# Information Security Schedule

This information security schedule ("**Information Security Schedule**") is subject to the terms and conditions of the Jamf Software License and Services Agreement or other license agreement between Customer and Jamf to which it is attached (the "**Agreement**"). For the purposes of this Information Security Schedule, Jamf shall ensure that its third-party providers, suppliers, agents, and subcontractors that provide Services to Customer comply 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. Jamf may modify this Information Security Schedule from time-to-time for consistency with Jamf's organizational security measures. To the extent this Information Security Schedule is modified, any such modifications will not materially degrade the levels of protection afforded under this schedule.

Jamf shall implement appropriate technical and organizational security measures based on Industry Standards and Data Protection Laws. "**Industry Standard**" means those commercially reasonable security measures designed to ensure the security of the Software and Services provided to Customer by Jamf. Such Industry Standard technical and organizational security measures include 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. Further, Jamf 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 Customer in its business operations

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 and Measures**

    a) Policies. Jamf's information security policies will be documented and approved by Jamf's senior management.

    b) Review of the Policies. Jamf's information security policies will be reviewed by Jamf at least annually, or promptly after material changes are made to the policies to confirm applicability and effectiveness. Jamf will not make changes to the policies that would materially degrade Jamf's security obligations.

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

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

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

        ii) Jamf's ability to restore the availability and access to Customer Content in a timely manner in the event of a physical or technical incident; and

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

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

2. **Information Security Framework**

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

    b) Security Roles and Responsibility. Jamf personnel, contractors and agents who are involved in providing Services will be subject to confidentiality agreements with Jamf.

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

i) recognize risk;

ii) assess the impact of risk;

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

3. **Human Resource Security**

a) Security Training. Jamf will provide appropriate security awareness, education, and training to all Jamf personnel and contractors with access to the 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 will be performed on Jamf personnel or agents assigned to provide Services at Customer's premises. Jamf will perform background checks in accordance with applicable law and Jamf's background screening policies and procedures. Only individuals who have passed background checks will be allowed by Jamf to provide Services at Customer's premises or be part of Jamf's teams managing Jamf's hosted infrastructure.

4. **Asset Management**

a) Asset Inventory.

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

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

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

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

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

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

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

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

b) Security of Software Components. Jamf agrees to appropriately inventory all Software components (including open-source software) used with Jamf's Software and 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. Jamf will perform such assessment prior to delivery of, or providing Customer access to, Jamf's Software and Services and on an on-going basis thereafter during the term of the Agreement. Jamf agrees to remediate any security defect or vulnerability it detects in a timely manner.

5. **Access Control**

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

b) Authorization.

i) Jamf will maintain user account creation and deletion procedures for granting and revoking access to all assets, Customer Content and all Jamf internal applications while providing Software and 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 Software and 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; provided, such personnel, agents or contractors comply with applicable Jamf technical and organizational measures.

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

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

c) Authentication.

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

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

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

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

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

d) Data-processing Equipment.

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

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

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

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

6. **Cryptography**

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

7. **Physical and Environmental Security**

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

b) Protection from Disruptions. Jamf will use reasonable efforts, and, to the best of Jamf's ability and to the extent within Jamf's control, protect equipment from power failures and other disruptions caused by failures in supporting utilities.

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

8. **Operations Security**

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

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

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

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

e) Encryption of Data. Encryption solutions will be deployed with no less than 256-bit Advanced Encryption Standard (AES) encryption.

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

9. **Communications Security**

a) Information Transfer.

i) With respect to Jamf's Hosted Services, Customer Content is encrypted in-transit to the Hosted Services and maintained in encrypted storage. Jamf will use Industry Standard encryption to encrypt Customer Content.

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

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

b) Security of Network Services. 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. Jamf will deploy intrusion detection or intrusion prevention systems for all systems used to provide Services to Customer to provide continuous surveillance for intercepting and responding to security events as they are identified and update the signature database as soon as new releases become available for commercial distribution.

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

10. **System Acquisition, Development and Maintenance**

a) Workstation Encryption. Jamf will require hard disk encryption of at least 256-bit Advanced Encryption Standard (AES) on all workstations and/or laptops used by personnel, contractors, and agents where such personnel are accessing or processing Customer Content.

b) Application Hardening.

i) Jamf will maintain and implement secure application development policies, procedures and standards that are aligned to Industry Standard practices such as the SANS Top 25 Security Development Techniques or the OWASP Top Ten project.

ii) All personnel responsible for secure application design, development, configuration, testing and deployment will be qualified 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 (at least quarterly) access reviews for system administrators for all supporting systems requiring access control.

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

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

d) Infrastructure Vulnerability Scanning. Jamf will scan its internal environment (e.g., servers, network devices, etc.) related to the Services monthly 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 no later than 30 days after discovery.

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

f) Penetration Tests and Security Evaluations of Websites. Jamf will perform a comprehensive penetration test and security evaluation of all systems and websites involved in providing 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 of discovery. Upon Customer's written request, but no more than once per year, Jamf will provide an assertion statement to validate the completion of the independent third-party penetration test and attest to the fact that Jamf maintains a process to address findings.

11. **Jamf Relationships**

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

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

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

12. **Information Security Breach Management**

a) Breach Response Process

i) A "**Security Breach**" shall mean a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure, or access to Customer Content (which may or may not contain Personal Data) transmitted, stored or otherwise processed by Jamf in the performance of Services.

ii) Jamf 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) In the event of a Security Breach, Jamf will:

1) notify the Customer of the Security Breach 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 Breach;

2) promptly investigate the Security Breach;

3) promptly provide Customer 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 provided to Customer shall be deemed to be Confidential Information.

13. **Security Compliance and Assessment**

a) SSAE18 SOC 2 Reports (or equivalent). Except for Jamf Pro purchased through the Microsoft Marketplace and hosted on Microsoft Azure, during each calendar year, Jamf will obtain, at Jamf's cost, a SSAE18 SOC2 Type II report (or equivalent) related to the provision of certain Services and 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. The report is Jamf's Confidential Information.

b) ISO 27001. Except for Jamf Pro purchased through the Microsoft Marketplace and hosted on Microsoft Azure, Jamf shall maintain and operate an Information Security Management System that conforms to the requirements of ISO/IEC 27001:2013 or its equivalent successor standard.

c) 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, 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.

Such documentation will 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 Services, Jamf shall provide reasonable technical support to assist Customer in appropriate use of the Services to remediate such deficiencies.

d) 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, Jamf will assign such security issues a 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.