Jamf Contract Documents
Frequently Asked Questions ("FAQ")

Thank you for reviewing Jamf's Software License and Services Agreement ("**SLASA**") and related documents. We hope that this FAQ provides you an overview of Jamf's Product Offerings and will be useful as you review the SLASA. This FAQ is for informational purposes only, is not legal advice, and will not become part of your contract with us. Capitalized terms used, but not defined in this FAQ, are defined in the SLASA or Jamf AI Addendum.

What is Jamf?

Jamf is a software company that provides a comprehensive suite of management and security solutions that enable customers to seamlessly manage and protect their Devices. Jamf is the standard for managing and securing Apple Devices in the workplace. As of the date of this FAQ, we have approximately 76,000 customers worldwide, including businesses, schools, and government entities.

What is the SLASA and how does it work with Jamf's other contract documents?

The SLASA is the main agreement between Jamf and its customers. The SLASA governs our provision of, and your use of, Jamf's Product Offerings (Software, Hosted Services, training, Standard Technical Support Services, optional professional services, etc.). The SLASA works with an Order or Quote, which will list the Product Offering(s) you are purchasing. Additionally, the SLASA governs any SOWs for services Jamf provides. A few documents are incorporated into the SLASA by reference, including the Standard Technical Support Description, Documentation, Service Level Agreement, Information Security Schedule, and Data Processing Agreement for Jamf Customers ("**DPA**"). You may view all these documents in the Jamf Trust Center.

Are any Jamf products not covered by the SLASA?

Yes. Jamf Executive Threat Protection and DataJar offerings have separate terms. In addition, Jamf recently acquired a company called Identity Automation ("**IA**"). The IA products will remain on separate IA terms for the time being.

Does the SLASA govern public education customers?

Yes. However, we recognize that certain public education institutions may be subject to laws, rules, and regulations that may impose additional restrictions on them when they contract with private businesses and that prevent them from agreeing to certain contractual terms. For these customers, we have the Education Customer Addendum, which amends the SLASA to align with those legal requirements and enables public education customers to purchase Jamf's Product Offerings under the SLASA. The Education Customer Addendum can be found in the Trust Center and may only be signed by public education institutions.

Where can I learn about the Product Offerings we are buying?

The Quote will identify the Product Offerings you are purchasing. An SOW will include a description of service engagements, such as onboarding services. The features and functionality of Product Offerings are set forth in the Documentation. If you have specific questions about the Product Offerings, please contact your Jamf sales representative.

Can I test the Software?

Yes. We offer free trials of our Software. You can request a trial on Jamf's website. The SLASA governs your use of Trial Offerings.

How does Jamf license Software?

Most customers license our Software as a Hosted Service for a Subscription Term. We provide fully functional enterprise cloud applications through the Internet. Customers access their hosted deployment on servers provided and maintained by Jamf. Some customers deploy the Software on-premise within their own environment on their own hardware for a Subscription Term. With an on-premise deployment, the customer is responsible for downloading and updating the software and maintaining all other infrastructure, hardware, and software needed to use it.

What is Jamf's pricing methodology?

Many of our Product Offerings are offered on a subscription basis at a price based on number of Devices and/or Users. During the Subscription Term specified in a Quote or Order, the fee may not be reduced or increased. Some Product Offerings have one-time-charge fees.

What happens if a customer reduces the number of Devices being managed during the Subscription Term?

We cannot accommodate a customer's request for a refund of prepaid fees based upon a reduction in the number of Devices and/or Users during the Subscription Term, regardless of the reason for such reduction (customer downsizing, customer acquired by another entity, etc.). However, when customers "true-up" with Jamf at renewal, fees may be reduced for future Subscription Terms if the number of Devices or Users have been reduced. If a customer adds Devices and/or Users during the Subscription Term, the customer will need to pay additional fees associated with that increase.

Does Jamf provide support to customers?

Yes. As noted in Section 5 of the SLASA, we provide customers with Standard Technical Support Services at no additional charge. Jamf's Standard Technical Support Description can be found in the Trust Center. We also offer optional premium support services, which you may choose to purchase.

Does Jamf offer an uptime commitment for Hosted Services?

Yes. Our service level commitment for the Hosted Services is set forth in the Jamf Service Level Agreement ("**SLA**"), which is referenced in the SLASA. Since Jamf has the same operational business model for our entire customer base, the SLA cannot be modified on a customer-by-customer basis.

What kind of Customer Content will be hosted by Jamf?

It depends. Customers decide what Customer Content to enter into the Software. Typically, a Customer's IT administrator will determine what information to provide to Jamf when configuring the Software to manage and secure Devices. This is usually directory-type information, such as Device IDs, that would contain minimal Personal Data. The DPA sets out categories of Personal Data that customers may enter into the Software (Schedule 1). We do not monitor or control the information that customers enter. Importantly, we do not access customer systems or require sensitive information like financial data or health data. In fact, the SLASA explicitly states that customers will not directly provide us with those types of information (see Section 10 d)ii)).

How does Jamf protect Customer Content?

Our Information Security and Compliance teams are dedicated to delivering and maintaining a comprehensive security and data privacy program that protects the data of all customers and have achieved various certifications that show our commitment to security and privacy (see next question). We treat all Customer Content as confidential. We only use Customer Content as necessary to provide the Product Offerings and only in accordance with the SLASA (see Section 17). With Jamf's standard Hosted Services, Customer Content is encrypted in-transit to Jamf's Hosted Services and stored encrypted at-rest. We provide employees security training and ensure that employees with access to Customer Content understand the confidential nature of it. In addition, all Jamf personnel with access to Personal Data are committed to confidentiality as part of their employment with Jamf. You can learn more about Jamf's security program and read our Information Security Schedule in Jamf's Trust Center.

Does Jamf have any security or privacy certifications?

Yes. As of the date of this FAQ, we have achieved and maintain several security and privacy certifications:

- We have ISO 27001 and ISO 27701 certifications for its Product Offerings (except for Jamf Pro hosted on Microsoft Azure and the optional Manager for Android that is part of Jamf for Mobile).
- We have a SOC 2 Type II report for most of our Product Offerings (except for Manager for Android) and a SOC 2 Type 1 report for Jamf Pro hosted on Microsoft Azure.
- We have achieved StateRAMP Authorized status for Jamf Pro and Jamf School.

- We are certified under the Data Privacy Framework and listed on the U.S. Department of Commerce's Data Privacy Framework Program List.

Learn more and request copies of Jamf's compliance documents through Jamf's security portal.

How does Jamf address customer data privacy concerns?

We know that data privacy is important to our customers and take several measures to address those concerns. First, we have a robust **DPA**, which is incorporated into the **SLASA** by reference (see Section 5 g)). The DPA ensures alignment with global Data Protection Laws and includes information and commitments such as:

- Compliance with the General Data Protection Regulation by including and implementing required contractual provisions.
- Incorporation of the EU Standard Contractual Clauses, UK International Data Transfer Addendum and Swiss Standard Contractual Clauses for lawful transfers of personal data from EEA, United Kingdom, and Switzerland to countries without an adequacy decision.
- Provisions aligned with the California Consumer Privacy Act, as amended by the California Privacy Rights Act of 2020.
- The technical and organizational security measures we have implemented to protect Personal Data are set out in Schedule 3.
- How our Sub-Processors are contractually obligated to meet the same data protection obligations that we provide to our customers.

Please see our DPA FAQ for more information.

We use a Privacy by Design approach in our internal processes, including product design and development, vendor selection and management, and around our Hosted Services. Our commitment to this approach allows us to comply with our legal obligations to our customers and proactively identify, evaluate, and implement full lifecycle protection over new Personal Data collection and use cases and any changes to existing collection and use practices. We have also achieved and maintain an ISO27701 (Privacy Information Management System) certification, which shows our commitment to handing and securing customer Personal Data.

Further, we assist customers with responding to Data Subject requests and conducting data protection impact and transfer impact assessments. For more information, please see our Data Transfer Impact Assessment document.

Can Jamf agree to customer-specific security/privacy requirements?

To ensure that we consistently meet our obligations under Data Protection Laws, we cannot agree to individual customer security or privacy policies. Like many global software providers, we need to maintain a consistent and comprehensive set of security and data privacy policies to ensure appropriate protections and consistency for all customers. Our ability to provide a consistently high level of service relies on the standardization of our processes, including security/data privacy methodologies. We do not agree to individual customer security or privacy policies because they are not tailored to our practices and it is not practical to do so in a fully automated environment that is designed to always run on the latest version of our code base. Our Information Security Schedule, which details our security controls, is incorporated by reference in the SLASA (see Section 5 f)).

Will Jamf permit customers to audit Jamf?

To maintain the security of our Product Offerings and facilities, we prefer not to host audits. To provide customers with objective evidence that we maintain security controls, we engage an independent third party to produce SOC 2 audit reports on an annual basis. Those reports are based on the Trust Service Principles of Security (also known as the Common Criteria). If a customer wants to conduct its own audit or applicable law requires us to allow an audit, we will reasonably cooperate by providing relevant information, responding to security assessments, and sharing a copy of our current SOC 2 report, provided appropriate confidentiality obligations are in place. As noted in the Information Security Schedule, we will complete customer information security questionnaires to verify compliance with the Information Security Schedule no more than once annually. You may request access to Jamf's SOC 2 reports on our Security Portal.

How do customers get data back when their relationship with Jamf ends?

Customers always own their Customer Content (see SLASA, Section 8). Customers can access the Customer Content stored in the Hosted Services at any time during the term of the SLASA. Upon termination of our relationship, you can request a backup that contains your Customer Content as noted in the [SLA](#).

How does Jamf use Generative Artificial Intelligence (AI) within its Product Offerings?

Jamf has integrated AI as Optional Features within Product Offerings to enhance customer experience and operational efficiency. For example, customers may now access Jamf's AI Assistant within their hosted deployment of Jamf Pro. Jamf's AI Assistant is an AI chatbot that answers technical questions and helps IT admins gain insights about their Devices, explain configurations, and search Device data. Optional Features with AI, like Jamf AI Assistant, are disabled by default and customers must opt-in to use them. If we offer standalone AI Product Offering(s), we will identify them in a Quote or Documentation. In other words, we will make sure our customers know when they are enabling AI with Jamf. Jamf does not use Customer Input or Customer Output to train, develop, improve, or refine any AI Model within any Product Offering. Jamf's AI Addendum, available on the Trust Center, governs customers' use of AI with any Optional Feature or Product Offering.

Last Updated: June 13, 2025