights granted under this EULA upon written notice to You and will refund You or your Approved Partner any prepaid fees prorated as of the effective date of the termination.

8.3 EXCLUSIONS. Menlo Security will have no obligation under this Section 8 or otherwise with respect to any IP Claims based on: (a) combination of the Menlo Security Technology with non-Menlo Security products or software; (b) use of the Menlo Security Technology for a purpose not permitted under this EULA; (c) any modification to the Menlo Security Technology made without Menlo Security's express written approval; (d) Your failure to use the most current release of the Software; or (e) use of any Evaluation Technology.

8.4 SOLE REMEDY. THIS SECTION 8 STATES MENLO SECURITY'S ENTIRE LIABILITY AND YOUR SOLE REMEDY WITH RESPECT TO ANY IP CLAIMS.

8.5 RESERVED.

SECTION 9. REPRESENTATIONS AND WARRANTIES

9.1 SOFTWARE AND CLOUD SERVICES WARRANTY. Except for Evaluation Technology (which is provided "AS-IS"), Menlo Security warrants that: (a) the Software will perform in substantial conformance with the Documentation for a period of thirty (30) days from the date of installation or first use of the Software; and (b) it will provide the Cloud Services with commercially reasonable skill and care in accordance with the Documentation for the duration of the applicable Subscription Term.

9.2 MUTUAL WARRANTY. Each party represents and warrants that it has the legal power and authority to enter into this Agreement.

9.3 REMEDIES. Upon Your prompt written notification to Menlo Security or Your Approved Partner during the applicable warranty period, Your sole and exclusive remedy and Menlo Security's sole liability for a breach of Section 9.1 is to repair or replace the applicable Menlo Security Technology. If Menlo Security fails to re-perform, You may terminate Your Subscription Term for the affected Menlo Security Technology and Menlo Security will refund any prepaid fees prorated for the unused period of the Subscription Term, provided that

such termination must occur within three (3) months of Menlo Security's failure to repair or replace the Menlo Security Technology.

9.4 WARRANTY DISCLAIMER. Menlo Security does not warrant that the Menlo Security Technology will be uninterrupted, entirely secure or error-free. EXCEPT AS EXPRESSLY SET FORTH HEREIN, MENLO SECURITY EXPRESSLY DISCLAIMES TO THE MAXIMUM EXTENT PERMISSIBLE UNDER APPLICABLE LAW, ALL WARRANTIES, EXPRESS, IMPLIED AND STATUTORY, INCLUDING WITHOUT LIMITATION ANY IMPLIED WARRANTY OF MERCHANTABILITY, SATISFACTORY QUALITY, FITNESS FOR A PARTICULAR PURPOSE, ACCURACY, AND NONINFRINGEMENT.

Section 10. LIMITATION OF LIABILITY

10.1 LIMITATION OF LIABILITY. TO THE MAXIMUM EXTENT PERMITTED BY LAW AND EXCEPT FOR A BREACH OF YOUR PAYMENT OBLIGATIONS, UNDER NO CIRCUMSTANCES AND UNDER NO LEGAL THEORY, INCLUDING, BUT NOT LIMITED TO, TORT, CONTRACT, NEGLIGENCESTRICT LIABILITY, OR OTHERWISE, SHALL EITHER PARTY OR ITS SUPPLIERS BE LIABLE FOR: (A) ANY INDIRECT, SPECIAL, INCIDENTAL, OR CONSEQUENTIAL DAMAGES OF ANY KIND INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOST PROFITS, LOSS OF GOODWILL, OR BUSINESS INTERRUPTION; OR (B) AN AMOUNT THAT EXCEEDS THREE TIMES (3X) THE FEES PAID OR PAYABLE TO MENLO SECURITY (EITHER DIRECTLY OR THROUGH AN APPROVED SOURCE) FOR THE RELEVANT MENLO TECHNOLOGY DURING THE TWELVE (12) MONTH PERIOD IMMEDIATELY PRECEDING THE FIRST EVENT GIVING RISE TO SUCH LIABILITY. . THE FOREGOING LIMITATIONS SHALL APPLY EVEN IF EITHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. THE FOREGOING LIMITATION OF LIABILITY SHALL NOT APPLY TO (1) PERSONAL INJURY OR DEATH RESULTING FROM LICENSOR'S NEGLIGENCE; (2) FOR FRAUD; OR (3) FOR ANY OTHER MATTER FOR WHICH LIABILITY CANNOT BE EXCLUDED BY LAW.

SECTION 11. GENERAL

11.1 SURVIVAL. Sections 3 (Intellectual Property Ownership), 4 (Orders, Fees and Payment), 6 (Confidential Information), 7 (Data Protection and Privacy), 9 (Representations and Warranties), 10 (Limitation of Liability), and 11 (General) survive termination or expiration of this EULA.

11.2 ASSIGNEMENT. Neither party may assign this EULA or any of its rights or obligations hereunder, whether by operation of law or otherwise, without the prior written consent of the other party (not to be unreasonably withheld). Any other attempt to assign a party's rights or obligations under this EULA is void. Subject to the foregoing, this EULA shall bind and inure to the benefit of the parties, their respective successors and permitted assigns.

11.3 SEVERABILITY. If any provision of this EULA is held to be unenforceable, this EULA shall be construed without such provision.

11.4 US GOVERNMENT USE. If You are part of an agency, department, or other entity of the United States Government ("Government"), the use, duplication, reproduction, release, modification, disclosure or transfer of the Menlo Security Technology is restricted in accordance with the Federal Acquisition Regulations as applied to civilian agencies and the Defense Federal Acquisition Regulation Supplement as applied to military agencies. The Menlo Security Technology is "commercial item," "commercial computer software" and "commercial computer software documentation." In accordance with such provisions, any use of the Menlo Security Technology by the Government shall be governed solely by the terms of this Agreement.

11.5 EXPORT CONTROLS. You will comply with all export laws and restrictions and regulations of the Department of Commerce, the United States Department of Treasury Office of Foreign Assets Control ("OFAC"), or other United States or foreign agency or authority, and You will not export, or allow the export or re-export of the Menlo Security Technology or any related technical information in violation of any such restrictions, laws or regulations. By installing or using the Menlo Security Technology, You agree to the foregoing and represent and warrant that You are not located in, under the control of, or a national or resident of any restricted country.

11.6 COMPLIANCE WITH LAWS. Each party will comply with all laws and regulations applicable to its obligations under this EULA.

11.7 EULA MODIFICATION. The non-material terms and conditions of this EULA may be updated by Menlo Security and the current version will be posted at https://www.menlosecurity.com/eula. Any changes to the EULA apply to Orders placed or renewed after the date of modification.

11.8 ENTIRE AGREEMENT, ADDITIONAL TERMS, AMENDMENT. This EULA represents the complete agreement concerning the Menlo Security Technology between the parties and prevails over any additional or inconsistent terms in: (a) a purchase order (or similar document) provided by You or Your Approved Partner; or (b) an agreement with Your Approved Partner. This EULA supersedes all prior agreements and representations, written or oral, provided however, that if there is already a mutually signed agreement directly between Menlo Security and You (not including a purchase order or similar document) covering Your license and/or use of the Menlo Security technology, then the terms of that agreement will govern. This EULA may be amended only by a written document executed by a duly authorized representative of each of the parties.

11.9 FORCE MAJEUR. Excusable delays shall be governed by FAR 552.212-4(f).

11.10 GOVERNING LAW. This Agreement shall be governed by and construed under the Federal laws of the United States, the United Nations Convention on the International Sale of Goods, or the Uniform Computer Information Transactions Act.

SECTION 12. DEFINITIONS

"Affiliate" means any entity which directly or indirectly controls, is controlled by, or is under common control by either party. For purposes of the preceding sentence, "control" means direct or indirect ownership or control of fifty-one percent (51%) of the voting interests of the subject entity.

"Aggregated Data" means the aggregated and statistical data derived from Your use and the operation of the Menlo Technology, including, without limitation, the number of records in the Menlo Technology, the number and types of transactions, configurations, and reports processed in the Menlo Technology and the performance results for the Menlo Technology.

"Approved Partner" means a third party resale partner authorized by Menlo Security to resell the Menlo Technology.

"Authorized Recipients" means each party's employees, affiliates, and contractors who have a need to know Confidential Information.

"Authorized User(s)" means an individual or entity that is authorized by You to use the Menlo Technology, or to whom You (or Menlo Security at Your request) have supplied a user identification and password.

"Cloud Services" means Menlo Technology's hosted enterprise software-as-a-service offering and may also include Software.

"Confidential Information" means all proprietary information obtained by a party (the "**Recipient**") from the other party (the
"**Discloser**") in connection with this EULA, orally or in writing, designated as confidential, or that reasonably should be understood to be confidential given the nature of the information and circumstance of disclosure.

"Customer Data" means all data or information generated by Your use of the Menlo Security Technology or submitted to the Menlo Technology by or on Your behalf. Customer Data does not include Aggregated Data.

"Documentation" means the published technical specifications and usage materials, whether in print or electronic form, or on-line help functions for the Menlo Technology, specifying the features and functionality of the Menlo Security Technology, as updated from time to time.

“Evaluation Technology” means Menlo Security Technology provided for trial, evaluation or beta purposes.

"Evaluation Term" means the use of Evaluation Technology for thirty (30) days, unless otherwise set forth on an Order.

“Fee” means the fee Menlo Security or an Approved Partner charges You for the Menlo Security Technology, as detailed in an Order.

“Initial Subscription Term” means the initial subscription term, as defined in Section 5.1.

“IP Claim” means any third party claim against You alleging that Your valid use of the Menlo Security Technology under an Order infringes or misappropriates such third party’s patent, copyright or registered trademark.

“Menlo Security” means Menlo Security, Inc. and its subsidiaries and Affiliates.

“Menlo Security Content” means any (a) data or content provided by Menlo Security to You and (b) Aggregated Data.

“Menlo Security Technology” means the Software and/or Cloud Services purchased by You and as set forth on an applicable Order.

“Order” means any ordering document that sets forth certain details of the order between Menlo Security and You or an Approved Partner and You.

“Personal Data” means (a) any personally identifiable information that is capable of identifying a natural person, and (b) information, the disclosure, use or confidentiality of which is regulated by a Privacy Law.

“Privacy Law” means any U.S. local, state and federal and non-U.S. information security, data breach or privacy law or regulation that regulate the privacy or security of Personal Data and that are directly applicable to Menlo Security.

“Records” means complete and accurate records of Your use of the Menlo Technology to verify compliance with this EULA.

“Renewal Subscription Term” means the renewal subscription term as defined in Section 5.1.

“Software” means Menlo Technology’s virtual and on-premise enterprise software product, including upgrades and updates.

“Subscription Term” means the Initial Subscription Term and all Renewal Subscription Terms (as defined in Section 5.1) together.

“Start Date” means the date set forth in an Order, or where no date is agreed: (a) for Software, the earlier of the date Software is made available for download or installation, and (b) for Cloud Services, the date on which the Cloud Service is made available for Your use.

"Third Party Agent(s)" means Your Authorized Users, Your Affiliates, Your third-party service providers, and each of their respective Authorized Users permitted to access and use the Menlo Technology on Your behalf.

“Third Party Claim” means any third party claim against Menlo Security arising from Your breach of Section 2.1 of this EULA.

“Use Rights” means Your rights set forth in Section 1.1.

"You" or "Your" means the government customer purchasing and using the Menlo Technology, as set forth in the "Company" signature block below or identified in the Order as applicable.

Each party, as evidenced by the signature below by its authorized representative, acknowledges that it has read and agrees to this EULA in its entirety.

Company:	**Menlo Security, Inc.**
By:_____	By:_____
Name:_____	Name:_____
Title:_____	Title:_____
Date:_____	Date:_____

EXHIBIT 1
Menlo Security

Data Protection Addendum for Customers

This Data Protection Addendum ("**DPA**") is expressly incorporated by reference into the End User License Agreement or other master agreement ("**Agreement**") entered by and between the party identified in the Agreement ("**You**" or "**Customer**") and Menlo Security, Inc. (together with its subsidiaries and Affiliates, "**Menlo Security**" or "**Menlo"**), each a "**Party**" and collectively the "**Parties**," and applies where, and to the extent that Menlo Security Processes Personal Data for Customer when providing Services (as defined below) under the Agreement and is effective as of the date of Your signature below.. The Parties agree as follows:

1. **Definitions**. For purposes of this DPA:

   a. "**Affiliate**" means any entity which directly or indirectly controls, is controlled by, or is under common control by a Party. For purposes of the preceding sentence, "control" means direct or indirect ownership or control of fifty-one percent (51%) of the voting interests of the subject entity.

   b. "**Controller**" means an entity that determines the purposes and means of the processing of Personal Data.

   c. "**Data Privacy Laws**" means all applicable laws, regulations, and other legal or self-regulatory requirements in any jurisdiction relating to privacy, data protection, data security, breach notification, or the Processing of Personal Data, including without limitation, to the extent applicable, the California Consumer Privacy Act, Cal. Civ. Code § 1798.100 *et seq.* ("**CCPA**"), the General Data Protection Regulation, Regulation (EU) 2016/679 ("**GDPR**"), the United Kingdom Data Protection Act of 2018 ("**UK Privacy Act**"), and the Swiss Federal Act on Data Protection ("**FADP**"). For the avoidance of doubt, if Menlo Security's Processing activities involving Personal Data are not within the scope of a given Data Privacy Law, such law is not applicable for purposes of this DPA.

   d. "**Data Subject**" means an identified or identifiable natural person about whom Personal Data relates.

   e. "**EU SCCs**" means the Standard Contractual Clauses issued pursuant to Commission Implementing Decision (EU) 2021/914 of 4 June 2021 *on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council*, located http://data.europa.eu/eli/dec_impl/2021/914/oj., and completed as set forth in Section 7 below.

   f. "**Personal Data**" includes "personal data," "personal information," "personally identifiable information," and similar terms, and such terms shall have the same meaning as defined by applicable Data Privacy Laws, that is Processed in relation to the Agreement.

   g. "**Process**" and "**Processing**" mean any operation or set of operations performed on Personal Data or on sets of Personal Data, whether or not by automated means, such as collection, recording, organization, creating, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure, or destruction.

   h. **"Processor"** means an entity that processes Personal Data on behalf of a Controller.

   i. "**Representative(s)**" means either Party including its Affiliates, officers, directors, employees, agents, contractors, temporary personnel, subcontractors and consultants.

j. "**Security Breach**" means any accidental or unlawful acquisition, destruction, loss, alteration, unauthorized disclosure of, or access to, Personal Data.

k. "**Services**" means the Menlo Security services purchased by Customer under the Agreement.

2. **Scope and Purposes of Processing**.

a. Menlo Security will Process Personal Data solely: (1) according to Customer's documented instructions; (2) to fulfill its obligations to Customer under the Agreement, including this DPA; (2) on Customer's behalf; and (3) in compliance with Data Privacy Laws. Menlo Security will not sell Personal Data or otherwise Process Personal Data for any purpose other than for the specific purposes set forth herein. For purposes of this paragraph, "sell" shall have the meaning set forth in the CCPA.

b. Menlo Security will not attempt to link, identify, or otherwise create a relationship between Personal Data and non-Personal Data or any other data without Customer's express authorization.

c. In jurisdictions that distinguish between Controllers and Processors, Menlo Security is the Controller for Personal Data processed to administer and manage the customer relationship. Menlo Security is the Processor for the Personal Data processed by the Services in order to provide its functionality.

3. **Personal Data Processing Requirements**. Menlo Security will:

a. Ensure that the persons it authorizes to Process the Personal Data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

b. Upon Customer's written request, assist Customer in the fulfilment of Customer's obligations to respond to verifiable requests by Data Subjects (or their lawful representatives) for exercising their rights under Data Privacy Laws (such as rights to access or delete Personal Data), at Customer's reasonable expense.

c. Promptly notify Customer of (i) any third-party or Data Subject complaints regarding the Processing of Personal Data; or (ii) any government or Data Subject requests for access to or information about Menlo Security's Processing of Personal Data on Customer's behalf, unless prohibited by Data Privacy Laws. Menlo Security will provide Customer with reasonable cooperation and assistance in relation to any such request. If Menlo Security is prohibited by applicable Data Privacy Laws from disclosing the details of a government request to Customer, Menlo Security shall inform Customer that it can no longer comply with Customer's instructions under this DPA, without providing more details, and await Customer's further instructions. Menlo Security shall use all available legal mechanisms to challenge any demands for data access through national security process that it receives, as well as any non-disclosure provisions attached thereto.

d. Provide reasonable assistance to and cooperation with Customer for Customer's performance of a data protection impact assessment of Processing or proposed Processing of Personal Data, when required by applicable Data Privacy Laws, and at Customer's reasonable expense.

e. Provide reasonable assistance to and cooperation with Customer for Customer's consultation with regulatory authorities in relation to the Processing or proposed Processing of Personal Data, including complying with any obligation applicable to Menlo Security under Data Privacy Laws to consult with a regulatory authority in relation to Menlo Security's Processing or proposed Processing of Personal Data.

4. **Data Security**. Menlo Security will implement appropriate administrative, technical, physical, and organizational measures to protect Personal Data, as set forth in Exhibit B.

5. **Security Breach**. Menlo Security will notify Customer promptly of any known Security Breach and will assist Customer in Customer's compliance with Customer's Security Breach-related obligations, including without limitation, by:

   a. Taking steps to mitigate the effects of the Security Breach and reduce the risk to Data Subjects whose Personal Data was involved; and

   b. Providing Customer with the following information, to the extent known:

      i. The nature of the Security Breach, including, where possible, how the Security Breach occurred, the categories and approximate number of Data Subjects concerned, and the categories and approximate number of Personal Data records concerned;

      ii. The likely consequences of the Security Breach; and

      iii. Measures taken or proposed to be taken by Menlo Security to address the Security Breach, including, where appropriate, measures to mitigate its possible adverse effects.

6. **Subprocessors**.

   a. Customer acknowledges and agrees that Menlo Security may use Affiliates and other subprocessors to Process Personal Data in accordance with the provisions within this DPA and Data Privacy Laws. Where Menlo Security sub-contracts any of its rights or obligations concerning Personal Data, including to any Affiliate, Menlo Security will take steps to select and retain subprocessors that are capable of maintaining appropriate privacy and security measures to protect Personal Data consistent with applicable Data Privacy Laws.

   b. Menlo Security's current subprocessors are set forth in Exhibit C (the "**Subprocessor List**"). Customer hereby consents to Menlo Security's use of such subprocessors. Menlo Security will maintain an up-to-date list of its subprocessors, and it will provide Customer with notice (which may be provided through email to Customer's administrator's email address that was communicated to Menlo Security, or such other reasonable means) of any new subprocessor added to the list. In the event Customer objects to a new subprocessor due to a reasonable belief that the subprocessor cannot provide the level of protection required under this DPA, Menlo Security will use reasonable efforts to make available to Customer a change in the services or recommend a commercially reasonable change to, Customer's use of the services to avoid Processing of Personal Data by the objected-to subprocessor without unreasonably burdening Customer. In the event that Customer objects to a subprocessor as set forth above and Menlo Security is unable to change the services to Customer's reasonable satisfaction, Customer may, in Customer's sole discretion, terminate the applicable part of the Agreement with respect only to those Services which cannot be provided by Menlo Security without the use of the objected to subprocessor by giving written notice to Menlo Security.

7. **Data Transfers and Additional Safeguards**.

   a. Menlo Security will not engage in any cross-border Processing of Personal Data, or transmit, directly or indirectly, any Personal Data to any country outside of the country from which such Personal Data was collected, without complying with applicable Data Privacy Laws. Where Menlo Security engages in an onward transfer of Personal Data, Menlo Security shall ensure that a lawful data transfer mechanism is in place prior to transferring Personal Data from one country to another.

   b. To the extent legally required, by signing this DPA, Customer and Menlo Security are deemed to have signed the EU SCCs, which form part of this DPA and (except as described in Section 7(c) and (d) below) will be deemed completed as follows:

i. Module 2 of the EU SCCs applies to transfers of Personal Data from Customer (as a controller) to Menlo Security (as a processor) and Module 3 of the EU SCCs applies to transfers of Personal Data from Customer (as a processor) to Menlo Security (as a sub-processor);

ii. Clause 7 of Modules 2 and 3 (the optional docking clause) is not included;

iii. Under Clause 9 of Modules 2 and 3 (Use of sub-processors), the Parties select Option 2 (General written authorization). The initial list of sub-processors is set forth in Exhibit C of this DPA and Menlo Security shall propose an update to that list at least 7 days in advance of any intended additions or replacements of sub-processors in accordance with Section 6(b) of this DPA;

iv. Under Clause 11 of Modules 2 and 3 (Redress), the optional language requiring that data subjects be permitted to lodge a complaint with an independent dispute resolution body shall not be deemed to be included;

v. Under Clause 17 of Modules 2 and 3 (Governing law), the Parties choose Option 1 (the law of an EU Member State that allows for third-Party beneficiary rights). The Parties select the law of Ireland;

vi. Under Clause 18 of Modules 2 and 3 (Choice of forum and jurisdiction), the Parties select the courts of Ireland;

vii. Annex I(A) and I(B) of Modules 2 and 3 (List of Parties) is completed as set forth in Exhibit A of this DPA;

viii. Under Annex I(C) of Modules 2 and 3 (Competent supervisory authority), the Parties shall follow the rules for identifying such authority under Clause 13 and, to the extent legally permissible, select the Irish Data Protection Commission.

ix. Annex II of Modules 2 and 3 (Technical and organizational measures) is completed with Exhibit B of this DPA; and

x. Annex III of Modules 2 and 3 (List of subprocessors) is not applicable as the Parties have chosen General Authorization under Clause 9.

c. With respect to Personal Data transferred from the United Kingdom for which United Kingdom law (and not the law in any European Economic Area jurisdiction) governs the international nature of the transfer, the International Data Transfer Addendum to the EU Commission Standard Contractual Clauses (available as of the effective date at https://ico.org.uk/media/for-organisations/documents/4019539/international-data-transfer-addendum.pdf) ("UK SCCs") forms part of this Addendum and takes precedence over the rest of this Addendum as set forth in the UK SCCs, unless the United Kingdom issues updates to the UK SCCs that, upon notice from Customer, will control. Undefined capitalized terms used in this provision shall mean the definitions in the UK SCCs. For purposes of the UK SCCs, they shall be deemed completed as follows:

i. Table 1 of the UK SCCs:

1. The Parties' details shall be the Parties and their affiliates to the extent any of them is involved in such transfer.

2. The Key Contact shall be the contacts set forth in the Agreement.

ii. Table 2 of the UK SCCs: The Approved EU SCCs referenced in Table 2 shall be the EU SCCs as

executed by the Parties.

iii. Table 3 of the UK SCCs: Annex 1A, 1B, II, and III shall be set forth in Exhibits A, B, and C below.

iv. Table 4 of the UK SCCs: Either Party may end this Addendum as set out in Section 19 of the UK SCCs.

v. By entering into this DPA, the Parties are deemed to be signing the UK SCCs, the Mandatory Clauses in Part 2, and its applicable Tables and Appendix Information.

d. For transfers of Personal Data that are subject to the FADP, the EU SCCs form part of this DPA as set forth in Section 7(b) of this DPA, but with the following differences to the extent required by the FADP: (1) references to the GDPR in the EU SCCs are to be understood as references to the FADP insofar as the data transfers are subject exclusively to the FADP and not to the GDPR; (2) references to personal data in the EU SCCs also refer to data about identifiable legal entities until the entry into force of revisions to the FADP that eliminate this broader scope; and (3) the relevant supervisory authority with respect to transfers from Switzerland is the Swiss Federal Data Protection and Information Commissioner.

e. Supplementary Measures. In addition to the obligations under Sections 7(a)-(d), if and to the extent that the Parties will engage in cross-border Processing of Personal Data or will transmit, directly or indirectly, any Personal Data to a country outside of the country from which such Personal Data was collected (including without limitation transfers of Personal Data outside of the EEA, Switzerland or the UK), the Parties agree to the following supplementary measures:

i. All Personal Data shall be encrypted both in transit and at rest using state of the art encryption technology that is robust against the performance of cryptanalysis;

ii. Menlo Security warrants and represents that, as of the date of the Agreement, it has not received any national security data production orders (e.g., pursuant to Section 702 of the Foreign Intelligence Surveillance Act ("FISA Section 702") or U.S. Presidential Policy Directive 28);

iii. Menlo Security will use all reasonable legal mechanisms to challenge any demands for data access through the national security process that Menlo Security receives; and

iv. Menlo Security will provide, up to once per calendar year upon Customer's request, a transparency report indicating the types of binding legal demands for the Personal Data it has received, including national security orders and directives.

8. **Audits**. Menlo Security will make available to Customer all reasonable information necessary to demonstrate compliance with this DPA and will allow for and contribute to audits, including inspections, conducted by Customer or another auditor mandated by Customer, provided that, such audit shall occur not more than once every twelve (12) calendar months, upon reasonable prior written notice, and to the extent Menlo Security's personnel are required to cooperate therewith, during Menlo Security's normal business hours.

9. **Return or Destruction of Personal Data**. Except to the extent required otherwise by Data Privacy Laws, Menlo Security will, at Customer's choice and upon Customer's written request, return to Customer and/or securely destroy all Personal Data upon such request or at termination of the Agreement. Except to the extent prohibited by Data Privacy Laws, Menlo Security will inform Customer if it is not able to return or delete the Personal Data.

10. **Survival**. The provisions of this DPA survive the termination or expiration of the Agreement for so long as Menlo Security or its subprocessors Process the *Personal Data*.

Customer:	**Menlo Security, Inc.**
By:_____	By:_____
Name:_____	Name:_____
Title:_____	Title:_____
Date:_____	Date:_____

Exhibit A

ANNEX I

A. LIST OF PARTIES

MODULE TWO: Transfer controller to processor

MODULE THREE: Transfer processor to processor

Data exporter(s):

Name: The data exporter is Customer.

Activities relevant to the data transferred under these SCCs: The data exporter is a user of the data importer's Services pursuant to their underlying Agreement. The data exporter acts as a controller with respect to its own personal data. To the extent permitted by the Agreement, the exporter also is permitted to use the contracted Services as a processor on behalf of third parties.

Signature and date: _____

Role: controller

Data importer(s):

Name: Menlo Security

Activities relevant to the data transferred under these SCCs: The data importer is the provider of Services to the data exporter and its customers pursuant to their underlying Agreement. The data importer acts as the data exporter's processor.

Signature and date: _____

Role: processor

B. DESCRIPTION OF TRANSFER

MODULE TWO: Transfer controller to processor

MODULE THREE: Transfer processor to processor

Categories of data subjects whose personal data is transferred:

The personal data transferred concerns employees, contractors, business partners, representatives and end customers of the data importer and other individuals residing in the European Economic Area, the United Kingdom and Switzerland, whose personal data is processed by or on behalf of the Customer or Customer's customers and delivered as part of the Services.

Categories of personal data transferred:

The personal data transferred concern the following categories of data (please specify):

Customer's personal data related directly or indirectly to the categories of data subjects listed above, including online and offline support, prospect, and partner data, and Personal Data provided by or on behalf of the Customer or its users of the Services. Such transfer of personal data is determined and controlled by the data exporter in its sole discretion, and may include, and is not limited to the following categories of personal data.

- Any personal data that may be contained in Customer's logs (e.g. user name, user id, IP address, time stamps, websites visited)
- Customer's active directory data
- Any personal data that may be contained in physical binary submitted for analysis
- Any personal data that may be contained in a file submitted for analysis
- Personal data contained in customer logs
- Personal data contained in policy settings
- Company, position
- Login credentials
- Log and usage data
- Device information (device name, device serial number, device type, device owner name, device owner email, timestamp for login)
- IP address
- First and last name, email address, and phone number of Customer's employee(s) appointed to open a support service request
- Browser information, IP address, and other web browsing related protocol information contained in a fille attached to a support ticket
- Personal data contained in a support ticket (Customer controls what it submits)

More detailed categories of personal data are reflected in Menlo Security's Privacy Data Sheet, made available to Customer upon request.

Sensitive data transferred (if applicable) and applied restrictions or safeguards that fully take into consideration the nature of the data and the risks involved, such as for instance strict purpose limitation, access restrictions (including access only for staff having followed specialised training), keeping a record of access to the data, restrictions for onward transfers or additional security measures:

Unless data exporter or its users use data importer's services to transmit or store sensitive data, data importer does not process sensitive data.

The frequency of the transfer (e.g. whether the data is transferred on a one-off or continuous basis):

Continuous.

Nature of the processing:

Data exporter's Processing activities shall be limited to those discussed in the Agreement and this DPA.

Purpose(s) of the data transfer and further processing:

The objective of the transfer and further processing of personal data by Menlo Security is the access and use of Menlo Security's Services.

The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period:

Personal data will be retained for the period of time necessary to provide the Services to Customer under the Agreement, this DPA, and/or in accordance with applicable legal requirements.

For transfers to (sub-) processors, also specify subject matter, nature and duration of the processing:

Same as above to the extent such information is provided to subprocessors for purposes of providing the Services.

C. COMPETENT SUPERVISORY AUTHORITY

MODULE TWO: Transfer controller to processor

MODULE THREE: Transfer processor to processor

See Section 7(b)(viii) of this DPA.

ANNEX II - TECHNICAL AND ORGANISATIONAL MEASURES INCLUDING

TECHNICAL AND ORGANISATIONAL MEASURES TO ENSURE THE SECURITY OF

THE DATA

MODULE TWO: Transfer controller to processor

MODULE THREE: Transfer processor to processor

EXPLANATORY NOTE:

The technical and organisational measures must be described in specific (and not generic) terms. See also the general comment on the first page of the Appendix, in particular on the need to clearly indicate which measures apply to each transfer/set of transfers.

Description of the technical and organisational measures implemented by the data importer(s) (including any relevant certifications) to ensure an appropriate level of security, taking into account the nature, scope, context and purpose of the processing, and the risks for the rights and freedoms of natural persons.

Annex 2 to Attachment B, the EU SCCs, is the data security measures located in Exhibit B.

For transfers to (sub-) processors, also describe the specific technical and organisational measures to be taken by the (sub-) processor to be able to provide assistance to the controller and, for transfers from a processor to a sub-processor, to the data exporter:

Data importer shall require its subprocessors to take appropriate technical and organizational measures to provide assistance to the controller and/or data exporter that are no less restrictive than those in Exhibit B.

Exhibit B

MENLO SECURITY DATA SECURITY MEASURES

Menlo Security will implement and maintain the following administrative, technical, physical, and organizational security measures for the Processing of Personal Data:

Menlo Security's Information Security Program includes specific security requirements for its personnel and all subprocessors or agents who have access to Personal Data ("Data Personnel"). Menlo Security's security requirements covers the following areas:

1. Information Security Policies and Standards. Menlo Security will maintain written information security policies, standards and procedures addressing administrative, technical, and physical security controls and procedures. These policies, standards, and procedures shall be kept up to date, and revised whenever relevant changes are made to the information systems that use or store Personal Data.

2. Physical Security. Menlo Security will maintain commercially reasonable security systems at all Menlo Security sites at which an information system that uses or stores Personal Data is located ("Processing Locations") that include reasonably restricting access to such Processing Locations, and implementing measures to detect, prevent, and respond to intrusions.

3. Organizational Security. Menlo Security will maintain information security policies and procedures addressing acceptable data use standards, data classification, and incident response protocols.

4. Network Security. Menlo Security maintains commercially reasonable information security policies and procedures addressing network security.

5. Access Control. Menlo Security agrees that: (1) only authorized Menlo Security staff can grant, modify or revoke access to an information system that Processes Personal Data; and (2) Menlo Security will implement commercially reasonable physical and technical safeguards to create and protect passwords.

6. Virus and Malware Controls. Menlo Security protects Personal Data from malicious code and will install and maintain anti-virus and malware protection software on any system that handles Personal Data.

7. Personnel. Menlo Security has implemented and maintains a security awareness program to train employees about their security obligations. Data Personnel follow established security policies and procedures. Disciplinary process is applied if Data Personnel fail to adhere to relevant policies and procedures.

8. Business Continuity. Menlo Security implements disaster recovery and business resumption plans that are kept up to date and revised on a regular basis. Menlo Security also adjusts its Information Security Program in light of new laws and circumstances, including as Menlo Security's business and Processing change.

Exhibit C

MENLO SECURITY SUBPROCESSORS

Sub-processor	Personal Data	Location of Data Center	Security Assurances
AWS	Customer Logs, Policy Settings, Business and Product Analytics	USA, Canada, Frankfurt, Ireland, London, Paris, Hong Kong, Tokyo, São Paulo, Seoul, Singapore, Sydney, Mumbai, Bahrain	ISO 27001, 27017, 27018, SOC2 Type II, FedRAMP authorized (us-east/west), PCI DSS Level 1, FinTech, FISC, ISMAP, NISC, OSPAR, MTCS Tier3 (and more)
Sophos	Sandbox Analysis, File Inspection	US, Germany (EU), UK (Brexit), Japan	InfoSec and Privacy Policies
Salesforce	Account and Registration Information	USA	FedRAMP High/Moderate, GDPR, HIPAA, HITRUST, ISMAP, ISO 27001, 27017, 27018, PCI NSS, SOC2 Type II (and more)
Zendesk	Support Ticket Information	USA	SOC2 Type II, ISO 27001, 27018, FedRAMP LI-SaaS, HIPAA, PCI DSS, Posted policies
Slack	Support Ticket Information	USA	ISO/IEC 27001, ISO/IEC 27017, ISO/IEC 27018, ISO/IEC 27701, SOC2 Type II, SOC3, APEC for Processors Certification, APEC for Controllers Certification, CSA
Keatext	Support Information, Administrator Contact Information	USA	InfoSec and Privacy Policies
Splunk	Customer Logs, Business and Product Analytics	USA	FedRAMP Moderate, ISO 27001
Marketo	Administrator Contact Information	USA	ISO/IEC 27001
Gainsight	Administrator Contact Information	USA	SOC2 Type II