DATA PROCESSING AGREEMENT FOR
JAMF EXECUTIVE THREAT PROTECTION CUSTOMERS

This Data Processing Agreement for Jamf Executive Threat Protection Customers (the "**DPA**"), effective as of the date of the last signature below (the "**Effective Date**"), is made by and between JAMF Software, LLC, a Minnesota limited liability company, having a principal place of business at 100 Washington Ave. S., Suite 1100, Minneapolis, MN 55401-2155 USA, and its Affiliates ("**Jamf**") and the organization identified below ("**Customer**"), each a "**Party**" and collectively the "**Parties**."

1. **Subject Matter of this DPA**. This DPA supplements the Jamf Executive Threat Protection Terms of Service or other negotiated agreement (as applicable) between the Parties pursuant to which Jamf provides Jamf Executive Threat Protection Services to Customer, along with any subsequent amendments or orders (the "**Agreement**"). It is applicable when Data Protection Laws apply to Customer's use of the Services to Process Personal Data. In consideration of the mutual obligations in this DPA, the Parties agree that the terms of this DPA will form part of the Agreement, which will remain in full force and effect except as modified below. If there is a conflict between the Agreement and this DPA regarding the processing of Personal Data, the DPA will govern. Capitalized terms used but not defined in the DPA have the meanings given in the Agreement.

2. **Definitions.**

   a) "**Data Protection Laws**" means all applicable data protection, privacy, and cyber security laws, rules, and regulations of any country, including (where applicable and without limitation) the GDPR, the UK GDPR, the Swiss Data Protection Act, data protection laws of the European Union ("**EU**"), European Economic Area ("**EEA**") member states, or the United Kingdom ("**UK**") that supplement the GDPR or UK GDPR (respectively), and the California Consumer Privacy Act of 2018, as amended by the California Privacy Rights Act of 2020 (collectively referred to as the **"CPRA"**), in each case as may be amended or superseded from time to time.

   b) "**Data Subject**" means the individual to whom the Personal Data relates, which is Processed for the performance of the Agreement by Jamf.

   c) "**GDPR**" means the EU General Data Protection Regulation 2016/679.

   d) "**ex-EEA Transfer**" means a Processing activity whereby Personal Data which is Processed in accordance with the GDPR is transferred from the Customer to Jamf outside the EEA, and such transfer is not governed by an adequacy decision made by the European Commission in accordance with the relevant provisions of the GDPR.

   e) "**ex-Swiss Transfer**" means a Processing activity whereby Personal Data which is Processed in accordance with Swiss Data Protection Laws is transferred from the Customer to Jamf outside Switzerland, and such transfer is not governed by an adequacy decision made by the Federal Data Protection and Information Commissioner of Switzerland ("**FDPIC**") in accordance with the relevant provisions of the Swiss Data Protection Act.

   f) "**ex-UK Transfer**" means a Processing activity whereby Personal Data which is Processed in accordance with the UK Data Protection Laws is transferred from the Customer to Jamf outside the UK, and such transfer is not governed by an adequacy decision pursuant to Section 17A of the UK Data Protection Act 2018**.**

   g) "**Government Agency Requests**" means formal legal requests from any government intelligence or security service/agencies in the country to which the relevant Personal Data is being exported, for access to (or for copies of) Personal Data that has been transferred to Jamf pursuant to the Agreement.

   h) "**Personal Data**" means any personal data (as defined in applicable Data Protection Laws) Processed by Jamf (or any Sub-processor) as part of Jamf's performance of the Agreement or provision of the Services to Customer.

   i) **"Personal Data Breach"** means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Personal Data, transmitted, stored, or otherwise Processed.

   j) "**Processing**" or "**Process**" means any operation or set of operations that is performed upon Personal Data or on sets of Personal Data, whether by automatic means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, blocking, erasure, or destruction.

   k) "**Restricted Transfer**" means (i) where the GDPR applies, an ex-EEA Transfer, (ii) where the UK GDPR applies, an ex-UK Transfer, and (iii) where the Swiss Data Protection Act applies, an ex-Swiss Transfer.

l) "**Services**" means Jamf Executive Threat Protection software-as-a-service solutions and professional services and/or solutions for cyber security, IT Ops and/or DevOps as specified in the Order and as further described in the Documentation (including any Updates and Upgrades to the applicable Service provided by Jamf, and any software, systems and locally-installed software agents, collectors, scripts, software, and connectors that interact with the Services as may be provided by Jamf in connection with the Services).

m) **"Standard Contractual Clauses**" means (i) where the GDPR applies, the standard contractual clauses approved by the European Commission and annexed to the European Commission's Implementing Decision 2021/914 dated 4 June 2021 on standard contractual clauses for transfers of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council ("**EEA Standard Contractual Clauses**"), (ii) where the UK GDPR applies, the "International Data Transfer Addendum to the EU Commission Standard Contractual Clauses" issued by the Information Commissioner under s.119A(1) of the UK Data Protection Act 2018 ("**UK Addendum**"), and (iii) where the Swiss Data Protection Act applies, the applicable standard contractual clauses issued, approved or recognized by the Swiss Federal Data Protection and Information Commissioner ("**Swiss Standard Contractual Clauses**"), in each case as may be amended or updated from time to time.

n) "**Sub-processor**" means any third party appointed by or on behalf of Jamf that Processes Personal Data.

o) "**Swiss Data Protection Act**" means the Swiss Federal Data Protection Act of June 1992, or the Revised Federal Data Protection Act when it comes into force (as applicable).

p) "**UK GDPR**" means the GDPR as transposed into United Kingdom national law by operation of Section 3 of the European Union (Withdrawal) Act 2018. Where the UK GDPR applies to the Processing of Personal Data under this DPA, references in this DPA to the GDPR and to provisions of the GDPR will be construed as references to the UK GDPR and to the corresponding provisions of the UK GDPR, and references to EU or Member State law will be construed as references to UK law.

3. **CPRA Processing of Personal Data**. In connection with Jamf's provision of Services to Customer, if the CPRA applies and Jamf receives any Personal Data from or on behalf of Customer, then:

a) Jamf will not retain, use, or disclose such Personal Data (i) for any purpose other than to perform the Services specified in the Agreement, or (ii) outside of the direct business relationship between Customer and Jamf;

b) Jamf will not sell, rent, release, disclose, disseminate, make available, transfer, or otherwise communicate such Personal Data to any third party for monetary or other valuable consideration, or share such Personal Data to any third party for cross-context behavioural advertising, whether or not for monetary or other valuable consideration;

c) Jamf may disclose Personal Data to Jamf's service providers in connection with such service providers providing services to Jamf and Jamf may permit such service providers to Process Personal Data as necessary for Jamf to provide the Services to Customer provided that Jamf notifies Customer of its engagement of such service providers and obligates any such service providers to provide the same level of protection as is required of Jamf under CPRA. Section 5 of this DPA sets forth Jamf's compliance with Civil Code § 1798.140 (ag) (2);

d) Jamf may combine Customer's Personal Data with Personal Data received from other entities to the extent necessary to detect security incidents or to protect against fraudulent or illegal activity and as otherwise permitted, when Jamf acts as a "service provider" as defined in California Civil Code § 1798.140(ag) (1) with regard to all such Personal Data;

e) As defined by CPRA, deidentified means information that cannot reasonably be used to infer information about, or otherwise be linked to, a particular consumer, provided that the possessor of the information complies with the requirements set forth in California Civil Code § 1798.140 (m). If Customer makes deidentified information available to Jamf in connection with the Agreement, Jamf will (i) take reasonable measures to ensure that the information cannot be associated with a consumer or household, (ii) publicly commit to maintain and use the information in deidentified form and not to attempt to re-identify the information except as allowed under the CPRA, and (iii) contractually obligate any recipients of the information to comply with all provisions of California Civil Code § 1798.140 (m);

f) In accordance with Section 8 below, Jamf confirms that it has implemented reasonable security procedures and practices to protect Personal Data from unauthorized or illegal access, destruction, modification, or disclosure;

g) As provided for in Section 9 below, Jamf grants Customer the right to take reasonable and appropriate steps to stop and remediate the unauthorized use of Personal Data, and pursuant to Sections 10 and 11 below, Jamf grants the Customer the right to take reasonable and appropriate steps to help ensure that Jamf uses Personal Data transferred to Jamf in a manner consistent with Customer's obligations under CPRA;

h) Jamf will notify Customer if Jamf determines that it can no longer meet its obligations under CPRA and grants Customer the right to take reasonable and appropriate steps to stop providing Personal Data to Jamf.

4. **Processing of Personal Data.**

a) Jamf's Relationship with Customer. Customer will be the controller of Personal Data and Jamf will be a processor.

b) Jamf's Processing of Personal Data. Jamf will Process Personal Data in accordance with the requirements of Data Protection Laws and only upon Customer's documented instructions and as set forth in the Agreement, except where Processing is otherwise permitted by Data Protection Laws. Details of the Processing, including the types of Personal Data and categories of Data Subjects, are further described in Schedule 1. Jamf will inform Customer if it becomes aware that Customer's Processing instructions infringe applicable Data Protection Laws, but without obligation to actively monitor Customer's compliance with applicable Data Protection Laws. In addition to assistance otherwise addressed in this DPA, Jamf will provide reasonable and timely assistance (at Customer's expense) to enable Customer to respond to any correspondence, inquiry, or complaint received from a Data Subject, regulator, or other third party in connection with the Processing of Personal Data provided that Jamf is not legally prohibited from doing so. If any such request, correspondence, inquiry, or complaint is made directly to Jamf, unless legally prohibited from doing so, Jamf will promptly inform Customer and provide the related details.

c) Transfers of EEA Personal Data. The Parties agree that when the transfer of Personal Data from Customer (as data exporter) to Jamf (as data importer) is an ex-EEA Transfer, such transfers will be subject to the EEA Standard Contractual Clauses (official text found here: https://commission.europa.eu/system/files/2021-06/1_en_annexe_acte_autonome_cp_part1_v5_0.pdf) and will be completed as follows:

i) Module Two will apply;

ii) In clause 7, the optional docking clause will not apply;

iii) In Clause 9, Option 2 will apply, and the time period for notice of Sub-processor changes will be as set out in clause 5 of this DPA;

iv) In Clause 11, the optional language will not apply;

v) In Clause 17, Option 1 will apply, and the EEA Standard Contractual Clauses will be governed by Irish law;

vi) In Clause 18 (b), disputes will be resolved before the courts of Ireland;

vii) Annex I of the EEA Standard Contractual Clauses will be deemed completed with the information set out in Schedule 1 to this DPA;

viii) Annex II of the EEA Standard Contractual Clauses will be deemed completed with the information set out in Schedule 3 to this DPA; and

ix) Annex III of the EEA Standard Contractual Clauses will be deemed completed with the information set out in Schedule 2 to this DPA.

d) Transfers of UK Personal Data. The Parties agree that when the transfer of Personal Data from Customer (as data exporter) to Jamf (as data importer) is an ex-UK Transfer, such transfers will be subject to the UK Addendum (official text found here: https://ico.org.uk/media/for-organisations/documents/4019539/international-data-transfer-addendum.pdf) and will be completed as follows:

i) The EEA Standard Contractual Clauses, completed as set out above in clause 4 c) of this DPA, will also apply to transfers of UK Personal Data, subject to sub-clause 4 d) ii) below;

ii) Tables 1 to 3 of the UK Addendum will be deemed completed with relevant information from the EEA Standard Contractual Clauses, completed as set out above, and the option "data importer" will be deemed checked in Table 4. The start date of the UK Addendum (as set out in Table 1) will be the date of this DPA.

e) Transfers of Swiss Personal Data. The Parties agree that when the transfer of Personal Data from Customer (as data exporter) to Jamf (as data importer) is an ex-Swiss Transfer, such transfers will be subject to the Swiss Standard Contractual Clauses:

i) The EEA Standard Contractual Clauses, completed as set out above in clause 4 c) of this DPA, will also apply to transfers of Swiss Personal Data Subject to the modifications and amendments prescribed by the Swiss Federal Data Protection and Information Commissioner (as described here: https://www.edoeb.admin.ch/edoeb/en/home/datenschutz/arbeit_wirtschaft/datenuebermittlung_ausland.html).

f) Further Assurance. If Data Protection Laws require Customer to execute the EEA Standard Contractual Clauses (for ex-EEA Transfers), UK Addendum (for ex-UK Transfers) and/or Swiss Standard Contractual Clauses (for ex-Swiss Transfers) applicable to a particular transfer of Personal Data to Jamf as a separate agreement, Jamf will, on Customer's request, promptly execute such EEA Standard Contractual Clauses, UK Addendum or Swiss Standard Contractual Clauses incorporating such amendments as may reasonably be required by Customer to reflect the applicable sections and Schedules of this DPA, the details of the transfer, and the requirements of the relevant Data Protection Law. If either (i) any of the means of legitimising transfers of Personal Data outside of the EEA or UK which are referred to in this DPA cease to be valid or (ii) any supervisory authority requires transfers of Personal Data pursuant to those means to be suspended, then Jamf may, by notice to Customer and with effect from the date set out in such notice, amend or put in place alternative arrangements for such transfers, as required by the relevant Data Protection Law.

g) Supplementary measures. For any Restricted Transfer, the following supplementary measures will apply:

i) Jamf represents and warrants that, as of the Effective Date, it has not received any Government Agency Requests;

ii) If, after the Effective Date, Jamf receives any Government Agency Requests, it will (unless prohibited by law from doing so) inform the Customer in writing as soon as reasonably practicable and the Customer and Jamf will (as soon as reasonably practicable) discuss and determine whether all or any transfers of Personal Data pursuant to this DPA should be suspended in the light of such Government Agency Requests; and

iii) The Customer and Jamf may meet, as reasonably requested by either Party or as required under applicable Data Protection Laws, to consider whether:

1) The protection afforded by the laws where Jamf is based to Data Subjects whose Personal Data is being transferred is sufficient to provide broadly equivalent protection to that afforded in Switzerland, the EEA and/or the UK;

2) Additional measures are reasonably necessary to enable the transfer to be compliant with the Data Protection Law; and

3) It is still appropriate for Personal Data to be transferred to Jamf, considering all relevant information available to the Parties, together with guidance provided by the supervisory authorities.

5. **Sub-processors.**

a) Approved Sub-processors. The Customer authorizes the Processing of Personal Data by the Sub-processors listed in Schedule 2 (*Approved Sub-Processors*). Jamf will notify the Customer of any change in Sub-processors, including the addition or replacement of Sub-processors, thereby giving the Customer the opportunity to object to such changes. If, within 30 business days of receipt of this notice, the Customer has not objected to the intended change, the Customer is deemed to have authorized the intended change.

b) Contract with Sub-processor. Jamf will impose on all Sub-processors written data protection obligations that offer at least the same protection of Personal Data as the data protection obligations to which Jamf is bound in the Agreement and this DPA. If a transfer of Personal Data between Jamf and a Sub-processor constitutes a Restricted Transfer, Jamf will enter the EEA Standard Contractual Clauses (for an ex-EEA Transfer), the UK Addendum (for an

ex-UK Transfer) and/or the Swiss Standard Contractual Clauses (for an ex-Swiss Transfer) with the Sub-processor. Jamf will remain responsible for complying with the obligations of this DPA and for any acts or omissions of the Sub-processors that cause Jamf to breach any of Jamf's obligations under this DPA.

6. **Data Subject Requests.** If Customer cannot independently address a Data Subject request regarding Personal Data, as required by applicable Data Protection Laws, Jamf will comply with any commercially reasonable request by Customer to facilitate such actions and provide such other assistance in relation to rights of Data Subjects if Jamf is legally required to do so. Customer is responsible for any costs arising from Jamf's assistance if any such assistance exceeds the scope of Jamf's obligations under Data Protection Laws and/or routine customer service. If Jamf expects to incur such additional costs, it will promptly inform Customer in advance and the Parties will then negotiate in good faith to agree on such costs. If a Data Subject contacts Jamf to exercise their rights under applicable Data Protection Laws, and such request relates to Personal Data provided to Jamf by Customer in Customer's role as the data controller, Jamf will use commercially reasonable efforts to redirect the Data Subject to Customer.

7. **Jamf Personnel.**

   a) Confidentiality. Jamf will ensure that its personnel engaged in the Processing of Personal Data are informed of the confidential nature of the Personal Data, have received appropriate training on their responsibilities, and have executed written confidentiality agreements. Jamf will ensure that such confidentiality obligations survive the termination of the personnel engagement.

   b) Limitation of Access. Jamf will ensure that access to Personal Data is limited to personnel performing Services in accordance with the Agreement.

   c) Privacy Officer. Jamf has appointed a privacy officer. The appointed person may be reached at privacy@Jamf.com.

8. **Security.** Jamf has implemented and will maintain technical and organizational measures to secure Personal Data against the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Personal Data and will comply with Data Protection Laws by taking the security measures set out in Schedule 3 (*Security Measures*). Jamf will ensure an appropriate level of security, taking into account the state of the art, the costs of implementation, and the nature, scope, context, and purposes of the Processing as well as the risk of varying likelihood and severity for the rights and freedoms of the Data Subjects.

9. **Personal Data Breach Management and Notification.** Jamf maintains security incident management policies and procedures and will notify Customer of a Personal Data Breach of which Jamf becomes aware without undue delay and provide such further assistance as may be required by Data Protection Laws. To the extent such Personal Data Breach is caused by Jamf's violation of the requirements of this DPA, Jamf will make reasonable efforts to identify and remediate the cause of such Personal Data Breach. If a Personal Data Breach is caused by Customer's violation of the requirements of this DPA, Customer will make reasonable efforts to identify and remediate the cause of such Personal Data Breach.

10. **Data Protection Impact Assessments.** Where the Customer is required to complete a data protection impact assessment or privacy impact assessment under Data Protection Laws, Jamf, upon written request by the Customer, will provide reasonable assistance to the Customer in relation to that requirement. Customer is responsible for any costs arising from Jamf's assistance to the extent such assistance exceeds the scope of Jamf's obligations under Data Protection Laws and/or routine customer service. If Jamf expects to incur additional costs, it will promptly inform Customer in advance and the Parties will then negotiate in good faith to agree on such costs.

11. **Audits.**

    a) In accordance with applicable Data Protection Laws, Jamf allows for, cooperates with, and contributes to audits, including inspections, conducted by Customer or an external auditor engaged by Customer. Audits may be conducted: (i) from time to time on reasonable notice, but no more than once annually; (ii) during normal business hours and so as not to unreasonably interfere with Jamf's performance of the Services under the Agreement or unreasonably interfere with Jamf's business; and (iii) during the term of this DPA. The notice requirement in this section 11a) (i) and the restrictions stated in 11a) (ii) will not apply to the extent the audit is initiated by a regulator or is requested due to a Personal Data Breach. Each Party will bear its own costs in relation to the audit.

    b) Jamf will provide to Customer, its auditors, and regulators reasonable assistance so they can perform an audit, including permitting them access to the following: the place, premises, and facilities from which the Services will be performed; the systems (including software, networks, firewalls, and servers) used to perform the Services; and data, records, manuals, and other information relating to the Services. Jamf will not be required to give Customer or

auditors any access or information that may cause Jamf to compromise its own internal, legal, or regulatory compliance obligations, is subject to confidentiality obligations with its customers, vendors, or other third parties, or is commercially sensitive (such as trade secrets).

c) If an audit results in Jamf being notified that it, or its Processing of Personal Data, does not comply with Data Protection Laws, the Parties will discuss that finding and, with respect to any such non-compliance, Jamf will take corrective actions to achieve compliance to the reasonable satisfaction of the auditor.

.

12. **Term.**

a) Duration. The term of this DPA is the same as the term of the Agreement. Regardless of the termination of this DPA, Jamf is obliged to comply with the provisions of this DPA as long as Personal Data are Processed by Jamf on behalf of Customer.

b) Obligation to Delete or Return Personal Data. Upon termination or expiration of the Agreement and this DPA, and, at the choice of and upon Customer's written request, Jamf will use commercially reasonable efforts to return the Personal Data and all copies to the Customer and/or will securely destroy (delete) the Personal Data and all existing copies in accordance with the Agreement, except if continued storage is required under applicable laws and permitted under Data Protection Laws. In such case, Jamf will inform the Customer of such legal obligation, keep the Personal Data confidential, and only Process the Personal Data if required by applicable laws.

13. **Limitation of Liability**. **NEITHER JAMF NOR ANY OF JAMF'S AFFILIATES OR LICENSORS WILL BE RESPONSIBLE TO CUSTOMER FOR ANY COMPENSATION, REIMBURSEMENT, OR DAMAGES ARISING IN CONNECTION WITH ANY UNAUTHORIZED ACCESS TO, ALTERATION OF, OR THE DELETION, DESTRUCTION, DAMAGE, LOSS, OR FAILURE TO STORE ANY PERSONAL DATA. IN ANY CASE, JAMF'S AND JAMF'S AFFILIATES' AND LICENSORS' AGGREGATE LIABILITY UNDER THIS DPA WILL NOT EXCEED THE AMOUNT CUSTOMER ACTUALLY PAYS JAMF UNDER THE AGREEMENT FOR THE SERVICE THAT GAVE RISE TO THE CLAIM DURING THE 12 MONTHS BEFORE THE LIABILITY AROSE. THE EXCLUSIONS AND LIMITATIONS IN THIS SECTION 13 APPLY ONLY TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW. FOR THE AVOIDANCE OF DOUBT, THIS LIMITATION DOES NOT APPLY TO DATA SUBJECT RIGHTS PROVIDED FOR UNDER APPLICABLE DATA PROTECTION LAWS.**

14. **General Provisions.**

a) Governing Law; Venue; Jurisdiction. Without prejudice to the provisions of the EEA Standard Contractual Clauses, Swiss Addendum, and the UK Addendum addressing the law that governs them, this DPA will be governed by and construed in accordance with the laws which govern the Agreement and the venue and dispute resolution provisions under the Agreement will also apply to disputes and claims under this DPA.

b) Entire Agreement/Order of Precedence. This DPA constitutes the entire agreement between the Parties with respect to its subject matter and supersedes all prior understandings regarding such subject matter, whether written or oral. If a conflict exists between this DPA and the Agreement regarding the subject matter of this DPA, the terms of this DPA will govern. If a conflict exists between this DPA and the Standard Contractual Clauses regarding the subject matter of this DPA, the applicable Standard Contractual Clauses will govern.

c) Amendment. No amendment or modification of this DPA will be binding unless in writing and signed by the Parties.

d) Waiver. Any waiver by a Party of a breach of any provision of this DPA will not operate as or be construed as a waiver of any further or subsequent breach.

e) Survival. Provisions of this DPA that by their nature are to be performed or enforced following any termination of this DPA will survive such termination.

f) Assignment. Jamf may assign this DPA to an affiliate or in connection with a merger of Jamf or the sale of substantially all Jamf's assets.

g) Binding Effect. This DPA will be binding upon and inure to the benefit of the Parties, their successors, and permitted assigns.

h) Unenforceability and Severability. If for any reason, a court of competent jurisdiction or duly appointed arbitrator finds any provision or portion of this DPA to be unenforceable, the remainder of this DPA will continue in full force and effect.

i) Translations. If this DPA is translated into languages other than English, the English version will control.

j) Headings. The headings are for convenience only and do not affect the interpretation of this DPA.

k) Counterparts. This DPA may be executed by electronic signature and in counterparts, which together constitute one binding agreement.

l) Third-party Rights. Except to the extent expressly provided by any of the Standard Contractual Clauses with respect to Data Subjects, this DPA does not give rise to any rights for third parties to enforce any term of this DPA.

15. **Authority of Signatories**. Each person signing this DPA represents and warrants that they are duly authorized and have legal capacity to execute it.

Jamf Software, LLC

Signature:

Name:

Title:

Date:

Jamf Internal Account Reference:

Customer

Signature:

Name:

Title:

Date:

Full Company Legal Name:

Type of Legal Entity:

Street Address:

State/Province:

Postal Code:

SCHEDULE 1
DETAILS OF PROCESSING

A. List of Parties

(1) Data exporter(s): [Identity and contact details of the data exporter(s) and, where applicable, of its/their data protection officer and/or representative in the European Union]

Name: _____

Address: _____

Contact person's name, position, and contact details: _____

_____

Activities relevant to the data transferred under these Clauses: use of Services provided by Jamf.

Signature and date: _____

Role (controller/processor): Controller

(2) Data importer:
Name: JAMF Software, LLC

Address: 100 Washington Avenue South, Suite 1100, Minneapolis, MN 55401 USA

Contact person's name, position, and contact details: Justin Francis, Vice President, Enterprise Risk & Compliance; privacy@jamf.com; +1 612-605-6625

Activities relevant to the data transferred under these Clauses: Jamf's provision of Services under the Agreement.

Signature and date:

Role (controller/processor): Processor

B. Description of Transfer

Categories of Data Subjects whose Personal Data is transferred: employees or contractors of Customer.

Categories of Personal Data transferred: Names, user identifier, device identifiers, IP addresses, telephone numbers, computer names, job titles and functions, and email addresses.

Sensitive data/special categories transferred (if any): none.

Frequency of transfer: the frequency of the transfer of Personal Data is directly related to the nature of processing.

Nature of the Processing: Process Personal Data if Customer enters Personal Data into Customer's instance of the Hosted Services provided by Jamf pursuant to the Agreement. Jamf utilizes sub-processors for infrastructure to provide the Hosted Services in which Personal Data is stored.

Purpose(s) of the data transfer and further processing: the purpose of data transfers is for Customer to utilize Jamf's Services.

The period for which Personal Data will be retained, or, if that is not possible, the criteria used to determine that period: Personal Data is retained in accordance with the Agreement and this DPA.
For transfers to (sub-) processors, also specify subject matter, nature, and duration of the Processing: Jamf utilizes the approved Sub-processors set forth in and as further described in Schedule 2. The duration of the Processing is equivalent to the length of time Customer utilizes Jamf's Services under the Agreement.

C. Competent Supervisory Authority (identify the competent supervisory authority/ies in accordance with Clause 13 of Schedule 4 to the DPA (EEA Standard Contractual Clauses)): The competent supervisory authority is identified in Clause 13 of the EEA Standard Contractual Clauses and will be either 13 (a) (i), (ii), or (iii), whichever is applicable to Customer (data exporter).

SCHEDULE 2
APPROVED SUB-PROCESSORS

Jamf's sub-processor list can be found at https://www.jamf.com/jamf-subprocessors/.

SCHEDULE 3
SECURITY MEASURES

Processing of Personal Data takes place on data processing systems for which technical and organizational measures for protecting such data have been implemented. In this context, Jamf assures Customer that it will take all reasonable measures required to ensure such Processing is done in accordance with applicable Data Protection Laws. Considering the state of technological development and the cost of implementing such measures, Jamf will ensure a level of security appropriate to the harm that might result from unauthorized or unlawful Processing or accidental loss, destruction, or damage, considering the nature of the Personal Data to be protected.

Jamf will implement the following measures:

1. **Information Security Policies and Measures.**

   a) Policies. Jamf's information security policies will be documented and approved by Jamf's senior management.

   b) Review of the Policies. Jamf's information security policies will be reviewed by Jamf at least annually, or promptly after material changes are made to the policies to confirm applicability and effectiveness. Jamf will not make changes to the policies that would materially degrade Jamf's security obligations.

   c) Information Security Reviews. Jamf will independently review its approach to managing information security and its implementation (i.e., control objectives, controls, policies, processes, and procedures for information security) at planned intervals or when significant changes occur.

   d) Disaster Recovery. During the term of the Agreement, Jamf will maintain a disaster recovery (DR) or high availability (HA) solution and related plan that is consistent with industry standards for the Services Jamf provides to Customer. Jamf will test the DR or HA solution and related plan at least once annually. In addition, the solution and related plan will ensure:

      i) that installed systems used to provide Services will be restored in case of interruption;

      ii) Jamf's ability to restore the availability and access to Customer Data in a timely manner in the event of a physical or technical incident; and

      iii) the ongoing confidentiality, integrity, availability, and resilience of systems Jamf uses to provide Services.

   e) Testing. Jamf will maintain a process for regularly testing the effectiveness of its technical and organizational measures for ensuring the security of the processing of Customer Data.

2. **Information Security Framework.**

   a) Security Accountability. Jamf will assign one or more security officers who will be responsible for coordinating and monitoring all information security functions, policies, and procedures.

   b) Security Roles and Responsibility. Jamf personnel, contractors and agents who are involved in providing Services will be subject to confidentiality agreements with Jamf.

   c) Risk Management. Jamf will perform appropriate information security risk assessments as part of an ongoing risk governance program with the following objectives (i) recognize risk, (ii) assess the impact of risk, and (iii) where risk reduction or mitigation strategies are identified and implemented, effectively manage the risk with recognition that the threat landscape constantly changes.

3. **Human Resource Security.**

   a) Security Training. Jamf will provide appropriate security awareness, education, and training to all Jamf personnel and contractors with access to the Services provided to Customer.

   b) Background Screening. Jamf will ensure that background checks have been performed on Jamf personnel who are part of teams managing Jamf's hosting infrastructure. Additionally, background checks will be performed on Jamf personnel or agents assigned to provide Services at Customer's premises. Jamf will perform background checks in accordance with applicable law and Jamf's background screening policies and procedures. Only individuals who

have passed background checks will be allowed by Jamf to provide Services at Customer's premises or be part of Jamf's teams managing Jamf's hosted infrastructure.

4. **Asset Management.**

a) Asset Inventory.

i) Jamf will maintain an asset inventory of all media and equipment where Customer Data is stored. Jamf will restrict access to such media and equipment to authorized personnel of Jamf. Jamf will prevent the unauthorized reading, copying modification or removal of data media.

ii) Jamf will classify Customer Data so that it is properly identified and will appropriately restrict access to Customer Data. Specifically, Jamf will ensure that no person appointed by Jamf to process Customer Data, will process Customer Data unless that person:

1) has a need to access Customer Data for the purpose of performing Jamf's obligations under the Agreement;

2) has been authorized by Jamf in a manner consistent with Jamf's information security policies;

3) has been fully instructed by Jamf in the procedures relevant to the performance of the obligations of Jamf under the Agreement, in particular the limited purpose of processing Customer Data; and

4) is aware that they are prohibited from copying any Customer Data transmitted by Customer to Jamf, provided, however, that Jamf may retain copies of Customer Data provided to it under the Agreement in its servers for backup and archive purposes until completion of the Agreement.

iii) Jamf will further maintain measures to ensure that persons appointed by Jamf to process Customer Data will prevent the unauthorized input of Customer Data and the unauthorized inspection, modification, or deletion of stored Customer Data.

iv) Jamf will maintain an appropriate approval process whereby approval is provided to personnel, contractors, and agents prior to storing Customer Data on portable devices or remotely accessing Customer Data. All approvals will be subject to measures designed to prevent the unauthorized reading, copying, modification or deletion of Customer Data during transfers of such content or during transportation of data media. If remote access is approved and granted, Jamf personnel, agents, and contractors will use multi-factor authentication. Multi-factor authentication may include techniques such as the use of cryptographic certificates, one-time-password (OTP) tokens, or biometrics.

b) Security of Software Components. Jamf agrees to appropriately inventory all software components (including open-source software) used with Jamf's Services. Jamf will assess whether any such software components have any security defects and/or vulnerabilities that could lead to unauthorized disclosure of Customer Data. Jamf will perform such assessment prior to delivery of, or providing Customer access to, Jamf's Services and on an on-going basis thereafter during the term of the Agreement. Jamf agrees to remediate any security defect or vulnerability it detects in a timely manner.

5. **Access Control.**

a) Policy.

i) Jamf will maintain an appropriate access control policy that is designed to restrict access to Customer Data and Jamf assets to authorized personnel, agents, and contractors. To ensure clarity, all references to user accounts and passwords in this section relate only to Jamf's users, user accounts, and passwords. This Section 5 does not apply to Customer's access to and use of the Services, Customer user accounts, or Customer passwords.

b) Authorization.

i) Jamf will maintain user account creation and deletion procedures for granting and revoking access to all assets, Customer Data, and all Jamf internal applications while providing Services under the Agreement. Jamf will assign an appropriate authority to approve creation of user accounts or elevated levels of access for existing accounts.

ii) Jamf will maintain and update records of employees and contractors who are authorized to access systems that are involved in providing Services to the Customer and review such records at least quarterly. Administrative and technical support personnel, agents, or contractors will only be permitted to have access to such data when required; provided, such personnel, agents, or contractors comply with applicable Jamf technical and organizational measures.

iii) Jamf will ensure the uniqueness of user accounts and passwords for everyone. Individual user accounts will not be shared.

iv) Jamf will remove access rights of personnel and contractors to assets that store Customer Data upon termination of their employment, contract, or agreement within 24 hours, or adjust access upon change of personnel role.

c) Authentication.

i) Jamf will use industry standard capabilities to identify and authenticate personnel, agents, and contractors who attempt to access information systems and assets.

ii) Jamf will maintain industry standard practices to deactivate passwords that have been corrupted or disclosed.

iii) Jamf will monitor for repeated access attempts to information systems and assets.

iv) Jamf will maintain industry standard password protection practices that are designed to maintain the confidentiality and integrity of passwords generated, assigned, distributed, and stored in any form.

v) Jamf will use multi-factor authentication for all administrative access, including domain and cloud portal administrative access. Multi-factor authentication may include techniques such as the use of cryptographic certificates, one-time-password (OTP) tokens or biometrics.

d) Data-processing Equipment.

i) Jamf will deny unauthorized persons access to systems and equipment used for processing Customer Data ("**Data-Processing Equipment**").

ii) Jamf will prevent the use of automated Data-Processing Equipment by unauthorized persons using data communication equipment.

iii) Jamf will ensure that persons authorized to use an automated Data-Processing Equipment only have access to the Customer Data covered by their access authorization.

iv) Jamf will ensure that it is subsequently possible to verify and establish which Customer Data has been put into automated Data-Processing Equipment when it was added and by whom the input was made.

6. **Cryptography**. Jamf will maintain policies and standards regarding the use of cryptographic controls that are implemented to protect Customer Data. Such protections will include the pseudonymization and encryption of Personal Data, as further detailed below in Section 9. Jamf will implement industry standard key management policies and practices designed to protect encryption keys for their entire lifetime.

7. **Physical and Environmental Security.**

a) Physical Access to Facilities. Jamf will limit access to facilities where systems that are involved in providing the Services are located to identified personnel, agents, and contractors.

b) Protection from Disruptions. Jamf will use reasonable efforts, and, to the best of Jamf's ability and to the extent within Jamf's control, protect equipment from power failures and other disruptions caused by failures in supporting utilities.

c) Secure Disposal or Reuse of Equipment. Jamf will verify that all Customer Data has been deleted or securely overwritten from equipment containing storage media using industry standard processes prior to disposal or re-use.

8. **Operations Security.**

a) Operations Policy. Jamf will maintain appropriate operational and security operating procedures and such procedures will be made available to all Jamf personnel who require them.

b) Protections from Malware. Jamf will maintain anti-malware controls that are designed to protect systems from malicious software, including malicious software that originates from public networks.

c) Configuration Management. Jamf will have policies that govern the installation of software and utilities by personnel.

d) Change Management. Jamf will maintain and implement procedures to ensure that only approved and secure versions of the code, configurations, systems, and applications will be deployed in the production environment(s).

e) Encryption of Data. Encryption solutions will be deployed with no less than 256-bit Advanced Encryption Standard (AES) encryption.

f) Systems. Jamf will ensure that the functions of the systems utilized to provide Services perform, that the appearance of faults in the functions is reported, and that stored Customer Data cannot be corrupted by means of a malfunctioning of such systems.

9. **Communications Security.**

a) Information Transfer.

i) With respect to Jamf's Hosted Services, Customer Data is encrypted in-transit to the Hosted Services and maintained in encrypted storage. Jamf will use industry standard encryption to encrypt Customer Data.

ii) Jamf will restrict access through encryption to Customer Data stored on media that is physically transported from Jamf facilities.

iii) Jamf will ensure that it is possible to verify and establish the extent to which Customer Data has been or may be transmitted or made available using data communication equipment.

b) Security of Network Services.

i) Jamf will ensure that industry standard security controls and procedures for all network services and components are implemented whether such services are provided in-house or outsourced.

c) Intrusion Detection.

i) Jamf will deploy intrusion detection or intrusion prevention systems for all systems used to provide Services to Customer to provide continuous surveillance for intercepting and responding to security events as they are identified and update the signature database as soon as new releases become available for commercial distribution.

d) Firewalls.

i) Jamf will have appropriate firewalls in place which will only allow documented and approved ports and services to be used. All other ports will be in a deny all mode.

10. **System Acquisition, Development and Maintenance.**

a) Workstation Encryption. Jamf will require hard disk encryption of at least 256-bit Advanced Encryption Standard (AES) on all workstations and/or laptops used by personnel, contractors, and agents where such personnel are accessing or processing Customer Data.

b) Application Hardening.

i) Jamf will maintain and implement secure application development policies, procedures and standards that are aligned to Industry Standard practices such as the SANS Top 25 Security Development Techniques or the OWASP Top Ten project.

ii) All personnel responsible for secure application design, development, configuration, testing, and deployment will be qualified to perform the Services and receive appropriate training regarding Jamf's secure application development practices.

c) System Hardening.

i) Jamf will establish and ensure the use of standard secure configurations of operating systems. Images should represent hardened versions of the underlying operating system and the applications installed on the system. Hardening includes removal of unnecessary accounts (including service accounts), disabling or removal of unnecessary services, applying patches, closing open and unused network ports, and implementing intrusion detection systems and/or intrusion prevention systems. These images should be validated on a regular basis to update their security configuration as appropriate.

ii) Jamf will perform periodic (at least quarterly) access reviews for system administrators for all supporting systems requiring access control.

iii) Jamf will implement patching tools and processes for both applications and operating system software. When outdated systems can no longer be patched, Jamf will update to the latest version of application software. Jamf will remove outdated, unsupported, and unused software from the system.

iv) Jamf will limit administrative privileges to only those personnel who have both the knowledge necessary to administer the operating system and a business need to modify the configuration of the underlying operating system.

d) Infrastructure Vulnerability Scanning. Jamf will scan its internal environment (e.g., servers, network devices, etc.) related to the Services monthly and external environment related to the Services on a weekly basis. Jamf will have a defined process to address any findings but will ensure that any high-risk vulnerabilities are addressed no later than 30 days after discovery.

e) Application Vulnerability Assessment. Jamf will perform an application security vulnerability assessment prior to any new public release. Jamf will have a defined process to address any findings but will ensure that any high-risk vulnerabilities are addressed within 30 days of discovery.

f) Penetration Tests and Security Evaluations of Websites. Jamf will perform a comprehensive penetration test and security evaluation of all systems and websites involved in providing Services on a recurring basis no less frequent than once annually. Additionally, Jamf will have an industry-recognized independent third party perform an annual test. Jamf will have a defined process to address any findings but will ensure that any high-risk vulnerabilities are addressed within 30 days of discovery. Upon Customer's written request, but no more than once per year, Jamf will provide an assertion statement to validate the completion of the independent third-party penetration test and attest to the fact that Jamf maintains a process to address findings.

11. **Jamf Relationships.**

a) If Jamf must use a third-party application or service to provide the Services, Jamf's contract with that third-party vendor must clearly outline security requirements for the third-party vendor consistent with the security requirements of this Information Security Schedule. In addition, service level agreements with the third party must be clearly defined.

b) Any third-party gaining access to Jamf systems must be covered by a signed agreement containing confidentiality and security provisions consistent with the confidentiality and security requirements of the Agreement and this Information Security Schedule.

c) Jamf will perform quality control and security management oversight of outsourced software development.