

Data Sharing/Use Agreement
Between
Jefferson County Board of Education
And
Jamf Software, LLC

This Data Sharing/Use Agreement ("Agreement") between the Jefferson County Board of Education, a political subdivision of the Commonwealth of Kentucky doing business as the Jefferson County Public Schools ("JCPS"), and Jamf Software, LLC, a limited liability company organized under the laws of Minnesota. ("Services Provider") describes the services to be provided to JCPS by Services Provider, and the means to be used by Services Provider to ensure the confidentiality and security of information and data exchanged between JCPS and Services Provider in connection with the provision of the services.

A. PERIOD OF THE AGREEMENT

This Agreement shall be effective as of June 24, 2020 and will terminate when the services contract referenced in Paragraph B.1. below terminates, unless terminated earlier by either party pursuant to Section H.

B. SCOPE OF THE AGREEMENT AND INTENDED USE OF THE DATA

1. Services Provider will provide the following services to JCPS under the terms of the Software License and Services Agreement ("Services Agreement") attached as Attachment B and previously accepted by JCPS effective as of June 24, 2020. Under the Services Agreement, JCPS purchased hosted software and services from Jamf including Jamf Pro and Jumpstart for Jamf Pro.
2. JCPS and Services Provider agree that Services Provider is an organization to which JCPS can disclose, personally identifiable information from an education record of a student, as defined in 34 CFR 99.3, under the "school official exception" of the Family Educational Rights and Privacy Act, 20 U.S.C. 1232(g) and 34 C.F.R. 99.31 (a)(1) ("FERPA"), because the disclosure is to a contractor to whom JCPS has outsourced institutional services or functions for which JCPS would otherwise use employees; the contractor is under the direct control of JCPS with respect to the use and maintenance of education records; and the contractor is subject to the requirements of 34 CFR 99.33(a) governing the use and redisclosure of personally identifiable information from education records.
3. JCPS shall disclose to Services Provider, confidential, personally identifiable information from an education record of a student, as defined in 34 C.F.R. 99.3, under the "school official exception" of FERPA, 34 C.F.R. 99.31 (a)(1), when the disclosure is within such exception as stated in Paragraph B.2 above and Services Provider has a legitimate educational interest for access to such education records. The confidential data, including student and non-student information to be disclosed, is described in a

document attached to this agreement as **Attachment A**. Services Provider shall use personally identifiable information from education records and other records in order to perform the services described in the Services Agreement. JCPS shall notify Service Provider and JCPS shall provide written consent, if approved, of any changes to the list of disclosed data necessary for the services. Service Provider will provide notice to JCPS of any changes to the services themselves. Any agreed upon changes to the data disclosed shall be reduced to writing and included in an update to Attachment A to this Agreement. Any agreed upon changes to the scope, purpose or duration of the services shall be reduced to writing and included in an amendment to the Services Agreement.

4. The confidential Data provided by JCPS will be transferred in accordance with the Services Agreement and the Information Security Schedule attached as Attachment C.

C. CONSTRAINTS ON USE OF DATA

1. Services Provider agrees that the services shall be provided in a manner that does not permit personal identification of parents and students by individuals other than representatives of Services Provider that have legitimate interests in the information.
2. Services Provider will not contact the individuals included in the data sets without obtaining advance written authorization from JCPS.
3. Services Provider shall not re-disclose any individual-level data with or without identifying information to any other requesting individuals, agencies, or organizations without prior written authorization by JCPS.
4. Services Provider shall use the data only for the purpose described in Paragraph B.1 above. The data shall not be used for personal gain or profit.

D. DATA CONFIDENTIALITY AND DATA SECURITY

Services Provider agrees to the following confidentiality and data security statements:

1. Services Provider acknowledges that the data is confidential data and proprietary to JCPS, and agrees to protect the data from unauthorized disclosures and to comply with all applicable Local, State and Federal confidentiality laws and regulations including but not limited to FERPA; the Kentucky Family Educational Rights and Privacy Act, KRS 160.700 et seq.; the Richard B. Russell National School Lunch Act, 42 U.S.C. 1751 et seq.; the Child Nutrition Act of 1966, 42 U.S.C. 1771 et seq.; 7 C.F.R. 245.6 et seq.; the Personal Information Security and Breach Investigation Procedures and Practices Act, KRS 61.931 et seq.; and the Kentucky Open Records Act, KRS 61.820 et seq.
2. If the performance of this Agreement involves the transfer by JCPS to Services Provider of any data regarding any JCPS student that is subject to FERPA, Services Provider agrees to:
 - a. In all respects comply with the provisions of FERPA.
 - b. Use any such data for no purpose other than to fulfill the purposes of the Services Agreement, and not share any such data with any person or entity other

than Services Provider and its employees, contractors and agents, without the prior written approval of JCPS.

- c. Require all employees, contractors and agents of Services Provider to comply with all applicable provisions of FERPA with respect to any such data.
 - d. Maintain any such data in a secure computer environment, and not copy, reproduce or transmit any such data except as necessary to fulfill the purposes of the Services Agreement.
 - e. Provide the services under the Services Agreement in a manner that does not permit the identification of an individual student by anyone other than employees, contractors or agents of Services Provider having a legitimate interest in knowing such personal identification.
 - f. Destroy or return to JCPS any such data obtained under this Agreement within thirty days (30) after the date within it is no longer needed by Services Provider for the purposes of the Services Agreement.
3. Services Provider shall not release or otherwise reveal, directly or indirectly, the data to any individual, agency, entity, or third party not included in this Agreement, unless such disclosure is required by law or court order. If Services Provider becomes legally compelled to disclose any confidential and otherwise personally identifiable data (whether by judicial or administrative order, applicable law, rule or regulation, or otherwise), then Services Provider shall use all reasonable efforts to provide JCPS with prior notice before disclosure so that JCPS may seek a protective order or other appropriate remedy to prevent the disclosure or to ensure JCPS's compliance with the confidentiality requirements of federal or state law; provided, however, that Services Provider will use all reasonable efforts to maintain the confidentiality of confidential and otherwise personally identifiable data. If a protective order or other remedy is not obtained prior to the deadline by which any legally compelled disclosure is required, Services Provider will only disclose that portion of confidential and otherwise personally identifiable data that Services Provider is legally required to disclose.
4. Services Provider shall not distribute, reprint, alter, sell, assign, edit, modify or create derivative works or any ancillary materials from or with the data except as permitted by the Services Agreement with respect to data that has been de-identified, anonymized and aggregated.
5. Services Provider shall not use data shared under this Agreement for any purpose other than the Services Agreement. Nothing in this Agreement shall be construed to authorize Services Provider to have access to additional data from JCPS that is not included in the scope of this Agreement (or addenda). Services Provider understands that this Agreement does not convey ownership of the data to Services Provider.
6. Services Provider shall take reasonable security precautions and protections to ensure that persons not authorized to view the data do not gain access to the data. Reasonable security precautions and protections include those included in the Information Security Schedule attached as Attachment C.

7. If Services Provider receives Personal Information as defined by and in accordance with the Kentucky Personal Information Security and Breach Investigation Procedures and Practices Act, KRS 61.931, et seq. (the "Act"), Services Provider shall secure, protect and maintain the confidentiality of the Personal Information by, without limitation, complying with all requirements applicable to "non-affiliated third parties" set forth in the Act, including but not limited to the following:
 - a. "Personal Information" is defined in accordance with KRS 61.931(6) as an individual's first name or first initial and last name; personal mark; or unique biometric or genetic print or image, in combination with one (1) or more of the following data elements:
 - i. An account, credit card number, or debit card number that, in combination with any required security code, access code or password, would permit access to an account;
 - ii. A Social Security number;
 - iii. A taxpayer identification number that incorporates a Social Security number;
 - iv. A driver's license number, state identification card number or other individual identification number issued by an agency;
 - v. A passport number or other identification number issued by the United States government; or
 - vi. Individually Identifiable Information as defined in 45 C.F.R. sec. 160.013 (of the Health Insurance Portability and Accountability Act), except for education records covered by FERPA.
 - b. As provided in KRS 61.931(5), a "non-affiliated third party" means any person or entity that has a contract or agreement with an agency and receives (accesses, collects or maintains) personal information from the agency pursuant to the contract or agreement.
 - c. Services Provider shall not re-disclose, without the written consent of JCPS, any "personal information," as defined in KRS 61.931, or any other personally identifiable information of a student or other persons, such as employees.
 - d. Services Provider agrees to cooperate with JCPS in complying with the response, mitigation, correction, investigation, and notification requirements of the Act.
 - e. Services Provider agrees to undertake a prompt and reasonable investigation of any breach as required by KRS 61.933.
8. If Services Provider is a cloud computing service provider (as defined in KRS 365.734(1)(b) as "any person other than an educational institution that operates a cloud computing service"), Services Provider agrees that:

- a. Services Provider shall not process student data for any purpose other than providing, improving, developing, or maintaining the integrity of its cloud computing services, as set forth in the Services Agreement unless the provider receives express permission from the student's parent. Services Provider shall work with the student's school and district to determine the best method of collecting parental permission. KRS 365.734 defines "process" and "student data."
 - b. Pursuant to KRS 365.734(2), Services Provider shall not in any case process student data to advertise or facilitate advertising or to create or correct an individual or household profile for any advertisement purposes.
 - c. Pursuant to KRS 365.734(2), Services Provider shall not sell, disclose, or otherwise process student data for any commercial purpose.
 - d. Pursuant to KRS 365.734(3), Services Provider shall certify in writing to the agency that it will comply with KRS 365.734(2).
9. Services Provider shall report all known or suspected breaches of the data, in any format, to Dr. Kermit Belcher, Chief Information Officer in accordance with the Information Security Schedule attached as Attachment C. The report shall include (1) the name, job title, and contact information of the person reporting the incident; (2) the name, job title, and contact information of the person who discovered the incident; (3) the date and time the incident was discovered; (4) the nature of the incident (e.g. system level electronic breach, an electronic breach of one computer or device, a breach of hard copies of records, etc.); (5) a description of the information lost or compromised; (6) the name of the electronic system and possible interconnectivity with other systems; (7) the storage medium from which information was lost or compromised; (8) the controls in place to prevent unauthorized use of the lost or compromised information; (9) the number of individuals potentially affected; and (10) whether law enforcement was contacted.
10. Services Provider shall securely and permanently destroy the data, and any and all hard and soft (electronic) copies thereof, upon the termination of this Agreement. Services Provider agrees to require all employees, contractors, or agents of any kind using JCPS data to comply with this provision. Services Provider agrees to document the methods used to destroy the data, and upon request, provide certification to JCPS that the data has been destroyed.
11. For purposes of this agreement and ensuring Services Provider's compliance with the terms of this Agreement and all application of the state and Federal laws, Services Provider designates Aaron Kiemele (or an alternative designee specified in writing) as the temporary custodian ("Temporary Custodian") of the data that JCPS shares with Services Provider. JCPS will release all data and information under this Agreement to Temporary Custodian. Temporary Custodian shall be responsible for performing the services as described in the Services Agreement in accordance with the Information Security Schedule attached as Attachment C.
12. Services Provider acknowledges that any violation of this Agreement and/or the provisions of FERPA or accompanying regulations related to the nondisclosure of

protected student information constitutes just cause for JCPS to immediately terminate this Agreement.

13. Services Provider shall maintain, during the term of this Agreement, a cyber-insurance liability policy, in the amount of \$5M. Upon request, Services Provider shall furnish the certificate of insurance evidencing this coverage. The certificate of insurance shall name the Board of Education of Jefferson County as additional insured in the Description of Operations section of the Certificate of Insurance which shall read:

Board of Education of Jefferson County
Attn: Insurance/Real Estate Dept.
3332 Newburg Road
Louisville, Kentucky 40218

14. Services provider shall maintain, during the term of this Agreement, ISO27001 or SOC2 certification. If Services Provider is unable to provide ISO27001 or SOC2 certification, minimum requirements on a JCPS-provided standardized questionnaire must be met. Upon request, Services Provider shall furnish a current ISO27001, SOC2 certification, or updated questionnaire.

E. FINANCIAL COSTS OF DATA-SHARING

Each party shall be responsible for their portion of costs that may result from data sharing. Examples of potential costs to JCPS are costs associated with the compiling of student data requested under this agreement and costs associated with the electronic delivery of the student data to Services Provider.

No payments will be made under this Agreement by either party. Any payments to Services Provider will be made under the Services Agreement.

F. OBLIGATIONS OF JCPS

During the term of this Agreement, JCPS shall:

1. Prepare and deliver the data described in **Attachment A**.

G. LIABILITY

Services Provider agrees to be responsible for and assumes liability for any claims, costs, damages or expenses (including reasonable attorneys' fees) that may arise from or relate to Services Provider's intentional or negligent release of personally identifiable student, parent or staff data ("Claim" or "Claims") up to and not to exceed three times the amount of money paid under the Services Agreement. Services Provider agrees to hold harmless JCPS and pay costs incurred by JCPS in connection with any Claim up to and not to exceed three times the amount of money paid under the Services Agreement. The provisions of this Section shall survive the termination or expiration of this Agreement.

H. TERMINATION

1. This Agreement may be terminated as follows, after notification via the United States Postal Service (certified mail or registered mail) or recognized overnight delivery service (e.g., UPS, DHL, or FedEx):
 - a. By either party in the event of a material breach of this Agreement by another party provided however, the breaching party shall have thirty (30) days to cure such breach and this Agreement shall remain in force.
 - b. By either party after thirty (30) days advance written notice to the other party, for any reason or no reason.
2. The confidentiality provisions of this Agreement shall survive the termination of this Agreement. If this Agreement is terminated by either party for material breach or for any other reason with thirty (30) days written notice, within seven (7) days of the termination the confidential information shall be returned or destroyed within seven (7) days of the termination and the Temporary Custodian shall provide JCPS confirmation of the return or destruction of the data pursuant to Paragraph D.11. If this Agreement terminates at the end of the term described in Section A, within seven (7) days after the end of the term, Services Provider shall return or destroy all confidential information and the Temporary Custodian shall provide JCPS confirmation of the return or destruction of the data pursuant to Paragraph D.11.
3. Destruction of the confidential information shall be accomplished by utilizing an approved method of confidential destruction, including but not limited to shredding, burning or certified/witnessed destruction for physical materials and verified erasure of magnetic media using approved methods of electronic file destruction.

I. PUBLICATIONS AND COPYRIGHTS

Both parties recognize that each organization may have extant work that predates this agreement. If those materials and/or data are used in the course of this work, they remain the property of the original developer. If new materials are developed during the term of the Services Agreement, ownership and copyright of such will be governed by the terms of the services contract.

J. MODIFICATION

No waiver, alteration or modification of the provisions of this Agreement shall be binding unless in writing and mutually agreed upon. Any modifications or additions to this Agreement must be negotiated and approved by both parties.

K. QUALITY OF SERVICES

JCPS reserves the right to review Services Provider's performance under this Agreement for effectiveness in serving the specific purposes as outlined in Paragraph B.1.

L. BREACH OF DATA CONFIDENTIALITY

Services Provider acknowledges that the breach of this agreement or its part may result in irreparable and continuing damage to JCPS for which money damages may not provide adequate relief. In the event of a breach or threatened breach of this agreement by Services

Provider, JCPS, in addition to any other rights and remedies available to JCPS at law or in equity, may be entitled to preliminary and permanent injunctions to enjoin and restrain the breach or threatened breach. If the United States Department of Education's Family Policy Compliance Office determines that Services Provider has violated paragraph 34 C.F.R. 99.31(a)(6)(iii)(B), JCPS may not allow Services Provider access to personally identifiable information from its education records for at least five (5) years.

M. CHOICE OF LAW AND FORUM

This Agreement shall be governed and construed in accordance with the laws of the Commonwealth of Kentucky. Any action or Claim arising from, under or pursuant to this Agreement shall be brought in the Jefferson County, Kentucky, Circuit Court, and the parties expressly waive the right to bring any legal action or Claims in any other courts.

N. WAIVER

No delay or omission by either party in exercising any right under this Agreement shall operate as a waiver of that or any other right or prevent a similar subsequent act from constituting a violation of this Agreement.

O. SEVERABILITY

If any part of this Agreement is held to be void, against public policy or illegal, the balance remaining provisions of this Agreement shall continue to be valid and binding.

P. NOTICES

Any notices or reports by one party to the other party under this Agreement shall be made in writing, to the address shown in the signature portions of this Agreement, or to such other address as may be designated in writing by one party to the other. Notices shall be effective when received if personally delivered, or three days after mailing if mailed.

Q. RELATIONSHIP OF PARTIES

JCPS is not an employee, agent, partner or co-venturer of or with Services Provider. Neither Services Provider nor JCPS shall represent or imply to any party that it has the power or authority to enter into a contract or commitment in the name of or on behalf of the other, or to otherwise bind the other.

R. ENTIRE AGREEMENT; ASSIGNMENT

This Agreement, together with any attachments hereto and any amendment or modifications that may hereafter be agreed to, constitute the entire understanding between the parties with respect to the subject-matter hereof and supersede any and all prior understandings and agreements, oral and written, relating hereto. Services Provider shall not assign this Agreement or any portion thereof to a subcontractor or other third party without the prior written consent of JCPS, and any attempted assignment without such prior written consent in violation of this Section R shall automatically terminate this Agreement.

AGREED:

Jamf Software, LLC
100 Washington Avenue South, Suite 100
Minneapolis, MN 55401

BY: 

Name: Shawn Abbas

Title: VP Financial Planning & Analysis

Date: June 1, 2020

AGREED:

Jefferson County Board of Education
3332 Newburg Road
Louisville KY 40218

BY: _____

Name: Dr. Martin Pollio

Title: Superintendent, JCPS

Date: _____

Attachment A

CONFIDENTIAL INFORMATION TO BE DISCLOSED

Student UserID

Student Email Address

Attachment B

SOFTWARE LICENSE AND SERVICES AGREEMENT

JAMF SOFTWARE, LLC, ("JAMF") PROVIDES ACCESS TO ITS SOFTWARE AND SERVICES SUBJECT TO THE TERMS AND CONDITIONS SET FORTH IN THIS SOFTWARE LICENSE AND SERVICES AGREEMENT, ALONG WITH ANY SUBSEQUENT AMENDMENTS OR ORDERS, (THE "AGREEMENT"). PLEASE READ THE TERMS OF THIS AGREEMENT CAREFULLY. AS USED IN THIS AGREEMENT, "CUSTOMER" REFERS TO THE PERSON OR ENTITY USING THE SOFTWARE OR RECEIVING THE SERVICES. BY USING THE SOFTWARE OR THE SERVICES, THE CUSTOMER AGREES TO BE BOUND BY THE TERMS OF THIS AGREEMENT. IF YOU DO NOT AGREE TO THE TERMS OF THIS AGREEMENT, RETURN THE SOFTWARE TO JAMF FOR A REFUND.

The "Effective Date" of this Agreement is the date the Customer accepts this Agreement as provided below. As used in this Agreement, Jamf and Customer are each a "Party" and are collectively the "Parties".

1. **Overview.** This Agreement is a master agreement under which Customer may license or access Jamf's Software and obtain Services (all as defined herein) requested by Customer in an applicable Order. This Agreement shall be implemented through one or more Orders that set forth the Software to be licensed by Customer and other Services purchased.
2. **Definitions.** The following defined terms are used in this Agreement, together with other terms defined herein.
 - a) **"Affiliate"** means any entity which is owned more than 50% by a Party, over which a Party exercises management control, which is under common control with a Part or which owns more than 50% of a Party's voting securities.
 - b) **"Components"** are optional plug-ins that add specific features to the Software to enable additional functionality or optional connectors used to connect third-party systems to the Software at the application programming interface level ("API") and may be provided to Customer by Jamf and/or subject to additional fees or terms.
 - c) **"Customer Content"** means any and all information entered by Customer into the Software that relates to Customer's use of the Software. Customer Content may include Personal Information. Customer Content does not include any third-party software Customer deploys in connection with its use of the Hosted Services ("**Third-party Content**").
 - d) **"Data Protection Laws"** means applicable domestic and foreign laws, rules, directives and regulations, on any local, provincial, state, federal or national level, pertaining to data privacy, data security and/or the protection of Personal Information in effect as of the date of this Agreement, including but not limited to, Regulation (EU) 2016/679, General Data Protection Regulation ("**GDPR**").
 - e) **"Device"** means an Apple iOS, macOS or tvOS device.
 - f) **"Documentation"** means Jamf's definitive technical specifications and user guides, in any form, that explain the capabilities of the Software and instructions for using the Software as updated from time to time found at <http://docs.jamf.com>.
 - g) **"Hosted Services"** means Customer's access to an instance of certain Software on a software as a service basis, located in selected regional data centers and made available for Customer's use.
 - h) **"Intellectual Property Rights"** means unpatented inventions, patent applications, patents, design rights, copyrights, trademarks, service marks, trade names, domain name rights, know-how and other trade secret rights, and all other intellectual property rights, derivatives thereof, and forms of protection of a similar nature anywhere in the world.
 - i) **"JumpStart"** means onsite or remote services during which a Jamf certified engineer assists Customer with the installation and/or configuration of the Software and instruction on the use of the Software and/or Hosted Services.
 - j) **"On-Premise"** means an instance of the Software deployed in Customer's or its Third-party Service Provider's environment utilizing Customer's or its Third-party Service Provider's hardware.

- k) **"Order"** means a purchase order, schedule or other ordering document issued by Customer indicating a promise to pay and acceptance of the then current Quote. All Orders are subject to this Agreement and any additional or inconsistent terms included on an Order are not binding on Jamf and Jamf expressly rejects them.
- l) **"Personal Information"** means any information relating to an identified or identifiable natural person that is stored, processed or transmitted in connection with, or as a result of, providing the Hosted Services or as otherwise specified in applicable Data Protection Laws. Personal Information does not include any information that is de-identified, anonymized and aggregated.
- m) **"Premium Cloud"** means an optional add-on for Hosted Services allowing additional flexibility and control over the server that is part of the Hosted Services.
- n) **"Premium Services"** means Jamf's optional professional services program for onsite or remote services provided by a Jamf professional services engineer or a Jamf certified integrator as further described at www.jamf.com/services/premium-services/.
- o) **"Premium Support"** means Jamf's optional premium technical support program, which includes enhanced support availability and access to dedicated support specialists as further described at www.jamf.com/support/jamf-pro/.
- p) **"Push Certificate"** means a certificate that establishes a trusted connection between Apple, Inc. ("Apple") and Customer's Apple Devices. Apple's Push Notification service ("**APNs**") sends Customer's Apple devices a silent notification that enables the Devices to communicate with the Software. Apple requires the Push Certificate to be renewed periodically.
- q) **"Quote"** means the system-generated offer from Jamf that identifies the Software and/or Services to be ordered by Customer and the Subscription and/or Services term and applicable fees.
- r) **"Services"** means, collectively, Hosted Services, Premium Cloud, JumpStart Services, Support and Maintenance, Premium Support, Premium Services, Training Services and/or other professional services. Services do not include custom development work.
- s) **"Software"** means Jamf's proprietary software identified in an applicable Order, together with modifications, updates and new versions provided by Jamf ("**Updates**"). Software and Updates do not include Components or other Jamf products having substantially enhanced or different functionalities or that require a separate license. Software does not include Test Software.
- t) **"Statement of Work" ("SOW")** means a description of JumpStart or Premium Services or other Services provided to Customer that includes the purpose, scope and Customer's requirements.
- u) **"Support and Maintenance"** means access to Jamf's standard technical support resources, as further described at www.jamf.com/support/jamf-pro/, and Software Updates.
- v) **"Test Software"** means an instance of the Software provided to Customer On-Premise, as Hosted Services, or for deployment on Devices for a limited term either for (i) trial or evaluation or similar purpose or (ii) testing a version of the Software not yet widely released, such as a beta, preview or release candidate.

- w) **"Third-party Service Provider"** means a third-party service provider or contractor that performs outsourced IT services for Customer's benefit solely to support Customer's internal business operations.
- x) **"Training Services"** means any of the optional certification courses offered by Jamf and/or private onsite training as further described at www.jamf.com/training/.

3. **Software License.** Subject to the terms and conditions of this Agreement, Jamf grants Customer a non-exclusive, non-sublicensable, non-transferable license to (i) access and use the Software either via the Hosted Services or On-Premise in object code form only and/or (ii) install and use the Software on Customer's Devices. In either case, such grant is for Customer's internal business purposes only and only for the number of Devices and term specified in the applicable Order (the **"Subscription"**).

- (a) Software is subject to the usage limits specified in an applicable Order (e.g., number of Devices). If Customer exceeds the contractual usage limit (**"Excess Use"**), Customer will execute an Order for additional quantities of the applicable Software promptly upon Jamf's request and/or pay any invoice for such Excess Use in accordance with Section 5 below.
- (b) Customer may (i) use only one instance of the Software in a production environment, (ii) create a reasonable number of instances of the Software in non-production environments solely to support Customer's internal business purposes and (iii) make a reasonable number of copies of the Software for archival and back-up purposes and a reasonable number of copies of the Documentation for internal business use only. Notwithstanding the foregoing, Customer may sublicense its instance of the Software to its Third-party Service Provider for the management of the Software for Customer's benefit. Test Software may only be used for the term and purpose authorized by Jamf, is provided "AS IS" without warranty of any kind and Jamf disclaims all warranties, indemnities and all other liabilities. Test Software is for non-production use only and is not eligible for Support and Maintenance. Customer's use of Test Software may be terminated upon notice by Jamf.

4. **Services.** This Agreement will govern the provision of all Services. Jamf shall ensure that all personnel performing Services are properly trained and supervised. Any Services performed on Customer's premises (**"Onsite Services"**) will be described in an applicable SOW and Customer may remove any of Jamf's personnel if Customer concludes, in its reasonable judgment, that such personnel are unqualified, incompetent or present a security risk to Customer. Jamf will not have access to Customer's systems or any unescorted access to Customer's premises, unless agreed in writing by the Parties. Customer acknowledges that Jamf is not performing creative work or custom software development in connection with any of the Services. Any creative work or custom development work will be performed pursuant to a separate written agreement.

- a) **Hosted Services.** Access to the Hosted Services is available 24 hours a day, 7 days a week with the exception of regularly scheduled or emergency maintenance and includes a server operating system, back-up and storage, firewall protection and monitoring of the Hosted Services to ensure they are operational at all times. Jamf will use commercially reasonable efforts to schedule maintenance during non-peak usage hours and provide advance notice. Jamf's Hosted Services Availability Commitment, scheduled maintenance, up-time and data restoration information is available at www.jamf.com/resources/product-documentation/hosted-services-availability-commitment/, which may be amended from time to time with notice to Customer. This section only applies if Customer is purchasing Hosted Services.

5. **Payment Terms.** Unless otherwise stated in the relevant Order, all invoices shall be due and payable net 30 days from the date of invoice. Customer shall pay fees and applicable taxes for the Software and/or Services as set forth on the applicable Order, including for Excess Use. If Customer is purchasing from a Jamf authorized reseller, payment terms are determined by Customer and the reseller.

6. **Permitted Use by Affiliates and Third-party Service Providers.** Customer may use the Software and/or Services for the benefit of its Affiliates to the extent Customer is permitted to use the Software under this Agreement. An Affiliate may license the Software or purchase Services under this Agreement. Customer may authorize one or more Third-party Service Providers to access and use the Software to the extent of Customer's permitted use under this Agreement, but solely on Customer's behalf and solely to support Customer's internal business operations. These authorizations may be revoked by Jamf if Customer, its personnel, Affiliates or Third-party Service Providers violate the terms and conditions of this Agreement. Customer is responsible for the full compliance of all provisions of this Agreement applicable to Customer by its Affiliates, their personnel and any Third-party Service Providers and their personnel.

7. **Customer Obligations, Representations and Warranties.**

- a) Customer must provide, at its expense, as applicable, such (i) internal network, hardware, mobile Devices, software applications, current operating systems and supported web browsers and (ii) broadband, cellular or Internet service, all as sufficient or necessary to access and use the Software and Services. In the event Jamf changes applicable technical requirements (which it may at its sole discretion), such changes will be communicated in advance to Customer.
- b) Customer will provide written acknowledgement of receipt or delivery of the Software or any Service in a format reasonably requested by Jamf. If no such acknowledgement is requested or provided, all Software and/or Services are deemed accepted upon delivery.
- c) Customer shall comply with all requirements imposed by Apple, and all other software vendors related to registration of software and/or requirements concerning Push Certificates, on Customer's systems or Devices.
- d) Customer is responsible for maintaining the confidentiality of the password(s) established by Customer and ensuring that they are not shared or otherwise disclosed. Customer is solely responsible for any and all activities conducted under the Customer user names.
- e) Customer will implement reasonable safeguards to prevent unauthorized access to or unauthorized use of the Software, Hosted Services and/or Test Software, and use the Software and/or Test Software only in accordance with the Documentation and this Agreement.
- f) The Customer represents and warrants that it owns or has the rights to use Personal Information, Customer Content and Third Party Content and that it has the necessary permissions and legal authority (including under Data Protection Laws) to provide it to Jamf and grant Jamf the rights to use it in connection with Jamf's performance of its obligations under this Agreement.

8. **Restrictions on Use of Software.** Customer shall not, except as provided in this Agreement, (a) copy, reproduce, distribute, transfer, rent, lend, loan, lease or sublicense any portion of the Software, (b) use or permit the Software to be used to perform services for third parties, whether on a service bureau, SaaS, time sharing basis or otherwise, (c) translate, adapt, modify, alter or combine with other software (combine does not mean using the Software in conjunction with other software), or prepare derivative works based in whole or in part on the Software, (d) reverse engineer, decompile, disassemble or otherwise reduce the Software to a human-perceivable form (except and solely to the extent expressly permitted by applicable law), (e) disclose or provide proprietary information regarding the Software to any third-party not authorized under this Agreement to use the Software on Customer's behalf, without Jamf's prior written consent, (f) externally provide, disclose or publish performance or evaluation results regarding the Software without Jamf's prior written consent, (g) alter or remove any proprietary notices or legends contained on or in the Software or Documentation, (h) use access to the Software to develop products, systems or services similar to or competitive with the Software, (i) upload any files or Third-party Content to the Hosted Services that contain viruses or harmful computer code or violates any intellectual property or proprietary rights of others, (j) interfere with or unreasonably burden the operation of the Hosted Services, including the servers, computers, routers, network, Internet or software that is part of, or interacts with the Hosted Services, (k) attempt to break, bypass, defeat or circumvent the controls or security measures of the Hosted Services and/or any components thereof or any software installed on the Hosted Services, (l) attempt to obtain access to any Jamf hardware, programs or data beyond the scope of the permitted access granted by Jamf, and (m) continue to access or use the Software and/or Hosted Services after Customer's access or authorization has been terminated or suspended or the Subscription has expired.

9. **Intellectual Property Ownership.** Customer owns all rights in Customer Content, including Intellectual Property Rights. The Software, Test Software and Services contain proprietary and copyright-protected material and trade secrets and other Intellectual Property Rights, which are exclusively owned by Jamf, its Affiliates or Jamf's licensors. Customer obtains no rights, title or interest of Jamf, its Affiliates or Jamf's licensors in and to the Software, Test Software and/or Services, including any Intellectual Property Rights and industrial property rights. Customer will not take, during or after the termination of this Agreement, any action inconsistent with such exclusive ownership. Customer is not obligated to provide Jamf any suggestions, recommendations, ideas, suggestions, or feedback about the Software, Test Software or Services ("**Feedback**") to Jamf. To the extent any Feedback is provided to Jamf by Customer (or Customer's Third-party Service Providers), Customer assigns any ownership rights of such Feedback to Jamf.

10. **Warranties.** Jamf represents and warrants to Customer that (a) it owns or has the right to license the Software and provide access to the Hosted Services; (b) the Software and Hosted Services shall substantially conform to the description thereof in the Documentation, (c) the Services shall be performed in a professional and workman-like manner, consistent with industry standards and (d) the Software and Services are provided free of viruses, malware or other malicious or destructive programs or features. These warranties are void if the Software and/or a Service is modified, combined with other product or services or used other than as provided in the Documentation or as expressly approved by Jamf in writing. Any claim made under any warranty shall be made within one year of the transaction or occurrence giving rise to such warranty.

11. **Disclaimers.** Except as set forth in Section 10, Jamf makes no warranties regarding the Software or Services. No oral information or advice given by Jamf or a Jamf authorized representative will create a warranty. Jamf disclaims all implied warranties, including without limitation, any warranties of merchantability and fitness for a particular purpose. Jamf does not warrant against all interference with Customer's enjoyment of the Software or Services, that the functions contained therein will meet Customer's requirements, that the operation thereof will be uninterrupted or error-free or that defects therein will be corrected. Jamf's patch management functionality contains information created and maintained by a variety of external sources that Jamf does not control or monitor and Jamf makes no guarantees whatsoever regarding the accuracy of the information contained in those external sources. Further, Jamf disclaims all liability for any damages or loss related to Customer's use of the patch management functionality or reliance on any information available therein.

12. **Limitations of Liability.** In no event will either Party or its successors or assigns be liable for incidental, special, indirect, consequential or punitive damages whatsoever, including, without limitation, damages for loss of profits, lost time, lost savings, loss of data or for business interruption arising out of or related to this Agreement or Customer's use of or inability to use the Software and/or Services. Customer's sole remedy and Jamf's sole liability for Jamf's breach of Section 10(a), 10(b) or 10(c) shall be to replace the Software and/or re-perform the Service. In no event, will either Party's total liability to the other Party for damages (other than as may be required by applicable law) exceed the amount of money paid with respect to the Software and/or Services to which they relate in the twelve (12) month period preceding any claim, except for Customer's breach of Jamf's Intellectual Property Rights or Section 17(c) or the Parties' third-party indemnity obligations under Section 13.

13. **Third-party Indemnification.** A Party, including its successors and assigns, will indemnify, hold harmless and defend the other Party, its agents, officers, directors, employees, affiliates, successors and assigns from and against any damage or liability, including reasonable costs and attorney's fees, asserted by third parties ("**Claim**"). In the case of Jamf indemnifying Customer, a Claim alleging that Customer's use or possession of the Software in accordance with this Agreement infringes a third-party's Intellectual Property Rights. In the case of Customer indemnifying Jamf, a Claim that (i) Customer's provision of Customer Content, Third-party Content or Personal Information to Jamf violates any third-party Intellectual Property Right or privacy right, (ii) Customer or its Third-party Service Provider's use of the Software and/or Services in violation of this Agreement violates any third-party Intellectual Property Right or privacy right or (iii) Customer violates Section 17(c) of this Agreement. A Party's indemnification obligations pursuant to this Section 13 are conditioned upon receipt of prompt written notice of the Claim from the Party seeking indemnification. A Party seeking indemnification shall also provide reasonable cooperation in the defense and settlement of any such Claim and take no action prejudicial to such defense and settlement.

14. **Term, Termination and Suspension.**

- a) **Term.** This Agreement is effective on the earlier of the Effective Date or the date the Customer begins using the Software and/or Services and shall remain in effect until the expiration of the applicable Subscription (unless extended by Jamf in its sole discretion) or otherwise terminated hereunder.
- b) **Termination.** Customer may terminate this Agreement, the Subscription and/or Services at any time by giving Jamf thirty (30) days' written notice and by paying any outstanding fees for the Subscription and Services. Jamf may terminate this Agreement, the Subscription and/or Services if Customer fails to pay applicable fees when due or otherwise breaches the Agreement and fails to cure any such breach within ten (10) days of receiving written notice from Jamf. Jamf may immediately terminate this Agreement, the Subscription and/or Services if Customer has ceased to operate in the ordinary course, made an assignment for the benefit of creditors or similar disposition of Customer's assets or becomes the subject of any bankruptcy, reorganization, liquidation, dissolution or similar proceeding. Upon termination for any reason, Customer shall cease using the Software and/or Services and destroy all copies of the Software and Documentation (certifying to such destruction) or return them to Jamf, as directed by Jamf.
- c) **Suspension of Hosted Services.** Notwithstanding the above, Jamf may suspend access to the Hosted Services immediately upon notice to Customer if Jamf determines that Customer's use of the Hosted Services (i) poses a security risk to the Hosted Services or any third party, (ii) may adversely impact the Hosted Services or the systems or

data of any other customer or (iii) may subject Jamf, its affiliates or any third party to liability. Jamf may terminate this Agreement, the Subscription and/or Services, if Customer fails to cure within thirty (30) days of the suspension notice. Customer remains responsible for payment under any Order and Customer will not be entitled to any service availability credits available pursuant to Jamf's service level commitment for any period of suspension.

- d) Termination of Hosted Services. Jamf may immediately terminate access to the Hosted Services (i) if Jamf's relationship with a third-party service provider who provides servers, software or other technology that Jamf uses to provide the Hosted Services terminates or requires Jamf to change the way Jamf provides the Hosted Services, (ii) if Jamf believes providing the Hosted Services could create a substantial security risk for Jamf or any third party or (iii) in order to comply with applicable law or requests of governmental entities.
- e) Return of Back-up. In the case of Hosted Services, Jamf will provide Customer a copy of the most recent backup of Customer's database that is available to Jamf and return copies of any Third-party Content that was provided to Jamf by Customer, if Customer requests a backup in writing thirty (30) days prior to termination.

15. **Notice.** All notices required or permitted under this Agreement shall be in writing and delivered to the attention of a Party's legal department at the address set forth above, either personally or via express or certified mail.

16. **Force Majeure.** Neither Party will be liable for damages for any delay or failure in performance or delivery arising out of causes beyond its reasonable control, including but not limited to, labor strikes, acts of God, acts of civil or military authority, fires, riots, wars, embargoes, Internet disruptions or electrical or communications failures.

17. **Compliance with Laws; Export Control.**

- a) Each Party will comply with all laws applicable to the actions contemplated by this Agreement.
- b) The United Nations Convention on Contracts for the International Sale of Goods, the application of which is expressly excluded, will not apply.
- c) The Services, Software, Test Software and other technology Jamf makes available and derivatives thereof may be subject to export laws and regulations of the United States and other jurisdictions. Each Party represents that it is not named on any United States government denied-party list nor is a Party owned by entities or individuals named to any United States government denied party list. Customer agrees that it shall not access or use the Software, Test Software or Services in any United States embargoed country or in breach of United States export laws or regulations.

18. **Confidentiality.** In connection with the performance of the Parties' obligations under this Agreement, either Party may provide information it considers proprietary or confidential to the other Party. "**Confidential Information**" includes all information relating to a Party's business that has value to a Party and is not generally known to the public, and, specifically includes, but is not limited to, Software, Test Software and Customer Content. Confidential Information excludes information that (a) lawfully is or becomes part of the public domain through no act or omission of the receiving Party, (b) comes into a Party's lawful possession without restriction on disclosure or (c) is independently created by a Party without use of or reliance on the other Party's Confidential Information. Each Party agrees that it shall protect the other Party's Confidential Information by using the same degree of care it uses to protect its own Confidential Information (but no less than a reasonable degree of care). Neither Party will use Confidential Information or divulge it to a third party, except as allowed or required to perform a Party's obligations under this Agreement. For avoidance of doubt, Customer may disclose Jamf Confidential Information to Customer's Affiliates to the extent reasonably necessary for a Customer Affiliate to use the Software as authorized under this Agreement. The Parties' confidentiality obligations under this Section 18 shall continue for three (3) years from the termination (for any reason) of this Agreement, except with respect to trade secrets for which the obligations shall continue so long as the Confidential Information legally remains a trade secret.

19. **Information Security and Data Processing.** At all times during the term of this Agreement, Jamf shall implement and maintain appropriate administrative, physical, technical and organizational safeguards and security measures designed to protect against anticipated threats to the security, confidentiality or integrity of Customer Content. Jamf shall only process Personal Information on behalf of and in accordance with Customer's instructions and applicable law, including Data Protection Laws. Jamf self-certifies and complies with the EU-US Privacy Shield Framework, as administered by the United States Department of Commerce and will maintain its self-certification. To the extent necessary, the Parties shall enter into an

appropriate and mutually agreed upon written agreement to satisfy cross-border transfer obligations relating to Personal Information that complies with Data Protection Laws.

The Parties agree that Jamf does not require (or request that) Customer provide Jamf any Personal Information to use the Software or to receive the benefit of the Services, and that it is Customer's choice alone to enter any Personal Information into the Software for the purpose of managing its Devices. Customer also has and is encouraged to use alternative methods to identify Devices managed with the Software, including by providing anonymous identifiers (e.g. Apple Mac serial no. xxx-xxx) that do not include or constitute Personal Information. In no event will Customer provide to Jamf any special categories of Personal Information as defined by GDPR.

20. **Government End Users.** The Software, Test Software and Documentation are "Commercial Computer Software" and "Commercial Computer Software Documentation" as those terms are defined at 48 C.F.R. § 2.101(b). Customer's rights in the Software, Test Software and Documentation are governed solely by the terms and conditions of this Agreement.

21. **Uniform Computer Information Transaction Act ("UCITA").** The UCITA or any version thereof adopted by any state in any form will not apply to this Agreement and to the extent that UCITA is applicable, the Parties agree to opt out of the applicability of UCITA pursuant to the opt out provision(s) contained therein.

22. **Third-party Acknowledgements.** Portions of the Software and/or Services may utilize or include open source and third-party software and other copyrighted material. Such software and Customer's use of the Software and/or Services is subject to any applicable third-party licenses as set forth within the Software or made available upon Customer's request. The terms and conditions of such third-party licenses shall govern Customer's use thereof. Jamf represents that it has the right and authorization to use and distribute open source and third-party software utilized in conjunction with the Software and Services or that is embedded in the Software and Jamf shall maintain compliance with all applicable open source and third-party software licenses.

23. **Data Collection.** Jamf and its service providers may collect and use statistical, usage, configuration and performance data of the Hosted Services and/or Software (collectively, "**Performance and Usage Data**") and Customer Content to monitor the performance, integrity and stability of the Hosted Services, address or prevent technical or security issues, provide Support Services, and improve the Hosted Services and/or Software. Jamf will not otherwise access, use or process Customer Content except as necessary to provide the Services. During and after the term of this Agreement, Jamf and its service providers may use and disclose Performance and Usage Data and Customer Content for any purpose, provided that such Performance and Usage Data and Customer Content have first been de-identified, anonymized and aggregated such that the data or content (as applicable) does not identify Customer or any individual, including, without limitation, a Customer employee or end user.

24. **Choice of Law, Jurisdiction and Venue.** This Agreement is governed by the laws of the State of Minnesota in the United States of America, without regard to its conflict of laws provisions.

a) **U.S. Customers.** If Customer is located in the United States of America, the sole and exclusive jurisdiction and venue for actions arising under this Agreement will be the federal and state courts located in Minneapolis, Minnesota. Customer agrees to this exclusive venue, to personal jurisdiction of these courts and to service of process in accordance with their rules of civil procedure and waives any objection that this venue is not convenient.

b) **International Customers.** If Customer is located outside of the United States of America, any dispute shall be submitted to binding arbitration in accordance with the Rules of Arbitration of the International Chamber of Commerce ("**ICC Rules**") then in effect in New York, New York in the United States of America. Arbitration will be conducted in the English language. The Parties will choose a single commercial arbitrator with substantial experience in software licensing and contract disputes. If the Parties are unable to choose an arbitrator within ten (10) days after an arbitration request, then a single arbitrator will be selected in accordance with the ICC Rules. The arbitrator will have the authority to grant specific performance and to allocate between the Parties the costs and expenses of arbitration in such equitable manner as the arbitrator may determine. Application may be made to a court having jurisdiction for acceptance, entry and/or an order for enforcement of the arbitrator's award.

c) **Injunctive Relief.** Jamf may institute an action in a court of proper jurisdiction for injunctive relief at any time.

25. **Miscellaneous.** This Agreement constitutes the entire agreement between the Parties with respect to the subject matter hereof and supersedes all prior understandings regarding such subject matter, whether written or oral. No amendment

or modification to the provisions of this Agreement will be binding unless in writing and signed both Parties. Any waiver by a Party of a breach of any provision of this Agreement will not operate as or be construed as a waiver of any further or subsequent breach. Provisions of this Agreement which by their nature are to be performed or enforced following any termination of this Agreement shall survive such termination. Jamf may assign this Agreement to an Affiliate or in connection with a merger or the sale of substantially all of Jamf's assets. This Agreement will be binding upon and inure to the benefit of the Parties, their successors and permitted assigns. If this Agreement is translated into languages other than English, the English version will control. This Agreement may be executed in counterparts, which together constitute one binding agreement. Jamf reserves all rights not expressly granted to Customer under this Agreement.

BY CLICKING THE "AGREE" BUTTON, YOU AGREE TO BE BOUND BY THE TERMS OF THIS AGREEMENT. IF YOU DO NOT AGREE TO THE TERMS OF THIS AGREEMENT, RETURN THE SOFTWARE TO JAMF FOR A REFUND. NOTWITHSTANDING THE FOREGOING, YOUR USE OF THE SOFTWARE OR SERVICES INDICATES ACCEPTANCE OF THESE TERMS.

Attachment C

Information Security Schedule

This information security schedule (“**Information Security Schedule**”) is subject to the terms and conditions of the agreement to which it is attached (the “**Agreement**”). For the purposes of this Information Security Schedule, Jamf shall ensure that third-party providers/suppliers/agents or subcontractors are in compliance with the applicable provisions of this Information Security Schedule. Terms not defined herein shall have the meaning set forth in the Agreement. In the event of a conflict between the Agreement and this Information Security Schedule, this Information Security Schedule shall prevail. This Information Security Schedule may be reasonably modified from time-to-time by Jamf and Customer will be notified of material changes.

Jamf shall implement appropriate technical and organizational security measures based on Industry Standards. “**Industry Standards**” means those commercially reasonable security measures that are designed to ensure the security, integrity and confidentiality of Customer Content, and, to protect against the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Customer Content. Further, Jamf will comply with applicable laws and regulatory requirements to ensure that Customer Content is not destroyed (except as expressly permitted under the Agreement), lost, altered, corrupted or otherwise impacted such that it is not readily usable by Customer in its business operations. Upon Customer’s request, Customer Content shall be immediately returned by Jamf using the Hosted Services.

Jamf has implemented and will maintain throughout the term of the Agreement, the following technical and organizational measures, controls, and information security practices:

1. Information Security Policies

- a. **Policies.** Jamf’s information security policies shall be documented and approved by Jamf’s management.
- b. **Review of the Policies.** Jamf’s information security policies shall 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’s approach to managing information security and its implementation (i.e. control objectives, controls, policies, processes and procedures for information security) shall be reviewed independently at planned intervals or when significant changes occur.
- d. **Disaster Recovery.** During the term of the Agreement, Jamf shall maintain a disaster recovery (DR) or high availability (HA) solution and related plan that is consistent with Industry Standards for the Services being provided. Jamf will test the DR or HA solution and related plan at least once annually.

2. Organization of Information Security

- a. **Security Accountability.** Jamf shall assign one or more security officers who will be responsible for coordinating and monitoring all information security functions, policies, and procedures.
- b. **Security Roles and Responsibility.** Jamf personnel, contractors and agents who are involved in providing Services shall be subject to confidentiality agreements with Jamf.
- c. **Risk Management.** Appropriate information security risk assessments shall be performed by Jamf as part of an ongoing risk governance program that is established with the following objectives (i) recognize risk, (ii) assess the impact of risk, and (iii) where risk reducing 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.** Appropriate security awareness, education, and training shall be provided to all Jamf personnel and contractors with access to the Software and Services provided to Customer.
- b. **Background Screening.** Jamf will ensure that background checks have been performed on Jamf personnel who are part of teams managing Jamf's hosting infrastructure. Additionally, background checks shall be performed on Jamf personnel or agents assigned to provide Services at Customer's premises. Subject to applicable law, background checks shall be conducted in accordance with Jamf's background screening policies and procedures. Only individuals who have passed such background checks will be allowed by Jamf to provide Services at Customer's premises or be part of Jamf's teams managing Jamf's hosted infrastructure.

4. Asset Management

- a. **Asset Inventory.**
 - i. Jamf will maintain an asset inventory of all media and equipment where Customer Content is stored. Access to such media and equipment shall be restricted to authorized personnel of Jamf.
 - ii. Jamf will classify Customer Content so that it is properly identified and access to Customer Content will be appropriately restricted.
 - iii. 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. 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. Notwithstanding the foregoing, Customer acknowledges that Jamf uses Amazon Web Services ("**AWS**") to provide Hosted Services and by entering into the Agreement, Customer specifically permits Jamf to use AWS for the provision of Hosted Services.
- b. **Security of Software Components.** Jamf agrees to appropriately inventory all Software components (including, but not limited to, open source software) used in Jamf's Hosted Services. Jamf will assess whether any such software components have any security defects and/or vulnerabilities that could lead to unauthorized disclosure of Customer Content or Customer's intellectual property. Jamf shall perform such assessment prior to delivery of or providing Customer access to such Hosted Services components and on an on-going basis thereafter during the term of the Agreement. Jamf agrees to remediate any security defect or vulnerability 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 and this Section 5 does not apply to access and use of the Software and Hosted Services by the Customer.
- b. **Authorization**
 - i. Jamf shall maintain user account creation and deletion procedures for granting and revoking access to all assets, Customer Content and all Jamf internal applications while providing Services under the Agreement. Jamf will assign an appropriate authority to approve creation of user accounts or elevated levels of access for existing accounts.

- ii. Jamf will maintain and update records of employees and contractors who are authorized to access systems that are involved in providing Services to the Customer and review such records at least quarterly. Administrative and technical support personnel, agents or contractors will only be permitted to have access to such data when required.
- iii. Jamf will ensure the uniqueness of user accounts and passwords for each individual. Individual user accounts will not be shared.
- iv. Jamf will remove access rights to assets that store Customer Content for personnel and contractors upon termination of their employment, contract or agreement within 24 hours, or access shall be appropriately adjusted 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 and in effect 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.

6. Cryptography.

- a. Jamf will maintain policies and standards regarding the use of cryptographic controls that are implemented to protect Customer Content. Jamf will implement Industry Standard key management policies and practices designed to protect encryption keys for their entire lifetime.

7. Physical and Environmental Security

- a. **Physical Access to Facilities.** Jamf will limit access to facilities where systems that are involved in providing the Services are located to identified personnel, agents and contractors.
- b. **Protection from Disruptions.** Jamf will use reasonable efforts, and, to the best of Jamf's ability, protect equipment from power failures and other disruptions caused by failures in supporting utilities.
- c. **Secure Disposal or Reuse of Equipment.** Jamf shall verify equipment containing storage media to confirm that all Customer Content has been deleted or securely overwritten 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 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 shall have policies that govern the installation of software and utilities by personnel.
- d. **Change Management.** Jamf shall maintain and implement procedures to ensure that only approved and secure versions of the code/configurations/systems/applications will be deployed in the production environment(s).

- e. **Encryption of Data.** With Jamf's standard Hosted Services, Customer Content is encrypted in-transit to the Hosted Services and stored encrypted at-rest. Encryption solutions will be deployed with no less than 256-bit Advanced Encryption Standard (AES) encryption.

9. Communications Security

a. Information Transfer.

- i. Jamf will use Industry Standard encryption to encrypt Customer Content that is in transit.
- ii. Jamf will restrict access through encryption to Customer Content stored on media that is physically transported from Jamf facilities.

b. Security of Network Services.

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

c. Intrusion Detection.

- i. Jamf will deploy intrusion detection or intrusion prevention systems for all systems providing service to Jamf's customers 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 shall 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 to perform the Services and receive appropriate training regarding Jamf's secure application development practices.

c. System Hardening.

- i. Jamf will establish and ensure the use of standard secure configurations of operating systems. Images should represent hardened versions of the underlying operating system and the applications installed on the system. Hardening includes removal of unnecessary accounts (including service accounts), disabling or removal of unnecessary services, applying patches, closing open and unused network ports, 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 access reviews for system administrators at least quarterly for all supporting systems requiring access control.
- iii. Jamf will implement patching tools and processes for both applications and operating system software. When outdated systems can no longer be patched, Jamf will update to the latest version of application software. Jamf will remove outdated, unsupported, and unused software from the system.
- iv. Jamf will limit administrative privileges to only those personnel who have both the knowledge necessary to administer the operating system and a business need to modify the configuration of the underlying operating system.

- d. **Infrastructure Vulnerability Scanning.** Jamf will scan its internal environment (e.g. servers, network devices, etc.) related to the Services on a monthly basis and external environment related to the Services on a weekly basis. Jamf will have a defined process to address any findings but will ensure that any high-risk vulnerabilities are addressed within 30 days.
- 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.
- 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 Hosted Services on a recurring basis no less frequent than once annually. Additionally, Jamf will have an industry recognized independent third party perform an annual test. Jamf will have a defined process to address any findings but will ensure that any high-risk vulnerabilities are addressed within 30 days. Upon Customer's written request, but no more than once per year, Jamf shall 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. Where other third-party applications or services must be used by Jamf, Jamf's contract with any third-party must clearly state security requirements consistent with the security requirements of this Information Security Schedule, which will be applied to the third party. In addition, service level agreements with the third party must be clearly defined.
- b. Any external third-party or resources gaining access to systems must be covered by a signed agreement containing confidentiality and security provisions consistent with the confidentiality and security requirements of the Agreement and this Information Security Schedule.
- c. Jamf will perform quality control and security management oversight of outsourced software development.

12. Information Security Incident Management

- a. **Incident Response Process**
 - i. A **"Security Incident"** shall mean any accidental or unlawful destruction, loss, alteration, unauthorized disclosure or access to any Customer Content stored on Jamf's equipment or in Jamf's facilities, or unauthorized access to such equipment or facilities resulting in the loss, disclosure, or alteration of Customer Content.
 - ii. Jamf will maintain a record of Security Incidents noting the description of the Security Incident, the applicable time periods, the impact, the person reporting and to whom the Security Incident was reported, and the procedures to remediate the incident.
 - iii. In the event of a Security Incident, Jamf will (a) notify the Customer of the Security Incident by contacting the Customer point of contact in writing promptly, and in any event within seventy-two (72) hours following the discovery of the Security Incident, (b) promptly investigate the Security Incident, (c) promptly provide Customer with all relevant detailed information about the Security Incident, and (d) take reasonable steps to mitigate the effects and to minimize any damage resulting from the Security Incident. All Security Incident information provided to Customer shall be deemed to be Confidential Information.

13. Security Assessment

- a. **SSAE18 SOC 2 Reports (or equivalent).** During each calendar year, Jamf will obtain, at Jamf's cost, a SSAE18 SOC2 Type II report (or equivalent) related to the provision of the Hosted Services, conducted by an independent public auditing firm. The minimum scope of these reports will be the Trust Service Principles of Security (also known as the Common Criteria), Availability, and Confidentiality. Jamf will comply with future guidance relating to SSAE18 as issued by the AICPA, IAASB, the Securities and Exchange Commission or the Public Company Accounting Oversight Board. Upon Customer's written request, no more than once annually, Jamf will provide a copy of the SSAE18 SOC2 Type II report (or equivalent) to Customer, which report is considered to be Jamf's Confidential Information.
- b. **Customer Security Assessment.** Upon Customer's reasonable request, but no more than once annually, Jamf will complete, in a timely and accurate manner, an information security questionnaire provided by Customer to Jamf, in order to verify Jamf's compliance with this Information Security Schedule ("**Security Assessment**"). If after completion of the Security Assessment, Customer reasonably determines, or in good faith believes, that Jamf's security practices and procedures do not meet Jamf's obligations pursuant to the Agreement or this Information Security Schedule, then Customer will notify Jamf of the perceived deficiencies. Jamf shall evaluate such perceived deficiencies and engage Customer (as necessary) to determine if such deficiencies are actual deficiencies in Jamf's security practices and procedures. If perceived deficiencies identified by Customer are confirmed to be deficiencies in Jamf's security practices and procedures, Jamf shall without unreasonable delay (i) correct such deficiencies at its own expense and (ii) provide Customer, or its duly authorized representatives, with reasonable documentation and information confirming the remediation of such deficiencies, which shall be deemed to be Jamf's Confidential Information. If any perceived deficiencies identified by Customer are deemed to be deficiencies caused by Customer's use of the Hosted Services, Jamf shall provide reasonable technical support to assist Customer in appropriate use of the Hosted Services to remediate such deficiencies.
- c. **Security Issues and Remediation Plan.** To the extent security issues identified by Customer during a Security Assessment have been deemed to be security issues with Jamf's security practices and procedure, such security issues will have an assigned risk rating and an applicable timeframe to remediate (based upon risk). Jamf shall remediate the security issues attributable to Jamf's security practice and procedures within applicable remediation timeframes. If Jamf fails to remediate any of the high or critical rated security issues within the stated remediation timeframes, Customer has the right to terminate the Agreement for material breach immediately upon notice to Jamf.

EDUCATION CUSTOMER ADDENDUM TO SOFTWARE LICENSE AND SERVICES AGREEMENT

JAMF Software, LLC ("**Jamf**") recognizes that certain public education institutions (collectively, "**Education Institutions**") are subject to laws, rules and regulations that may restrict them from agreeing to certain contractual terms in contracts with private businesses. This Education Customer Addendum (this "**Addendum**") is an addendum to the Software License and Services Agreement (the "**Agreement**") between Jamf and Customer, the Education Institution identified below. Customer represents and warrants that it is an Education Institution. This Addendum amends the Agreement as set forth herein. Terms used but not defined herein have the meaning given to them in the Agreement.

1. Section 1 d) (Data Protection Laws definition) is replaced with the following:

"Data Protection Laws" means applicable domestic and foreign laws, rules, directives and regulations, on any local, provincial, state, federal or national level, pertaining to government data protection, student and education data privacy, data privacy, data security and/or the protection of Personal Information in effect as of the date of this Agreement, including but not limited to, Regulation (EU) 2016/679, General Data Protection Regulation ("**GDPR**").

2. Section 5 (Payment Terms) is replaced with the following:

Payment Terms. Unless otherwise stated in the relevant Order, all invoices shall be due and payable net 30 days from the date of invoice. Customer shall pay fees and applicable taxes for the Software and/or Services as set forth on the applicable Order, including for Excess Use. If Customer is purchasing from a Jamf authorized reseller, payment terms are determined by Customer and the reseller.

If Customer is a tax-exempt entity that is exempt from applicable taxes, Customer will provide Jamf with a copy of Customer's tax-exempt certificate by the Effective Date. Provided Jamf has received the tax-exempt certificate from Customer, Jamf will not invoice, nor will Customer pay for any such applicable taxes. Customer will promptly notify Jamf of any changes in Customer's tax-exempt status.

3. Section 13 (Third-party Indemnification) is intentionally omitted from the Agreement.
4. Section 17 (Compliance with Laws; Export Control) is revised so that subsection a) is replaced with the following:
 - a) Each Party will comply with all laws applicable to the actions contemplated by this Agreement, specifically including all Data Protection Laws applicable in the jurisdiction of Customer's principal place of business to the extent applicable to Jamf's Services.
5. Section 18 (Confidentiality) is deleted in its entirety and replaced with:

Confidentiality.

- a) In connection with the performance of the Parties' obligations under this Agreement, either Party may provide information it considers proprietary or confidential to the other Party. "**Confidential Information**" includes all information relating to a Party's business that has value to a Party and is not generally known to the public or that meets the definitions of confidential, trade secret or similar information under applicable state open records or data practices laws. Confidential Information specifically includes, but is not limited to, Software, Test Software and Customer Content. Confidential Information excludes information that (i) lawfully is or becomes part of the public domain through no act or omission of the receiving Party, (ii) comes into a Party's lawful possession without restriction on disclosure or (iii) is independently created by a Party without use of or reliance on the other Party's Confidential Information. Each Party agrees that it shall protect the other Party's Confidential Information by using the same degree of care it uses to protect its own Confidential Information (but no less than a reasonable degree of care). Neither Party will use Confidential Information or divulge it to a third party, except as allowed or required to perform a Party's obligations under this Agreement. It is understood that Customer's obligations under this Section 18 a) are subject to any applicable disclosure obligations it has under applicable state open records or data practices laws. For avoidance of doubt, Customer may disclose Jamf Confidential Information to Customer's Affiliates to the extent reasonably necessary for a Customer Affiliate to use the Software as authorized under this Agreement. The Parties' confidentiality obligations under this Section 18 shall continue for three (3) years from the termination (for any reason) of this Agreement, except with respect to trade secrets for which the obligations shall continue so long as the Confidential Information legally remains a trade secret.

- b) Neither Party will publicly use or refer to the other Party's name, trademarks, service marks or logos in any advertising, marketing materials, business development activities, press releases, websites, social media or other publicity-related matter, without the prior written consent of the other Party.

6. Section 24 (Choice of Law, Jurisdiction and Venue) is revised to replace in its entirety the existing text of the Section with the following:


Choice of Law and Injunctive Relief. This Agreement is governed by the laws of the jurisdiction of Customer's principal business address set forth in the signature block below, without regard to its conflict of laws provisions. Customer acknowledges that any breach by it of this Agreement may cause immediate and irreparable harm to Jamf. Therefore, Jamf may institute an action in a court of proper jurisdiction for injunctive relief at any time without proof of actual damages and without the necessity of securing or posting any bond in connection with such remedy.

7. This Addendum will be binding upon and inure to the benefit of the Parties, their successors and permitted assigns.

8. If any conflicts exist between the Agreement and this Addendum, this Addendum shall prevail. With the exception of any conflicts and revisions amended herein, the Agreement shall remain unchanged and in full force and effect.

9. This Addendum will become effective as of the last signature date below.

JAMF Software, LLC

Signature: 

Name: Shawn Abbas

Title: VP, Finance

Date: June 1, 2020

Jamf Internal Account Reference:

Customer

Name of Educational Institution:

Address: _____

Signature: _____

Name: _____

Title: _____

Date: _____