EXHIBIT D

DATA SHARING AND CONFIDENTIALITY AGREEMENT

INCLUDING

PARENTS BILL OF RIGHTS FOR DATA SECURITY AND PRIVACY

AND

SUPPLEMENTAL INFORMATION ABOUT THE MLSA

1. **Purpose**

(a) This Exhibit supplements the Master License and Service Agreement ("MLSA") to which it is attached, to ensure that the MLSA conforms to the requirements of New York State Education Law Section 2-d and any implementing Regulations of the Commissioner of Education (collectively referred to as "Section 2-d"). This Exhibit consists of the terms of this Data Sharing and Confidentiality Agreement, a copy of Erie 1 BOCES' Parents Bill of Rights for Data Security and Privacy signed by the Vendor, and the Supplemental Information about the MLSA that is required to be posted on Erie 1 BOCES' website.

(b) To the extent that any terms contained within the MLSA, or any terms contained within any other Exhibits attached to and made a part of the MLSA, conflict with the terms of this Exhibit, the terms of this Exhibit will apply and be given effect. In the event that Vendor has online or written Terms of Service ("TOS") that would otherwise be applicable to its customers or users of its Product that is the subject of the MLSA, to the extent that any term of the TOS conflicts with the terms of this Exhibit, the terms of this Exhibit will apply and be given effect.

2. **Definitions**

Any capitalized term used within this Exhibit that is also found in the MLSA will have the same definition as contained within the MLSA.

In addition, as used in this Exhibit:

(a) "Student Data" means personally identifiable information, as defined in Section 2-d, from student records that Vendor receives from a Participating Educational Agency pursuant to the MLSA.

(b) "Teacher or Principal Data" means personally identifiable information relating to the annual professional performance reviews of classroom teachers or principals that is confidential and not subject to release under the provisions of New York Education Law Sections 3012-c or 3012-d, that Vendor receives from a Participating Educational Agency pursuant to the MLSA.

(c) "Protected Data" means Student Data and/or Teacher or Principal Data to the extent applicable to Vendor's Product.

(d) "Participating Educational Agency" means a school district within New York State that purchases certain shared instructional technology services and software through a Cooperative Educational Services Agreement with a RICS, and as a result is licensed to use Vendor's Product pursuant to the terms of the MLSA. For purposes of this Exhibit,

the term also includes Erie 1 BOCES or another RIC that is licensed to use Vendor's Product pursuant to the MLSA to support its own educational programs or operations.

3. **Confidentiality of Protected Data**

(a) Vendor acknowledges that the Protected Data it receives pursuant to the MLSA may originate from several Participating Educational Agencies located across New York State, and that this Protected Data belongs to and is owned by the Participating Educational Agency from which it originates.

(b) Vendor will maintain the confidentiality of the Protected Data it receives in accordance with federal and state law (including but not limited to Section 2-d) and Erie 1 BOCES's policy on data security and privacy. Vendor acknowledges that Erie 1 BOCES is obligated under Section 2-d to adopt a policy on data security and privacy, Erie 1 BOCES will provide Vendor with a copy of its policy as soon as practicable following adoption. Vendor and Erie 1 BOCES agree to engage in good faith negotiations to modify this Data Sharing Agreement to the extent necessary to ensure Vendor's continued compliance with Section 2-d.

4. **Data Security and Privacy Plan**

Vendor agrees that it will protect the confidentiality, privacy and security of the Protected Data received from Participating Educational Agencies in accordance with Erie 1 BOCES' Parents Bill of Rights for Data Privacy and Security, a copy of which has been signed by the Vendor and is set forth below.

Additional elements of Vendor's Data Security and Privacy Plan are as follows:

(a) In order to implement all state, federal, and local data security and privacy requirements, including those contained within this Data Sharing and Confidentiality Agreement, consistent with Erie 1 BOCES' data security and privacy policy, Vendor will: Review its data security and privacy policy and practices to ensure that they are in conformance with all applicable federal, state, and local laws and the terms of this Data Sharing and Confidentiality Agreement. In the event Vendor's policy and practices are not in conformance, the Vendor will implement commercially reasonable efforts to ensure such compliance.

(b) In order to protect the security, confidentiality and integrity of the Protected Data that it receives under the MLSA, Vendor will have the following reasonable administrative, technical, operational and physical safeguards and practices in place throughout the term of the MLSA: access control policy designed to restrict access to any Protected Data only to authorized personnel; background screening and employee training; encryption of data when in transit to Hosted Services and stored encrypted at rest; and the measures outlined in Vendor's Information Security Schedule, which is attached as Attachment 1 to this Exhibit D.

(c) Vendor will comply with all obligations set forth in Erie 1 BOCES' "Supplemental Information about the MLSA" below.

(d) For any of its officers or employees (or officers or employees of any of its subcontractors or assignees) who have access to Protected Data, Vendor has provided or will provide training on the federal and state laws governing confidentiality of such data prior to their receiving access, as follows: Annually, Vendor will require that all of its employees undergo data security and privacy training to ensure that these individuals are aware of and familiar with all applicable data security and privacy laws.

(e) Vendor [___X___will _____will not utilize sub-contractors for the purpose of fulfilling one or more of its obligations under the MLSA. In the event that Vendor engages any subcontractors, assignees, or other authorized agents to perform its obligations under the MLSA, it will require such subcontractors, assignees, or other authorized agents to execute written agreements as more fully described in Erie 1 BOCES' "Supplemental Information about the MLSA," below.

(f) Vendor will manage data security and privacy incidents that implicate Protected Data, including identifying breaches and unauthorized disclosures, and Vendor will provide prompt notification of any breaches or unauthorized disclosures of Protected Data in accordance with Section 6 of this Data Sharing and Confidentiality Agreement.

(g) Vendor will implement procedures for the return, transition, deletion and/or destruction of Protected Data at such time that the MLSA is terminated or expires, as more fully described in Erie 1 BOCES' "Supplemental Information about the MLSA," below.

5. **Additional Statutory and Regulatory Obligations**

Vendor acknowledges that it has the following additional obligations with respect to any Protected Data received from Participating Educational Agencies, and that any failure to fulfill one or more of these statutory or regulatory obligations shall be a breach of the MLSA and the terms of this Data Sharing and Confidentiality Agreement:

(a) Limit internal access to education records to those individuals that are determined to have legitimate educational interests within the meaning of Section 2-d and the Family Educational Rights and Privacy Act (FERPA).

(b) Limit internal access to Protected Data to only those employees or subcontractors that need access in order to assist Vendor in fulfilling one or more of its obligations under the MLSA.

(c) Not use education records for any purposes other than those explicitly authorized in this Data Sharing and Confidentiality Agreement.

(d) Not disclose any personally identifiable information to any other party, except for authorized representatives of Vendor using the information to carry out Vendor's obligations under the MLSA, unless:

(i) the parent or eligible student has provided prior written consent; or

(ii) the disclosure is required by statute or court order and notice of the disclosure is provided to Participating Educational Agency no later than the time of disclosure, unless such notice is expressly prohibited by the statute or court order.

(e) Maintain reasonable administrative, technical, and physical safeguards to protect the security, confidentiality, and integrity of personally identifiable student information in its custody;

(f) Use encryption technology that complies with Section 2-d, as more fully set forth in Erie 1 BOCES' "Supplemental Information about the MLSA," below.

(g) Provide notification to Erie 1 BOCES (and Participating Educational Agencies, to the extent required by, and in accordance with, Section 6 of this Data Sharing and Confidentiality Agreement) of any breach of security resulting in an unauthorized release of Protected Data by Vendor or its assignees or subcontractors in violation of state or federal law or other obligations relating to data privacy and security contained herein.

(h) Promptly reimburse Erie 1 BOCES, another RIC, or a Participating School District for the reasonable cost of notification, in the event they are required under Section 2-d to notify affected parents, students, teachers or principals of a breach or unauthorized release of Protected Data attributed to Vendor or its subcontractors or assignees.

6. **Notification of Breach and Unauthorized Release**

(a) Vendor shall promptly notify Erie 1 BOCES of any breach or unauthorized release of Protected Data in the most expedient way possible and without unreasonable delay, but no more than seven (7) calendar days after Vendor has discovered or been informed of the breach or unauthorized release.

(b) Vendor will provide such notification to Erie 1 BOCES by contacting Michelle Okal-Frink directly by email at mokal@e1b.org, or by calling (716) 821-7200 (office) or (716) 374-5460 (cell).

(c) Vendor will cooperate with Erie 1 BOCES and provide as much information as possible directly to Michelle Okal-Frink or her designee about the incident, including but not limited to: a description of the incident, the date of the incident, the date Vendor discovered or was informed of the incident, a description of the types of personally identifiable information involved, an estimate of the number of records affected, the Participating Educational Agencies affected, what the Vendor has done or plans to do to investigate the incident, stop the breach and mitigate any further unauthorized access or release of Protected Data, and contact information for Vendor representatives who can assist affected individuals that may have additional questions.

(d) Vendor acknowledges that upon initial notification from Vendor, Erie 1 BOCES, as the educational agency with which Vendor contracts, has an obligation under Section 2-d to in turn notify the Chief Privacy Officer in the New York State Education Department ("CPO"). Vendor shall not provide this notification to the CPO directly. In the event the CPO contacts Vendor directly or requests more information from Vendor regarding the

incident after having been initially informed of the incident by Erie 1 BOCES, Vendor will promptly inform Michelle Okal-Frink or her designees.

(e) Vendor will consult directly with Michelle Okal-Frink or her designees prior to providing any further notice of the incident (written or otherwise) directly to any other RIC or Regional Information Center, or any affected Participating Educational Agency.

wnyric www.wnyric.org
Erie 1 BOCES Education Campus • 355 Harlem Road • West Seneca, NY 14224-1892
erie boces

EXHIBIT D (CONTINUED)

PARENTS BILL OF RIGHTS FOR DATA PRIVACY AND SECURITY

Erie 1 BOCES is committed to protecting the privacy and security of student, teacher, and principal data. In accordance with New York Education Law § 2-d, the BOCES wishes to inform the community of the following:

(1) A student's personally identifiable information cannot be sold or released for any commercial purposes.

(2) Parents have the right to inspect and review the complete contents of their child's education record.

(3) State and federal laws protect the confidentiality of personally identifiable information, and safeguards associated with industry standards and best practices, including but not limited to, encryption, firewalls, and password protection, must be in place when data is stored or transferred.

(4) A complete list of all student data elements collected by the State is available for public review at **http://www.nysed.gov/data-privacy-security/student-data-inventory**, or by writing to the Office of Information & Reporting Services, New York State Education Department, Room 863 EBA, 89 Washington Avenue, Albany, New York 12234.

(5) Parents have the right to have complaints about possible breaches of student data addressed. Complaints should be directed in writing to the Chief Privacy Officer, New York State Education Department, 89 Washington Avenue, Albany, New York 12234. Complaints may also be submitted using the form available at the following website **http://www.nysed.gov/data-privacy-security/report-improper-disclosure**.

BY THE VENDOR:

DocuSigned by:
Shawn Abbas
89B2C6B5E420480...
Signature

Shawn Abbas
Printed Name

VP Finance
Title

6/20/2023
Date

EXHIBIT D (CONTINUED)

SUPPLEMENTAL INFORMATION

ABOUT THE MASTER LICENSE AND SERVICE AGREEMENT
BETWEEN
ERIE 1 BOCES AND *JAMF SOFTWARE LLC.*]

Erie 1 BOCES has entered into a Master License and Service Agreement ("MLSA") with *Jamf Software LLC* which governs the availability to Participating Educational Agencies of the following Product(s):

Jamf Pro- On Premise
Jamf Pro- Cloud

Pursuant to the MLSA, Participating Educational Agencies may provide to Vendor, and Vendor will receive, personally identifiable information about students, or teachers and principals, that is protected by Section 2-d of the New York State Education Law ("Protected Data").

Exclusive Purpose for which Protected Data will be Used: The exclusive purpose for which Vendor is being provided access to Protected Data is to provide Participating Educational Agencies with the functionality of the Product(s) listed above. Vendor agrees that it will not use the Protected Data for any other purposes not explicitly authorized in the MLSA. Protected Data received by Vendor, or any of Vendor's subcontractors, assignees, or other authorized agents, will not be sold, or released or used for any commercial or marketing purposes.

Oversight of Subcontractors: In the event that Vendor engages subcontractors, assignees, or other authorized agents to perform one or more of its obligations under the MLSA (including any hosting service provider), it will require those to whom it discloses Protected Data to execute legally binding agreements acknowledging the obligation under Section 2-d of the New York State Education Law to comply with the same data security and privacy standards required of Vendor under the MLSA and applicable state and federal law. Erie 1 BOCES acknowledges and consents to Vendor's use of Amazon Web Services ("AWS") to provide Hosting Services. Vendor will ensure that such subcontractors, assignees, or other authorized agents abide by the provisions of these agreements by: entering into appropriate confidentiality agreements that contain similar restrictions to those outlined in the Agreement

Duration of MLSA and Protected Data Upon Expiration:

- The MLSA commences on July 1, 2023 and expires on June 30, 2026.
- Upon expiration of the MLSA without renewal, or upon termination of the MLSA prior to expiration, Vendor will securely delete or otherwise destroy any and all Protected Data remaining in the possession of Vendor or its assignees or stored in a subcontractor's infrastructure. If requested by Erie 1 BOCES and/or any Participating Educational Agency, Vendor will assist a Participating Educational Agency in exporting all Protected Data previously received back to the Participating Educational Agency for its own use,

prior to deletion, in such formats as may be requested by the Participating Educational Agency.

- In the event the Master Agreement is assigned to a successor Vendor (to the extent authorized by the Master Agreement), the Vendor will cooperate with Erie 1 BOCES as necessary to transition Protected Data to the successor Vendor prior to deletion.
- Neither Vendor nor any of its subcontractors or other authorized persons or entities to whom it has disclosed Protected Data will retain any Protected Data, copies, summaries or extracts of the Protected Data, or any de-identified Protected Data, on any storage medium whatsoever after expiration of the Master Agreement and any renewal terms unless required by law to do so. Upon written request, Vendor, , will provide Erie 1 BOCES with a certification from an appropriate officer that these requirements have been satisfied in full by Vendor and/or any subcontractor to whom Vendor has disclosed Protected Data.
-

Challenging Accuracy of Protected Data: Parents or eligible students can challenge the accuracy of any Protected Data provided by a Participating Educational Agency to Vendor, by contacting the student's district of residence regarding procedures for requesting amendment of education records under the Family Educational Rights and Privacy Act (FERPA). If applicable, Teachers or principals may be able to challenge the accuracy of APPR data provided to Vendor by following the appeal process in their employing school district's applicable APPR Plan.

Data Storage and Security Protections: Any Protected Data Vendor receives will be stored on systems maintained by Vendor, or by a subcontractor under the direct control of Vendor, in a secure data center facility located within the United States. The measures that Vendor will take to protect Protected Data include adoption of technologies, safeguards and practices that align with the NIST Cybersecurity Framework and industry best practices including, but not necessarily limited to, disk encryption, file encryption, firewalls, and password protection.

Encryption of Protected Data: Vendor (or, if applicable, its subcontractors) will protect Protected Data in its custody from unauthorized disclosure while in motion or at rest, using a technology or methodology specified by the secretary of the U.S. Department of HHS in guidance issued under Section 13402(H)(2) of P.L. 111-5 or encryption solutions with no less than 256-bit Advanced Encryption Standard(AES) encryption.

.

Exhibit D- Attachment 1

Vendor 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.

Exhibit F
Vendor Standard Technical Support

Subject to the terms and conditions of the Jamf Software License and Services Agreement or other applicable agreement between Jamf and Customer (the "Agreement"), Jamf will provide the Standard Technical Support Services as detailed in this Standard Technical Support Description. Capitalized terms used, but not defined, here will have the meaning set forth in the Agreement.

Scope of Standard Technical Support Services

- Jamf will provide electronic support to Customer. Electronic support may include email, in-product, portal-based or chat support depending on the Software or Services Customer has purchased.
- Jamf may provide telephone support, depending on the Software or Services that Customer has purchased.
- Telephone and electronic support are available regionally in the United States, Europe, Australia/Asia, and Japan during local business hours. For more information on local business hours please see:

  Technical Support Desk

For further information on contact mediums and resources see: Support

Incident Response Times

Once a Customer submits a case via electronic or telephone support, Jamf will determine whether the case is an Incident and the Priority Status of that Incident. An "Incident" is a single reproducible issue focusing on one aspect of the Software or Hosted Services' failure to perform in substantial conformity with the Documentation that can be re-created and identified by isolating specific symptoms. If a submitted case can be broken down into subordinate Incidents, each Incident will be handled separately. Jamf will use commercially reasonable efforts to respond as follows:

Priority Status of Incident | New Case Response Time | In Progress Case Response Time
Low | 8 hours | 32 Hours

Medium | 4 hours | 24 Hours

High | 2 hours | 12 Hours
Urgent (Emergency) | 1 hour | 4 Hours

- Priority Statuses

  - Low Priority Status means an Incident that does not materially impact functionality.
  - Medium Priority Status means an Incident causing some loss in functionality.
  - High Priority Status means an Incident causing a significant loss in functionality.
  - Urgent (Emergency) Priority Status means an Incident causing a total loss of functionality.

- Incidents are resolved when, in Jamf's sole discretion, Jamf has:
  - Provided information regarding a reasonable solution or workaround to the Customer.
  - Notified the Customer that the issue will be resolved by upgrading to a newer release.
  - Provided information that isolates the issue to a third-party product.
  - Determined that the issue is an enhancement request or identified product issue.

Documentation

Jamf makes Documentation available online at Product Documentation

Updates

Jamf will provide periodic updates to the Software under the terms of the Agreement. Updates will be made available solely when and as determined by Jamf. For On-Premise installations, the Customer is responsible for installing Updates.

Effective Date

- Standard Technical Support Services are available beginning on the Effective Date of the Agreement.
- Standard Technical Support Services are included with Hosted Services subscriptions.
- For On-Premise installations, Standard Technical Support Services is usually purchased in 12-month increments.

Customer Obligations

- Customer will promptly notify Jamf of any Incident by submitting a case and providing Jamf with all reasonably necessary information in a timely manner.
- Customer will comply with the terms of this Standard Technical Support Description and the Agreement.
- Customer will cooperate with Jamf's requests for assistance or information.

Limitations

- Standard Technical Support Services do not include custom coding, consulting or other professional services, optional paid premium support offerings, or training.
- Jamf is not responsible for any delay or failure of performance due to a failure or delay of Customer.
- Jamf has no obligation to provide Standard Technical Support Services for:
    - Any operation or use of Software or Hosted Services other than as specified in the Documentation or as permitted by the Agreement;
    - Customer's negligence, abuse, or misuse of the Software or Hosted Services;
    - Any Test Software; or
    - Any third-party software or tools.

Service Changes

Jamf may, in its sole discretion, change any aspect of this Standard Technical Support Description with advanced notice. With any such changes, Jamf will not materially reduce the Standard Technical Support Services.