DATA PROCESSING AGREEMENT FOR JAMF CUSTOMERS

This Data Processing Agreement (the "**DPA**") is made by and between the Jamf Contracting Party that entered into the Agreement, and its Affiliates ("**Jamf**" or "**we**" or "**us**"), and the organization identified below or who has clicked through and accepted the Agreement as part of the Product Offering ("**Customer**" or "**you"**), each a "**Party**" and collectively the **"Parties**." It is incorporated by reference and supplements either Jamf's Software License and Services Agreement or other negotiated agreement between the Parties pursuant to which we provide Services to you, and any subsequent amendments or orders (the **"Agreement"**).

1) **Overview**. This DPA applies when we Process any Personal Data when providing Services under the Agreement. It is effective from the earliest of either the date of the last signature below, or the date that you click to accept the Agreement as part of the Product Offering (the **"DPA Effective Date"**) and will terminate on the same date that the Agreement terminates (the "**Term"**).

2) **Definitions**. Capitalized terms not defined in the DPA will have the meanings given to them in the Agreement. 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. Any terms not defined in this DPA or the Agreement will have the same meaning as set out in the Standard Contractual Clauses, the CPRA or the GDPR or UK GDPR, as relevant.

   a) "**Data Protection Laws**" means all applicable data protection, privacy, and cyber security laws, rules, and regulations of any country, including (i) the EU General Data Protection Regulation 2016/679 ("**GDPR**"), (ii) the UK General Data Protection Regulation, with the meaning given in section 3(10) (as supplemented by section 205(4)) of the Data Protection Act 2018 ("**UK GDPR**"), (iii) the Swiss Federal Act on Data Protection of 25 September 2020 (SR 235.1), as in force from 1 September 2023 ("**Swiss Data Protection Act**"), (iv) 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), (v) the California Consumer Privacy Act of 2018, as amended by the California Privacy Rights Act of 2020 (collectively referred to as the "**CPRA**"), and (vi) any other data protection, privacy, or data security law applicable to our Processing of Personal Data in our capacity as a Processor in connection with the Services, in each case as amended or superseded from time to time.

   b) "**Data Subject**" means the identified or identifiable individual to whom Personal Data relates.

   c) "**ex-EEA Transfer**" means a Processing activity whereby you transfer Personal Data that is Processed under the GDPR to us outside the EEA, and such transfer is not governed by an adequacy decision made by the European Commission ("**EC**") in accordance with the relevant provisions of the GDPR.

   d) "**ex-Swiss Transfer**" means a Processing activity whereby you transfer Personal Data that is Processed under Swiss Data Protection Laws to us 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.

   e) "**ex-UK Transfer**" means a Processing activity whereby you transfer Personal Data that is Processed under the UK Data Protection Laws to us outside the UK, and such transfer is not governed by an adequacy decision pursuant to Section 17A of the UK Data Protection Act 2018**.**

   f) "**Government Agency**" means a government agency or law enforcement authority, including judicial authorities.

   g) "**Personal Data**" means any personal data (as defined in applicable Data Protection Laws) we or our Sub-processors Process when providing Services to you under the Agreement.

   h) **"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 Processed by us.

   i) "**Processing**" or "**Process**" means any operation or set of operations that is performed upon Personal Data or on sets of Personal Data, whether or not by automatic means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making

available, alignment or combination, restriction, blocking, erasure, or destruction.

j) "**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.

k) "**Services**" means the services that we provide you as defined in the Agreement and includes Product Offerings.

l) **"Standard Contractual Clauses**" or "**SCCs**" means

i) where the GDPR applies, the standard contractual clauses approved by the EC and annexed to the EC'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.199A(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.

m) "**Sub-processor**" means any third party we engage to Process Personal Data.

3) **CPRA Processing of Personal Data**. If the CPRA applies to any Personal Data we receive from or on behalf of you during the provision of Services, then:

a) You agree you are disclosing such Personal Data to us only for the limited and specified business purposes relating to the Services under the Agreement.

b) We will comply with all applicable sections of the CPRA, including providing the same level of privacy protection to such Personal Data as required of businesses under the CPRA, and 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 you and us unless expressly permitted by the CPRA.

c) We 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 behavioral advertising (as defined by the CPRA), whether for monetary or other valuable consideration.

d) We may disclose such Personal Data to our service providers in connection with their provision of Services and permit such service providers to Process Personal Data as necessary for us to provide the Services to you if we notify you of our engagement of such service providers and obligate them to provide the same level of protection under the CPRA. Section 5 of this DPA sets out our compliance with Civil Code § 1798.140 (ag) (2).

e) We will not combine or update such Personal Data with other personal data that we receive from, or on behalf of, other entities or persons, or collected from our own interaction with a Data Subject, except as expressly permitted under the CPRA.

f) As defined by the 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 out in California Civil Code § 1798.140 (m). If you make deidentified information available to us in connection with the Agreement, we 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).

g) In accordance with Section 8 below, we confirm that we have implemented reasonable security procedures and practices designed to protect such Personal Data from unauthorized or illegal access, destruction, modification, or disclosure.

h) As provided for in Section 9 below, we grant you the right, upon your notice, to take reasonable and appropriate steps

to stop and remediate the unauthorized use of such Personal Data, and pursuant to Sections 10 and 11 below, we grant you the right to take reasonable and appropriate steps to help ensure that we use such Personal Data transferred to us in a manner consistent with your obligations under the CPRA.

i) We will notify you if we determine that we can no longer meet our obligations under the CPRA and grant you the right to take reasonable and appropriate steps to stop providing Personal Data to us.

j) We certify that we understand the restrictions set out in this Section 3 and will comply with them.

4) **Processing of Personal Data**.

a) Relationship of the Parties. You are the Controller of Personal Data, and we are a Processor.

b) Processing. We will Process Personal Data as necessary to perform our obligations under the Agreement as set out in Schedule 1 to this DPA, and strictly in accordance with your documented instructions, except where otherwise required by any law applicable to us. We may make reasonable amendments to Schedule 1 from time to time as reasonably necessary to reflect new product features. We will notify you in advance in writing of any amendment to Schedule 1 that expands the scope, categories, or purposes of existing Processing and make the updates available on our Trust Center at https://www.jamf.com/trust-center/legal/. You will be deemed to have accepted the change (and thereby updated your instructions to us) if you continue to use the Services. We will inform you if we become aware that your Processing instructions infringe applicable Data Protection Laws (but without obligation to actively monitor your compliance with applicable Data Protection Laws).

c) Transfers of EEA Personal Data. The Parties agree that when the transfer of Personal Data from you (as data exporter) to us (as data importer) is an ex-EEA Transfer, such transfers will be subject to the EEA Standard Contractual Clauses (official text found here: Implementing decision - 2021/914 - EN - EUR-Lex) and will be completed as follows:

i) Module Two will apply;

ii) In Clause 7, the optional docking clause will not apply (unless requested by you giving a detailed reason);

iii) In Clause 9, Option 2 will apply, and the time period for notice of Sub-processor changes will be as set out in Section 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 you (as data exporter) to us (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/media2/migrated/4019539/international-data-transfer-addendum.pdf) and will be completed as follows:

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

ii) Tables 1 to 3 of the UK Addendum will be 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 DPA Effective Date.

e) Transfers of Swiss Personal Data. The Parties agree that when the transfer of Personal Data from you (as data exporter) to us (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 Section 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/dam/en/sd-web/smvG75WY5Vsi/%C3%9Cbermittlung).

f) Conflict. If any provision of this DPA contradicts, directly or indirectly, the Standard Contractual Clauses, the Standard Contractual Clauses shall prevail.

g) Further Assurance. If Data Protection Laws require Customer to execute the applicable Standard Contractual Clauses as a separate agreement, we will provide this on Customer's request. If either (i) any of the means of legitimizing transfers of Personal Data outside of the EEA, UK, or Switzerland 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 we may, with notice to you 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 Laws. If this DPA needs to be modified because of a change in Data Protection Laws, including a change to the Standard Contractual Clauses, then either Party may provide written notice to the other Party of the change. The Parties will discuss and negotiate, in good faith, any necessary changes to this DPA to address such changes in Data Protection Laws.

h) Supplementary measures.

i) We represent and warrant that, as of the DPA Effective Date, we have not received any Government Agency requests for customer data, which may include Personal Data;

ii) Subject to Section 4 (h)(iii) below, if, after the DPA Effective Date, we receive any Government Agency requests for your data, which may include Personal Data, we will

1) inform you in writing as soon as reasonably practicable (unless prohibited by applicable law) so that you, as the Controller, can work directly with the Government Agency;
2) inform the Government Agency that we are a Processor of the Personal Data and that the Controller has not authorized us to disclose Personal Data to the Government Agency;
3) inform the Government Agency that all requests or demands for access to the Personal Data should be notified to and served upon you (as the Controller) in writing;
4) not provide the Government Agency with access to the Personal Data, unless and until authorized by you; and;
5) together we will discuss and determine whether all or any transfers of Personal Data pursuant to this DPA should be suspended in the light of such requests.

iii) If there is an applicable law that prevents us from complying with Section 4 (h)(ii) above in full, we will use reasonable and lawful efforts to challenge such prohibition or compulsion (though you acknowledge that such challenge may not always be reasonable or possible in light of the nature, scope, context and purposes of the intended Government Agency access request).

iv) We will only disclose such Personal Data if we are legally required to do so and in accordance with applicable lawful process.

v) Sections 4 (h)(ii) and (iii) will not apply if, taking into account the nature, scope, context, and purposes of the intended Government Agency's access to the Personal Data, we have a reasonable and good faith belief that urgent access is necessary to prevent an imminent risk of serious harm to any individual. If that happens, we will notify you as soon as possible following such Government Agency's access and provide you with full details of the same, unless we are prohibited from doing so.

vi) We will not knowingly disclose Personal Data to a Government Agency in a massive, disproportionate, and indiscriminate manner that goes beyond what is necessary in a democratic society.

vii) We will maintain and comply with a policy governing Personal Data access requests from Government Agencies which at a minimum prohibits:

1) Massive, disproportionate, or indiscriminate disclosure of Personal Data relating to Data Subjects in Europe; and

2) Disclosure of Personal Data relating to Data Subjects in Europe to a Government Agency without a subpoena, warrant, writ, decree, summons, or other legally binding order that compels disclosure of Personal Data.

viii) We will have in place and maintain in accordance with good industry practice measures to protect the Personal Data from interception (including in transit from you to us and between different systems and services). This includes having in place and maintaining network protection to deny attackers the ability to intercept data and encryption of the Personal Data while in transit to deny attackers the ability to read data.

ix) The primary transfer mechanism used for the transfer of Personal Data outside the EEA, UK, or Switzerland to the United States is the approved and applicable SCCs that are incorporated into this DPA. We are also certified as a participant in the EU-U.S. Data Privacy Framework ("DPF")", which replaced the EU-U.S. Privacy Shield and is a supplementary measure for international transfers.

5) **Sub-processors**.

a) Approved Sub-processors. You authorize the Processing of Personal Data by the Sub-processors listed in Schedule 2 ("**Approved Sub-processors**"). We will notify you of any intended addition or replacement of a Sub-processor, giving you the opportunity to object to the intended change. If, within 30 calendar days of receipt of that notice you have not objected to the intended change, you are deemed to have authorized the change. If you object to a new or replacement Sub-processor on reasonable grounds relating to the protection of the Personal Data, we will use reasonable efforts to recommend a commercially reasonable alternative. If we are unable to provide an alternative within 30 days of receipt of your objection, either Party may terminate the affected Services giving written notice.

b) Contract with Sub-processor. We will impose on all Sub-processors written data protection obligations that offer the same standard of protection of Personal Data as the data protection obligations to which we are bound in the Agreement and this DPA. If a transfer of Personal Data between us and a Sub-processor constitutes a Restricted Transfer, we will enter into the relevant SCCs with the Sub-processor. We will remain responsible for complying with the obligations of this DPA and for any acts or omissions of the Sub-processors that cause us to breach any of our obligations under this DPA.

6) **Cooperation, Data Subject Requests, and Data Protection Complaints.** Considering the nature of Processing and the information available, the Parties will assist each other to fulfil their obligations to respond to Data Subject rights requests and data protection complaints under applicable Data Protection Laws. If we receive a (i) Data Subject request or (ii) any other correspondence, inquiry, or complaint from a Data Subject, regulator, or other third party in connection with the processing of the Personal Data by us on your behalf we will, unless legally prohibited from doing so, notify you in writing without undue delay and provide full details of the same. We will not respond substantively to any such correspondence without your prior written instructions, unless required to do so by applicable law. If you are unable to respond to a Data Subject request or complaint independently, we will, on your written request, provide reasonable assistance to enable you to investigate and respond, including by making available relevant information and personnel. If any costs we incur in providing such assistance exceed the scope of our obligations under Data Protection Laws and/or routine customer service, we will inform you in advance and the Parties will negotiate in good faith to agree to such costs.

7) **Jamf Personnel.**

a) Confidentiality. We will ensure that 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. We will ensure that such confidentiality obligations survive the termination of the personnel engagement.

b) Limitation of Access. We will ensure that access to Personal Data is limited to personnel performing Services in

accordance with the Agreement.

c) Privacy Officer. We have appointed a privacy officer, who may be reached at privacy@jamf.com.

8) **Security**. We have implemented and will maintain appropriate 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 referred to in Article 32(1) of the GDPR as appropriate, and at a minimum, meet the requirements set out in Schedule 3 to this DPA (*Security Measures*).

9) **Personal Data Breach Management and Notification**. We maintain security incident management policies and procedures and will notify you of any Personal Data Breach without undue delay and, when possible, no later than 72 hours upon becoming aware of a Personal Data Breach. We will provide you with timely information and cooperation as needed for you to fulfil your breach reporting obligations under applicable Data Protection Laws. Our Personal Data Breach notification to you will include, if known and available to us: (a) nature of the breach; (b) contact details of our designated contact; (c) likely consequences; and (d) remediation measures taken or proposed. If the Personal Data Breach was caused by our violation of our obligations under this DPA, we will make reasonable efforts to identify and remediate the cause of the Personal Data Breach. If your violation of your obligations under this DPA causes a Personal Data Breach, you will make reasonable efforts to identify and remediate the cause and we will have no obligation to independently investigate it, though we will cooperate with your investigation. Unless required by applicable Data Protection Laws, we will not inform any third party of any such Personal Data Breach without your prior written consent. If you notify us of any unauthorized use of Personal Data, we will take reasonable steps to stop and remediate that use.

1) **Data Protection Impact Assessments.** Jamf's Trust Center (found at https://www.jamf.com/trust-center/legal/) contains resources to assist customers with completing data protection or privacy impact assessments required under Data Protection Laws. Upon your reasonable request, and if you cannot reasonably complete them independently with the provided resources, we will provide you with reasonable assistance to complete a data protection impact or privacy impact assessment or, if necessary, consult with the relevant data protection authority. If such assistance exceeds the scope of our obligations under Data Protection Laws, and/or routine customer service, we will promptly inform you in advance and the Parties will then negotiate in good faith to agree on any additional costs.

2) **Audits.**

a) **Audit Reports.** We are regularly audited against recognized compliance standards (such as SOC 2 and ISO 27001) by independent third-party auditors and/or internal auditors. Upon written request, and provided that you have entered into a non-disclosure agreement with us, we will provide you with a summary copy of the relevant third-party audit report(s) (a **"Summary Audit Report")** so you can verify our compliance with the audit standards against which it has been assessed and this DPA. All Summary Audit Reports are designated as Jamf Confidential Information. If you cannot reasonably verify our compliance with the terms of this DPA based on the Summary Audit Report, we will provide written responses to your reasonable requests for information related to our Processing of Personal Data, no more than once every 12 months. Where the scope of a requested audit is covered by a Summary Audit Report and we confirm that, to our knowledge, there have been no material changes to the audited controls, you agree to rely on that report instead of auditing the same controls under Section 11 (b).

b) **Audits.** Only if you cannot reasonably confirm our compliance with this DPA by one of the options listed in Section 11 (a) above, or if required by applicable Data Protection Laws or a competent data protection authority, you, or your authorized representatives, may, at your expense, conduct an audit to assess our compliance with the terms of this DPA. Any audit must be conducted during our regular business hours, with advance written notice of at least 60 calendar days, unless a shorter interval or additional audit is required by a competent data protection authority, or you believe a further audit is necessary due to a Personal Data Breach suffered by us. You must ensure that you and your authorized representatives keep confidential any information disclosed in the audit. You may perform an audit no more than once every 12 months and must restrict the scope to only information relevant to you. If an audit identifies material non-compliance with this DPA, we will reimburse your reasonable, documented, third-party audit costs.

c) You may exercise the information request right under Section 11 (a) or conduct an on-site audit under Section 11 (b), but not both, within any rolling 12-month period, unless a shorter interval or additional audit is required by applicable Data Protection Laws.

d) We will provide to you, your auditors, and regulators reasonable assistance with an audit, including, where applicable,

permitting access to (i) the premises and facilities under our control (or that we are permitted to provide access to) from which the Services will be performed; (ii) the systems (including software, networks, firewalls, and servers) used to perform the Services; and (iii) data, records, manuals, and other information relating to the Services. We will not be required to give you or auditors any access or information that may cause us to compromise our own internal, legal, or regulatory compliance obligations; is subject to confidentiality obligations with our customers, vendors, or other third parties; or is commercially sensitive (such as trade secrets).

e) If an audit shows that our Processing of Personal Data does not comply with Data Protection Laws, the Parties will discuss that finding and we will take any required corrective actions to achieve compliance.

3) **Obligations upon Termination**. 90 days following termination or expiration of the Agreement and this DPA, on your request, we will return the Personal Data and all copies to you and/or will securely delete the Personal Data and all existing copies in accordance with the Agreement, except if continued storage is required and permitted under Data Protection Laws. In such case, we will inform you of such legal obligation and keep the Personal Data confidential.

4) **Limitation of Liability**. **TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, AND EXCEPT AS SPECIFICALLY PROVIDED IN THE STANDARD CONTRACTUAL CLAUSES AS APPLICABLE, THE TOTAL AGGREGATE LIABILITY OF EACH PARTY AND ITS AFFILIATES ARISING OUT OF OR RELATED TO THIS DPA IS SUBJECT TO THE LIMITATION OF LIABILITY SECTION OF THE AGREEMENT, AND ANY REFERENCE IN SUCH SECTION TO THE LIABILITY OF A PARTY MEANS THE AGGREGATE LIABILITY OF THAT PARTY AND ALL OF ITS AFFILIATES UNDER THE AGREEMENT AND DPA TOGETHER. FOR THE AVOIDANCE OF DOUBT, THIS LIMITATION DOES NOT APPLY TO DATA SUBJECT RIGHTS PROVIDED FOR UNDER APPLICABLE DATA PROTECTION LAWS.**

5) **General Provisions**.

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

b) Entire Agreement and 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. We may assign this DPA to an Affiliate or in connection with a merger, acquisition, sale, or other transfer of substantially all our 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.

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

Jamf Contracting Party identified in the Agreement	**Customer**
Signature:	Signature:
Name:	Name:
Title:	Title:
Date:	Date:
	Full Company Legal Name:
	Type of Legal Entity:
	Street Address:
	State/Province:
	Postal Code:
	City:
	Country:

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: _____ or as set out in the Customer Order

Address: _____or as set out in the Customer Order

Contact person's name, position, and contact details: _____or as set out in the Customer Order

Activities relevant to the data transferred under these Clauses: Use of Jamf Services.

Signature and date: _____or as accepted in the Product Offering

Role (controller/processor): Controller

(2) Data importer:

Name: The Jamf Contracting Party identified in the Agreement

Address: The registered address of the Jamf Contracting Party identified in the Agreement

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: _____ October 1st 2026

Role (controller/processor): Processor

B. Description of Transfer

Description	**Details**
Subject matter of the processing	The provision of Jamf Services under the Agreement.
Duration of the processing	The Processing will continue until the termination of the Agreement.
Categories of Data Subjects whose personal data is transferred	Any user of the Services, including (but not limited to) employees, contractors, or students of Customer, as applicable.

Nature and purposes of the processing	We will Process the Personal Data provided to us by you as part of the provision of Services.

Frequency of the transfer (e.g., whether the data is transferred on a one-off or continuous basis):	The frequency of the transfer of Personal Data is directly related to the nature of Processing.
For transfers to (sub-) processors, also specify subject matter, nature, and duration of the Processing:	We use the Approved Sub-processors to provide Services to you, as set out in Schedule 2. The duration of the Processing is equivalent to the length of time you use our Services under the Agreement.
Type of Personal Data	**All Product Offerings** process the following: Names, user identifiers, device identifiers, IP addresses, telephone numbers, computer names, job titles and functions, general employment data, browser information, school enrollment information and email addresses. **AI Governance** may also process telemetry data. **Jamf Pro** may also process photos. **Jamf School** may also process photos and approximate location based on device IP address. **Manager for Android** may also process geolocation of devices. **RapidID** and **Seamless Learning** may also process parent contact information, password and authentication data, date of birth, and student ID numbers.
Sensitive data/special category data transferred (if any):	**Jamf Protect** may process domain name history of website traffic, through its Internet Content Filtering and Usage Controls features. **Jamf Safe Internet** (for optional "**Limited Privacy**" mode) may process domain name history of website traffic. **RapidID** may also process disability code, gender identity and pronouns. Whether special category data (as defined by applicable Data Protection Laws) is processed through the Product Offerings depends on your configuration and use of the Product Offerings. You are responsible for ensuring that your use of the Product Offerings, including any processing of special category data, complies with applicable Data Protection Laws.
Plan for return and destruction of the data once the processing is complete UNLESS requirement under union or member state law to preserve that type of data	Personal Data is retained for 90 days following termination of the Agreement and this DPA, after which it will be returned to you or deleted in accordance with Section 12 of this DPA.

C. Competent Supervisory Authority

Competent Supervisory Authority (identify the competent supervisory authority/ies in accordance with Clause 13 of the EEA Standard Contractual Clauses): The competent supervisory authority will be determined in accordance with Clause 13 (a) of the EEA Standard Contractual Clauses.

SCHEDULE 2
APPROVED SUB-PROCESSORS

Jamf's Sub-processor list can be found here:

https://www.jamf.com/trust-center/legal/jamf-sub-processors/

SCHEDULE 3
SECURITY MEASURES

We will take all reasonable measures required to ensure Processing of Personal Data is done in accordance with applicable Data Protection Laws and will have the required technical and organizational measures in place to ensure this. Considering the state of technological development and the cost of implementing such measures, we 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.

We will implement the following measures:

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

   a) Policies. We will document information security policies and senior management will approve them.

   b) Review of the Policies. We will review information security policies at least annually, or promptly after we make any material changes to them to confirm applicability and effectiveness. We will not make changes to the policies that would materially degrade our security obligations.

   c) Information Security Reviews. We will independently review our 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, we will maintain a disaster recovery ("**DR**") or high availability ("**HA**") solution and related plan that is consistent with industry standards for the Services we provide to you. We 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 we can restore installed systems used to provide Services in case of interruption;

      ii) that we can restore the availability and access to Customer Content in a timely manner if there is a physical or technical incident; and

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

   e) Testing. We will maintain a process for regularly testing the effectiveness of the technical and organizational measures for ensuring the security of the Processing of Customer Content.

2. **Information Security Framework.**

   a) Security Accountability. We 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 Responsibilities. We will have confidentiality agreements with our personnel, contractors and agents who provide Services under the Agreement.

   c) Risk Management. We 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. We will provide appropriate security awareness, education, and training to all our personnel and contractors with access to the Services we provide to you.

   b) Background Screening. We will perform background checks on our personnel who are part of teams managing our hosting infrastructure and on personnel or agents who will provide Services at your premises, if applicable. We will perform background checks in accordance with applicable law and our background screening policies and procedures. We will only permit individuals who have passed background checks to provide Services at your premises or manage our hosted infrastructure.

4. **Asset Management.**

a) Asset Inventory.

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

ii) We will classify Customer Content so that it is properly identified and will appropriately restrict access to Customer Content. Specifically, we will ensure that no person we appoint to Process Customer Content will do so unless that person:

1) has a need to access Customer Content for the purpose of performing our obligations under the Agreement;

2) has been authorized by us in a manner consistent with our information security policies;

3) has been fully instructed by us in the procedures relevant to the performance of our obligations under the Agreement, in particular the limited purpose of Processing Customer Content; and

4) is aware that they are prohibited from copying any Customer Content you transmit to us, provided, however, that we may retain copies of Customer Content in our servers for backup and archive purposes until completion of the Agreement.

iii) We will further maintain measures to ensure that the persons we appoint to Process Customer Content will prevent the unauthorized input of Customer Content and the unauthorized inspection, modification, or deletion of stored Customer Content.

iv) We will maintain an appropriate approval process whereby approval is provided to personnel, contractors, and agents prior to storing Customer Content on portable devices or remotely accessing Customer Content. All approvals will be subject to measures designed to prevent the unauthorized reading, copying, modification, or deletion of Customer Content during transfers of such content or during transportation of data media. If remote access is approved and granted, our 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. We agree to appropriately inventory all Software components (including open-source software) used with our Software and Services. We will assess whether any such software components have any security defects and/or vulnerabilities that could lead to unauthorized disclosure of Customer Content. We will perform such assessment prior to delivery of, or providing you access to, the Software and Services and on an ongoing basis thereafter during the term of the Agreement. We agree to remediate any security defect or vulnerability we detect in a timely manner.

5. **Access Control.**

a) Policy.

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

b) Authorization.

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

ii) We will maintain and update records of employees and contractors who are authorized to access systems that

are involved in providing Software and Services to you 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 our applicable technical and organizational measures.

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

iv) We will remove access rights of personnel and contractors to assets that store Customer Content upon termination of their employment, contract, or agreement within twenty-four (24) hours, or adjust access upon change of personnel role.

c) Authentication.

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

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

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

iv) We 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) We 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, OTP tokens, or biometrics.

d) Data-Processing Equipment.

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

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

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

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

6. **Cryptography**. We will maintain policies and standards regarding the use of cryptographic controls that we implement to protect Customer Content. Such protections will include the pseudonymization and encryption of Personal Data, as further detailed below in Section 8 (e) and 9 (a). We 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. We 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. We will use reasonable efforts, and, to the best of our ability and to the extent within our control, protect equipment from power failures and other disruptions caused by failures in supporting utilities.

c) Secure Disposal or Reuse of Equipment. We will verify that all Customer Content has been deleted or securely overwritten from equipment containing storage media using industry standard processes prior to disposal or reuse.

8. **Operations Security.**

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

b) Protections from Malware. We 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. We will have policies that govern the installation of software and utilities by personnel.

d) Change Management. We 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. We will deploy encryption solutions with no less than 256-bit Advanced Encryption Standard ("**AES**") encryption.

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

9. **Communications Security.**

a) Information Transfer.

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

ii) We will restrict access through encryption to Customer Content stored on media that is physically transported from our facilities.

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

b) Security of Network Services.

i) We 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) We will deploy intrusion detection or intrusion prevention systems for all systems used to provide Services to you 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) We 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. We will require hard disk encryption of at least 256-bit AES encryption on all workstations and/or laptops used by personnel, contractors, and agents where such personnel are Processing Customer Content.

b) Application Hardening.

i) We 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 our secure application development practices.

c) System Hardening.

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

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

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

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

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

11. **Jamf Relationships.**

a) If we must use a third-party application or service to provide the Services, our contract with that third-party vendor must clearly outline security requirements for the third-party vendor consistent with the security requirements of this Schedule 3. In addition, service level agreements with the third party must be clearly defined.

b) Any third-party gaining access to our 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 Schedule 3.

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