CHANNEL PARTNER DPA

This Channel Partner Data Processing Agreement ("**DPA**") is effective as of the date of the Agreement (the "**Effective Date**") and is made by and between **Jamf** and the **Channel Partner**, each a "**Party**" and collectively the "**Parties**."

1. **Subject Matter of this DPA**. This DPA applies when Data Protection Laws apply to Channel Partner's provision of Jamf's Product Offerings to Customers and Jamf Processes Personal Data on behalf of (a) a Reseller who is authorised by Jamf to provide certain services directly to the Customer; and/or (b) an MSP providing Managed Services. In both cases, Channel Partner is the Processor of Personal Data for Customers and Jamf is a Sub-processor of Channel Partner. This DPA constitutes an appendix to the Agreement. This DPA prevails over any conflicting terms in the Agreement with respect to the Processing of Customer Personal Data.

2. **Definitions.** The following defined terms are used in this DPA, together with other terms defined in the Agreement. Capitalized terms used but not defined in this DPA have the meanings given in the Agreement.

   a) "**Agreement**" means the Channel Partner Agreement entered into by and between Jamf and Channel Partner that governs the rights and obligations of the Parties under Jamf's Channel Partner Program.

   b) "**Controller**" means the Channel Partner's Customers whose Personal Data may be Processed by the Channel Partner.

   c) "**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 European Union ("**EU**") or 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California Privacy Rights Act of 2020 (collectively referred to as the "**CPRA**"), in each case as may be amended or superseded from time to time.

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

   e) "**ex-EEA Transfer**" means a Processing activity whereby Personal Data which is Processed in accordance with the GDPR is transferred from the Channel Partner 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.

   f) "**ex-Swiss Transfer**" means a Processing activity whereby Personal Data which is Processed in accordance with Swiss Data Protection Laws is transferred from the Channel Partner 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.

   g) "**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 Channel Partner 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.

   h) "**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.

   i) "**Personal Data**" means personal data as defined in applicable Data Protection Laws.

   j) "**Personal Data Breach**" means any known or reasonably suspected unauthorized access to, disclosure of Personal Data, and any loss, theft or unauthorized or unlawful acquisition or alteration of Personal Data, or any incident that compromises the security of Personal Data.

   k) "**Process**" or "**Processing**" means any operation or set of operations that is performed upon Personal Data or on sets of Personal Data, whether by automated 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.

l) "**Processor**" means the Channel Partner, who may Process its Customers' Personal Data in the provision of Managed Services to its Customers or certain Jamf authorized support services relating to the Product Offerings provided directly by a Channel Partner acting as a Reseller.

m) "**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.

n) "**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.

o) "**Sub-processor**" means Jamf, who may Process the Personal Data of the Channel Partner's Customers as part of Jamf's role in providing Product Offerings to the Channel Partner pursuant to the Agreement.

p) "**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).

q) **"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 Product Offerings to Channel Partner, if the CPRA applies to any Personal Data received by Jamf from or on behalf of the Channel Partner, then:

a) Channel Partner agrees it is disclosing such Personal Data to Jamf only for the limited and specified business purposes set forth under the Agreement;

b) Jamf 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 Jamf will not retain, use, or disclose such Personal Data (i) for any purpose other than to provide the Product Offerings or (ii) outside of the direct business relationship between the Channel Partner and Jamf, unless expressly permitted by the CPRA;

c) 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 behavioral advertising (as defined by the CPRA), whether or not for monetary or other valuable consideration;

d) 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 subprocess Personal Data as necessary for Jamf to provide the Product Offerings to the Channel Partner; provided that Jamf notifies the Channel Partner 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 the CPRA. Section 6 of this DPA sets forth Jamf's compliance with California Civil Code § 1798.140 (ag) (2);

e) Jamf may not combine or update Personal Data provided by the Channel Partner with Personal Data Jamf receives from other entities or persons, or collects from Jamf's 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 forth in California Civil Code § 1798.140 (m). If the Channel Partner makes deidentified

information available to Jamf in connect 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 CPRA; and (iii) contractually obligate any recipients of the information to comply with all provision of California Civil Code § 1798.140 (m);

g) In accordance with Section 9 below, Jamf confirms that it has implemented reasonable security procedures and practices designed to protect Personal Data from unauthorized or illegal access, destruction, modification, or disclosure;

h) As provided for in Section 10 below, Jamf grants the Channel Partner the right to take reasonable and appropriate steps to stop and remediate the unauthorized use of Personal Data, and pursuant to Sections 11 and 12 below, Jamf grants the Channel Partner the right to take reasonable and appropriate steps to help ensure that Jamf uses Personal Data transferred to Jamf in a manner consistent with the Channel Partner's obligations under CPRA; and

i) Jamf will notify the Channel Partner if Jamf determines that it can no longer meet its obligations under the CPRA and grants the Channel Partner the right, upon notice by the Channel Partner, to take reasonable and appropriate steps to stop providing Personal Data to Jamf.

4. **Engagement of Sub-processors.**

a) The Channel Partner has entered into contracts with its Customers by which the Channel Partner may Process Personal Data on behalf of its Customers who are the Controllers of such Personal Data.

b) The Channel Partner represents and warrants that the Channel Partner's Customers have, in their capacity as Controllers of Personal Data, by a general or specific written authorization, approved the engagement of Jamf to perform specific Processing activities. The Channel Partner has engaged Jamf, as Sub-processor, for carrying out specific Processing activities on behalf of the Channel Partner's Customers (Controllers).

c) The Channel Partner's Customers are, in their capacity as Controllers of Personal Data, responsible for Personal Data being processed under this DPA in accordance with applicable Data Protection Laws. The Channel Partner is responsible for ensuring that Jamf, as Sub-processor, does not Process any categories of Personal Data other than those specified in Schedule 1 and to the extent specified therein.

5. **Processing of Personal Data.**

a) Jamf's Processing of Personal Data. Jamf will Process Personal Data in accordance with the requirements of Data Protection Laws and only upon the Controller(s)' documented instructions, except where Processing is otherwise permitted by Data Protection Laws. Where Processing is otherwise permitted, Jamf will inform the Channel Partner about this obligation before the Processing begins if permissible under applicable Data Protection Laws. Channel Partner will thereafter inform the Controller(s) about this obligation. Channel Partner represents and warrants that this DPA constitutes the Controller(s)' complete instructions for the processing of Personal Data under this DPA, except for any written instructions that the Controller(s) are obliged to provide during the term of the Agreement to comply with applicable Data Protection Laws. Channel Partner is responsible for ensuring that the Controller(s)' complete instructions are set out in this DPA and that the Controller(s)' complete instructions are provided to Jamf. Jamf will inform the Channel Partner if it becomes aware that such Processing instructions infringe applicable Data Protection Laws, but without obligation to actively monitor the Channel Partner's or its Controller's compliance with applicable Data Protection Laws.

b) EEA Transfers of Personal Data. The Parties agree that when the transfer of Personal Data from Channel Partner (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 Three 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 6 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.

c) UK Transfers of Personal Data. The Parties agree that when the transfer of Personal Data from the Channel Partner (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 5 b) of this DPA will also apply to transfers of such Personal Data, subject to sub-clause 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.

d) Transfers of Swiss Personal Data. The Parties agree that when the transfer of Personal Data from the Channel Partner (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 5 b) of this DPA, will also apply to transfers of such 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).

e) Further Assurance. If Data Protection Law requires Channel Partner to execute the EEA Standard Contractual Clauses, UK Addendum and/or Swiss Standard Contractual Clauses applicable to a particular transfer of Personal Data to Jamf as a separate agreement, Jamf will, on Channel Partner's request, promptly execute such EEA Standard Contractual Clauses, UK Addendum and/or Swiss Standard Contractual Clauses incorporating such amendments as may reasonably be required by the Channel Partner to reflect the applicable clauses and Schedules of this DPA, the details of the transfer, and the requirements of the relevant Data Protection Laws. 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 the Channel Partner, with effect from the date set out in such notice, amend, or put in place alternative arrangements in respect of such transfers, as required by the relevant Data Protection Laws.

f) Supplementary Measures. In respect of any Restricted Transfer, the following applies:

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 Channel Partner in writing as soon as reasonably practicable and the Channel Partner (and the relevant Controller) 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 Channel Partner 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 applicable Data Protection Laws; and

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

6. **Jamf's Sub-processors.**

a) Approved Sub-processors. Jamf will be entitled to engage sub-processors for the processing of Personal Data under this DPA. The Channel Partner, on behalf of its Customers (the Controller(s)), authorizes the Processing of Personal Data by the sub-processors listed in Schedule 2 (*Approved Sub-processors*). Jamf will notify the Channel Partner of any changes concerning the addition or replacement of other sub-processors, thereby giving the Channel Partner the opportunity to object to such changes. If, within 30 business days of receipt of this notice, the Channel Partner has not objected to the intended change, the Channel Partner is deemed to have authorized the intended change. The Channel Partner is responsible for ensuring that the Controller(s) have authorized any sub-processor changes hereunder.

b) Contract with Sub-processors. 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 based on this DPA. Jamf will remain responsible for complying with the obligations of this DPA and for any acts or omissions of its sub-processors that cause Jamf to breach any of Jamf's obligations under this DPA.

7. **Disclosure of Personal Data.**

a) Nondisclosure of Personal Data. Jamf will not disclose or otherwise reveal any Personal Data covered by this DPA to a Data Subject or third party, unless otherwise stated in the Agreement or as required by Data Protection Laws or a court or official authority's decision. If Jamf must disclose such Personal Data due to Data Protection Laws or a court or official authority's decision, Jamf will notify the Channel Partner of the disclosure, unless prohibited by Data Protection Laws or a court or official authority's decision.

b) Data Subject Requests. Jamf will notify the Channel Partner without undue delay about any inquiries from a Data Subject, a data protection authority, or another supervisory authority that refer specifically to the Processing of Personal Data under this DPA, and refer such Data Subject, data protection authority or other supervisory authority to the Channel Partner. Jamf will be entitled to reasonable compensation from the Channel Partner for any requested cooperation that refers specifically to the Processing of Personal Data Processed under this DPA that is not a consequence of Jamf being in breach of its obligations under this DPA.

c) The Channel Partner is responsible for informing the Controller(s) about any notification from Jamf under this Section 7.

8. **Jamf Personnel.**

a) Confidentiality. Jamf will ensure that its personnel engaged in the Processing of Personal Data under this DPA 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 those personnel performing services in the provision of Product Offerings.

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

9. **Security.** Jamf has implemented and will maintain technical and organizational measures designed to secure the 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. The Channel Partner is responsible for ensuring that the security measures referenced in this Section 9 and Schedule 3 comply with the Controller(s) data security obligations pursuant to the applicable Data Protection Laws as regards the Personal Data Processed.

10. **Personal Data Breach Management and Notification.** Jamf maintains security incident management policies and procedures and will notify the Channel Partner 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. The Channel Partner is responsible for notifying the Controller(s) of the Personal Data Breach in accordance with applicable Data Protection Laws.

11. **Obligation to Assist the Channel Partner and Controller.** Jamf will, in addition to Section 9 (Security), implement appropriate technical and organizational measures to, upon the Channel Partner's written request, assist the Controller(s) in fulfilling the Controller(s)' obligation to respond to the requests for exercising the Data Subject's rights under applicable Data Protection Laws. Jamf will only be required to perform its obligations as set forth in this Section 11 insofar as it is possible and to the extent the nature of the Processing requires it.

    a) Taking into account the nature of Processing and the information available to Jamf, Jamf will also be obliged, at the written request of the Channel Partner, to assist the Controller(s) in ensuring compliance with the Controller(s)' obligations in respect of security for Processing, Personal Data Breaches, data protection impact assessments and prior consultation in accordance with applicable Data Protection Laws.

    b) Unless otherwise agreed in writing, Jamf will be entitled to reasonable compensation for Jamf's assistance to Controller(s) in accordance with this Section 11.

12. **Audits.** Jamf will make available to the Channel Partner and/or a Controller all reasonable information necessary to demonstrate compliance with applicable Data Protection Laws' requirements on processors, and allow for, cooperate with, and contribute to audits, including inspections, conducted by a Controller or an external auditor engaged by a Controller. However, an inspection may only be conducted if an audit cannot, according to Data Protection Laws, be met by Jamf providing information only. 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 provision of Software and/or performance of the Product Offerings under the Agreement or with Jamf's business generally, and (iii) during the term of this DPA. The notice requirement in this section 12(i) and the restrictions stated in 12(ii) will not apply to the extent the audit is initiated by a regulator. Jamf will provide to the Channel Partner and/or a Controller and their auditors and regulators reasonable assistance as they require for the purpose of performing an audit. As a precondition to an audit, the Channel Partner and/or a Controller or their auditor must enter necessary confidentiality undertakings and comply with Jamf's applicable security regulations. Jamf will not be required to give the Channel Partner and Controllers or their 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). All information provided by Jamf in relation to an audit will be Jamf Confidential Information (as defined in the Agreement). Jamf may charge the Channel Partner for any reasonable costs incurred in conjunction with an audit.

13. **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 the Channel Partner. The Channel Partner is responsible for immediately notifying Jamf when the agreement between the Channel Partner and a Controller has terminated and the Personal Data Jamf is Processing on such Controller's behalf will be deleted by Jamf subject to Section 13 b) below.

    b) Obligation to Delete or Return Personal Data.

        i) Upon termination or expiration of the agreement between the Channel Partner and a Controller, Jamf will at the Channel Partner's request, that will be made no later than 20 days after the termination of the agreement between the Channel Partner and a Controller, and, at the option of the Channel Partner,

delete or promptly return all Personal Data to the Channel Partner or a party nominated by the Channel Partner.

ii) Upon termination or expiration of the Agreement and this DPA, and, at the choice of and upon the Channel Partner's written request, Jamf will return the Personal Data and all copies thereof to the Channel Partner and/or will securely destroy (delete) such Personal Data and all existing copies thereof 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 Channel Partner of such legal obligation, will keep the Personal Data confidential and will only Process the Personal Data if required by the applicable laws.

iii) The Channel Partner is responsible for ensuring that its requests to Jamf under this Section 13 b) are made in accordance with the Controller's instructions. It will be the Channel Partner's obligation to ensure that it complies with its obligations to its Controllers in respect of this DPA, specifically including this Section 13 b).

14. **Limitation of Liability**. **NEITHER JAMF NOR ANY OF JAMF'S AFFILIATES OR LICENSORS WILL BE RESPONSIBLE 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' AGGREGATE LIABILITY UNDER THIS DPA WILL NOT EXCEED THE AMOUNT THE CHANNEL PARTNER ACTUALLY PAYS JAMF UNDER THE AGREEMENT FOR THE PRODUCT OFFERING THAT GAVE RISE TO THE CLAIM DURING THE TWELVE (12) MONTHS BEFORE THE LIABILITY AROSE. THE EXCLUSIONS AND LIMITATIONS IN THIS SECTION 14 APPLY ONLY TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW**.

15. **Third-Party Rights.** Except if expressly provided by 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.

16. **General Terms.**

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. In the case of any conflict or inconsistencies between the terms of this DPA and the EEA Standard Contractual Clauses (for ex-EEA Transfers), Swiss Standard Contractual Clauses (for ex-Swiss Transfers) or UK Addendum (for ex-UK Transfers) the EEA Standard Contractual Clauses, Swiss Standard Contractual Clauses or UK Addendum will control (as applicable).

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 DSPA 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 of 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.

SCHEDULE 1
DETAILS OF PROCESSING

A. LIST OF PARTIES

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 Product Offerings provided by Jamf.

Signature and date: _____

Role (controller/processor): Processor (on behalf of the Channel Partner's Customer as the Controller)
Data importer(s): [Identity and contact details of the data importer(s), including any contact person with responsibility for data protection]

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 Product Offerings under the Agreement.

Signature and date: _____

Role (controller/processor): Sub-processor

B. Description of Transfer

Categories of Data Subjects whose Personal Data is transferred: employees of the Channel Partners Customers (and students of the Channel Partner's Customers, if Customer is an education 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 the Channel Partner enters Customer's Personal Data into Customer's instance of the Hosted Services provided by Jamf to Channel Partner 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 the Channel Partner to utilize Jamf's Product Offerings to provide Managed Services or authorized Reseller services to the Channel Partner's Customers.

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 Schedule 2. The duration of the Processing is equivalent to the length of time the Channel Partner utilizes Jamf's Product Offerings on behalf of its Customers 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, is based on the where the Channel Partner is established and will be either 13 (a) (i), (ii), or (iii), whichever is applicable to the Channel Partner (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 the Channel Partner 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 Product Offerings 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 Product Offerings will be restored in case of interruption;

        ii) Jamf's ability to restore the availability and access to Customer Content 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 Product Offerings.

    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 Content.

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 Product Offerings 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 Product Offerings 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 professional 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 professional 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 Content 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 Content so that it is properly identified and will appropriately restrict access to Customer Content. Specifically, Jamf will ensure that no person appointed by Jamf to process Customer Content, will process Customer Content unless that person:

1) has a need to access Customer Content 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 Content; and

4) is aware that they are prohibited from copying any Customer Content transmitted by Customer to Jamf, provided, however, that Jamf may retain copies of Customer Content 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 Content will prevent the unauthorized input of Customer Content and the unauthorized inspection, modification, or deletion of stored Customer Content.

iv) Jamf 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, 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 Product Offerings. Jamf will assess whether any such software components have any security defects and/or vulnerabilities that could lead to unauthorized disclosure of Customer Content. Jamf will perform such assessment prior to delivery of, or providing Customer access to, Jamf's Product Offerings 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 Content 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 Product Offerings, 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 Content and all Jamf internal applications while providing Product Offerings 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 Product Offerings 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, agents, and contractors to assets that store Customer Content 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 Content ("**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 Content covered by their access authorization.

iv) Jamf 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.** Jamf will maintain policies and standards regarding the use of cryptographic controls that are implemented to protect Customer Content. 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 Hosted 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 Content 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 Product Offerings 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 Jamf's Hosted Services, Customer Content is encrypted in-transit to the Hosted Services and maintained in encrypted storage. Jamf will use industry standard encryption to encrypt Customer Content.

ii) Jamf will restrict access through encryption to Customer Content 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 Content 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 Product Offerings 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 Product Offerings 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 Content.

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 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 Product Offerings monthly and external environment related to the Product Offerings 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 Product Offerings 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 Product Offerings, 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 Schedule 3 (Security Measures). 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 Schedule 3 (Security Measures).

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