Jamf Information Security Schedule

This Information Security Schedule ("**Information Security Schedule**") is incorporated into the Jamf Software License and Services Agreement or supplements the license agreement between you and Jamf to which it is attached (the "**Agreement**"). We will ensure that our third-party providers, suppliers, agents, and subcontractors that provide Product Offerings to you comply with the applicable provisions of this Information Security Schedule. Capitalized terms used but not defined in this Information Security Schedule will have the meaning given to them in the Agreement. If there is a conflict between the Agreement and this Information Security Schedule, this Information Security Schedule will prevail. We may modify this Information Security Schedule for consistency with any changes in Jamf's organizational security measures so long as any such modifications do not materially degrade the levels of protection afforded under it.

We will implement appropriate technical and organizational security measures based on applicable Industry Standards and Data Protection Laws. "**Industry Standard(s)**" means those commercially reasonable security measures designed to ensure the security of the Product Offerings Jamf provides to you and include standard technical and organizational security measures 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. We will comply with applicable Data Protection Laws to ensure that Customer Content, as it is provided to Jamf, is not destroyed (except as expressly permitted under the Agreement), lost, altered, corrupted, or otherwise impacted such that it is not readily usable by you in your business operations.

We have 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 and Measures

a) Policies. Jamf's senior management will document and approve our information security policies.

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

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

d) Disaster Recovery. During the term of the Agreement, we will maintain a disaster recovery (DR) or high availability (HA) solution and related plan that is consistent with Industry Standards for the Product Offerings we provide to you. We will test the DR or HA solution and related plan at least once annually. In addition, the solution and related plan will ensure:

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

ii) we can restore the availability and access to Customer Content in a timely manner in the event of a physical or technical incident; and

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

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

2. Information Security Framework

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

b) Security Roles and Responsibility. Jamf personnel, contractors, and agents who provide Product Offerings will have confidentiality agreements with Jamf.

c) Risk Management. We will perform appropriate information security risk assessments as part of an ongoing risk governance program with the following objectives:

i) recognize risk;

ii) assess the impact of risk;

iii) where risk reduction or mitigation strategies are identified and implemented, effectively manage the risk with recognition that the threat landscape constantly changes.

3. Human Resource Security

a) Security Training. We will provide appropriate security awareness, education, and training to all our personnel and contractors who have access to the Product Offerings we provide you.

b) Background Screening. We will ensure that background checks have been performed on personnel who are part of teams managing our hosting infrastructure. Additionally, we will perform background checks on our personnel or agents who are assigned to provide Product Offerings at your premises. We will perform background checks in accordance with applicable law and our background screening policies and procedures. We will only allow individuals who have passed background checks to provide Product Offerings at your premises or be part of teams managing our hosted infrastructure.

4. Asset Management

a) Asset Inventory.

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

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

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

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

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

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

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

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

b) Security of Software Components. We agree to appropriately inventory all Software components (including open-source software) used with the Product Offerings. We will assess whether any components have any

security defects and/or vulnerabilities that could lead to unauthorized disclosure of Customer Content. We will perform an assessment prior to delivery of, or providing you access to, the Product Offerings and on an ongoing basis during the term of the Agreement. We agree to remediate any security defect or vulnerability we detect in a timely manner.

5. Access Control

a) Policy. We will maintain an appropriate access control policy that is designed to restrict access to Customer Content and Jamf assets to authorized personnel, agents, and contractors. All references to user accounts and passwords in this Section 5 relate only to Jamf's users, user accounts, and passwords. Section 5 does not apply to your access to and use of the Product Offerings, your user accounts, or your passwords.

b) Authorization.

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

ii) We will maintain and update records of employees and contractors who are authorized to access systems that are involved in providing Product Offerings to you and review such records at least quarterly. Administrative and technical support personnel, agents, or contractors will only be permitted to have access to such data when required and only if they comply with our applicable technical and organizational measures.

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

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

c) Authentication.

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

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

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

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

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

d) Data-processing Equipment.

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

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

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

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

6. Cryptography

a) We will maintain policies and standards regarding the use of cryptographic controls that we implement to protect Customer Content. Such protections will include the pseudonymization and encryption of Personal Data, as further detailed below in Section 9. We will implement Industry Standard key management policies and practices designed to protect encryption keys for their entire lifetime.

7. Physical and Environmental Security

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

b) Protection from Disruptions. We will use reasonable efforts, and if within our control, protect equipment from power failures and other disruptions caused by failures in supporting utilities.

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

8. Operations Security

a) Operations Policy. We will maintain appropriate operational and security operating procedures and we will make them available to all Jamf personnel who require them.

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

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

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

e) Encryption of Data. We will deploy encryption solutions with no less than 256-bit Advanced Encryption Standard ("**AES**") encryption.

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

9. Communications Security

a) Information Transfer.

i) For Hosted Services, Customer Content is encrypted in-transit to the Hosted Services and maintained in encrypted storage. We will use Industry Standard encryption to encrypt Customer Content.

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

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

b) Security of Network Services. We will ensure that Industry Standard security controls and procedures for all network services and components are implemented whether such services are provided in-house or outsourced.

c) Intrusion Detection. We will deploy intrusion detection or intrusion prevention systems for all systems used to provide Product Offerings to you to provide continuous surveillance for intercepting and responding to security events as they are identified and we will update the signature database as soon as new releases become available for commercial distribution.

d) Firewalls. We will have appropriate firewalls in place to only allow documented and approved ports and services to be used. All other ports will be in a deny-all mode.

10. System Acquisition, Development, and Maintenance

a) Workstation Encryption. We will require hard disk encryption of at least 256-bit AES 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) We will maintain and implement secure application development policies, procedures, and standards that are aligned to Industry Standard practices such as the SANS Top 25 Security Development Techniques or the OWASP Top Ten project.

ii) All personnel responsible for secure application design, development, configuration, testing, and deployment will be qualified to perform the Product Offerings and receive appropriate training regarding our secure application development practices.

c) System Hardening.

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

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

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

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

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

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

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

independent third-party penetration test and attest to the fact that we maintain a process to address findings.

11. Jamf Relationships

a) If we use a third-party application or service to provide the Product Offerings, our contract with that third-party vendor must clearly outline security requirements for the third-party vendor consistent with the security requirements of this Information Security Schedule. In addition, we will ensure clearly defined service level agreements with the third party are in place.

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

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

12. Information Security Breach Management

a) Security Breach Response Process

i) A "**Security Breach**" means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure, or access to Customer Content that we transmit, store or otherwise process in providing the Product Offerings.

ii) We will maintain a record of Security Breaches noting the description of the Security Breach, the applicable time periods, the impact, the person reporting it, to whom the Security Breach was reported, and the actions taken to remediate the Security Breach.

iii) If there is a Security Breach, we will:

1) notify you of the Security Breach by contacting your point of contact in writing promptly, and in any event within 72 hours following the discovery of the Security Breach;

2) promptly investigate the Security Breach;

3) promptly provide you with all relevant detailed information about the Security Breach; and

4) take reasonable steps to mitigate the effects and to minimize any damage resulting from the Security Breach. All Security Breach information we provide to you is Confidential Information.

13. Security Compliance and Assessment

a) SSAE18 SOC 2 Reports (or equivalent). During each calendar year, we will obtain, at our cost, a SSAE18 SOC2 Type II report (or equivalent) related to the provision of certain Hosted Services and conducted by an independent public auditing firm.[1] The minimum scope of these reports will be the Trust Service Principles of Security (also known as the Common Criteria). We 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 your written request, no more than once annually, Jamf will provide a copy of the SSAE18 SOC2 Type II and Type I reports (or equivalent) to Customer. The reports are Jamf's Confidential Information.

b) ISO 27001. We will maintain and operate an Information Security Management System that conforms to the requirements of ISO/IEC 27001:2022 or its equivalent successor standard.[2] In addition, we have obtained and will maintain an ISO 27701 (Privacy Information Management System) certification.

c) Customer Security Assessment. Upon your reasonable request, but no more than once annually, we will complete, in a timely and accurate manner, an information security questionnaire you provide to verify our compliance with this Information Security Schedule ("**Security Assessment**"). If after completion of the Security Assessment, you reasonably determine, or in good faith believe, that our security practices and procedures do not meet our obligations under the Agreement or this Information Security Schedule, then you

will notify us of the perceived deficiencies. We will evaluate such perceived deficiencies and engage you (as necessary) to determine if such deficiencies are actual deficiencies in our security practices and procedures. If we deem any perceived deficiencies you identified to be deficiencies caused by your use of the Product Offerings, we will provide reasonable technical support to assist you in appropriate use of the Product Offerings to remediate such deficiencies. If we confirm that perceived deficiencies you identified are deficiencies in our security practices and procedures, we will, without unreasonable delay:

i) correct such deficiencies at our own expense; and

ii) provide you or your duly authorized representatives, with reasonable documentation and information confirming the remediation of such deficiencies. This documentation is our Confidential Information.

d) Security Issues and Remediation Plan. If we confirm that security issues you identified during a Security Assessment are security issues with our security practices and procedure, we will assign such security issues a risk rating and an applicable timeframe to remediate based upon risk. We will remediate the security issues attributable to our security practice and procedures within applicable remediation timeframes. If we fail to remediate any of the high or critical rated security issues within the stated remediation timeframes, you have the right to terminate the Agreement for material breach immediately upon written notice to Jamf.

[1] There are two exceptions. We currently have a SOC2 Type I report dated March 31, 2025 for Jamf Pro hosted on Microsoft Azure. In addition, the optional Jamf Manager for Android console that is available with the Jamf for Mobile Product Offering does not yet have a SOC 2 report, but it is anticipated that it will have one by the end of 2026.

[2] Jamf Pro hosted on Microsoft Azure and the optional Jamf Manager for Android console that is available with the Jamf for Mobile Product Offering are not covered by our ISO 27001 certification. We anticipate bringing Jamf Pro hosted on Microsoft Azure into scope for our 2026 ISO 27001 certification. It is anticipated that Jamf Manager for Android will obtain ISO 27001 certification by the end of 2026.