Foxit

# FOXIT ESIGN SECURITY OVERVIEW

WHITE PAPER

# TABLE OF CONTENTS

Security is the foundational core of Foxit eSign. As with all our products, Foxit eSign was developed and designed with security at the top of mind.

This document gives an overview of the security technologies, policies, and practices used by Foxit eSign that protect your documents and data, including information that enables you to make security configurations to meet your company's unique risk management and compliance requirements.

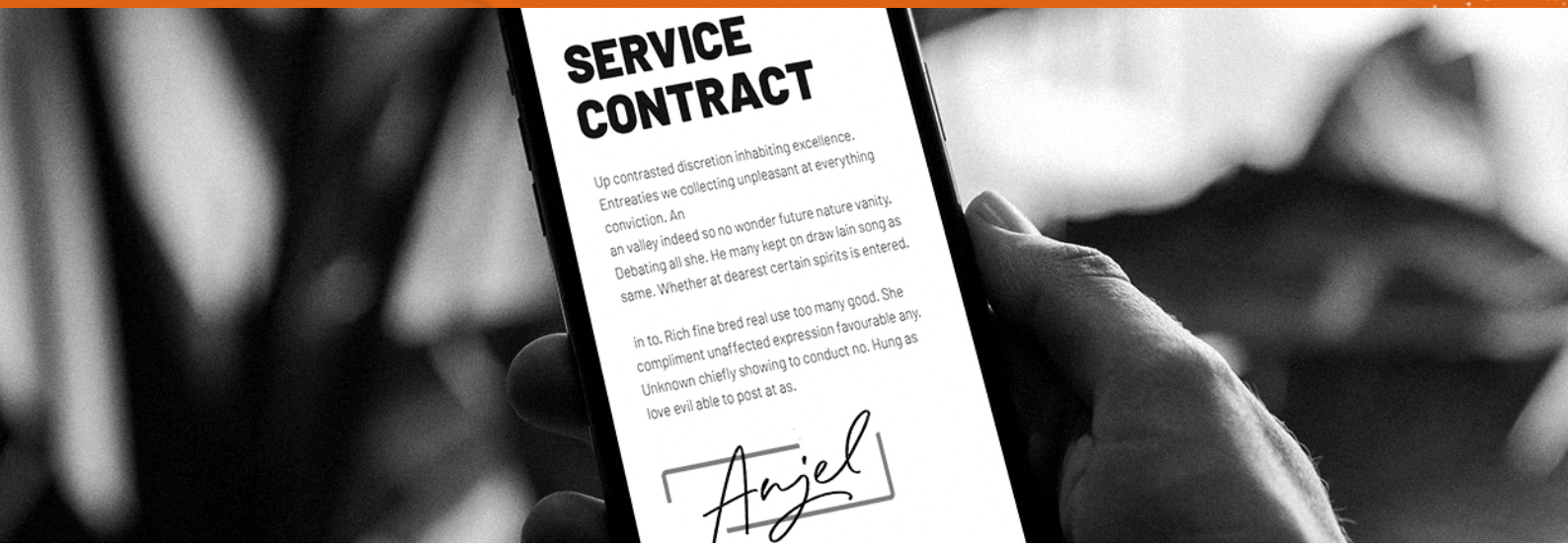
This document also identifies several regional regulations which Foxit eSign strictly complies with to ensure you're able to deploy.

# DYNAMIC SECURITY AND ENCRYPTION

Foxit eSign is SOC 2 Type 2 certified. It is regularly audited by independent industry auditors to ensure strict compliance with the 5 Trust Service Principles. The following outlines the service commitments Foxit eSign makes to user entities, the laws and regulations that govern the provision of its electronic signature and productivity management services, and the financial, operational, and compliance requirements that Foxit eSign has established for its services.

**Security** - Protection of your data from unauthorized access and viewing through our system

- Foxit eSign commits to employing administrative and technical measures in accordance with applicable industry practices to protect the system and prevent the accidental loss or unauthorized access, use, alteration, or disclosure of customer data under its control during each order term.
- All data transmitted between our systems and users is protected using transport layer security (TLS) and HTTP strict transport security (HSTS).
- Access to environments that contain customer data requires a series of authentication and authorization controls, including multi-factor authentication (MFA).




**Availability** - Ensuring our software is available as needed and agreed upon

- Foxit eSign commits to using commercially reasonable efforts to make the system available for access and use by end users over the internet at least 99.95% of the time as measured over the course of each calendar month, excluding unavailability as a result of scheduled maintenance. However, Foxit eSign has maintained an uptime of over 99.99% over the past 5 years.

**Confidentiality** – Keeping your data protected, private, and confidential

- Foxit eSign commits to protecting confidential information against any unauthorized use or disclosure to the same extent that we protect our own confidential information. In no event will we use less than a reasonable standard of care to protect such confidential information.
- We use confidential information solely for the purpose for which it was disclosed.

**Processing Integrity** – All system processing is complete as authorized, accurate, and prompt

- Foxit eSign's system requirements and practices include application programming interface (API) performance monitoring controls, monitoring of data intakes, and maintaining policies and procedures that aid in the prevention, detection, and correction of data processing errors.

**Privacy** – Strict adherence to Generally Accepted Privacy Principles (GAPP) which dictates all personal information is retained, collected, used, disclosed, and destroyed as established in our privacy notice

- Foxit eSign commits to protecting personally identifiable information against any unauthorized use or disclosure to the same extent that we protect our own personally identifiable information. In no event will we use less than a reasonable standard of care to protect such personally identifiable information.
- We use personally identifiable information solely for the purpose for which it was disclosed.

Additionally, your documents are locked and secured with industry-grade 256-bit encryption and paired with strict firewall controls – all incoming and outgoing traffic is monitored and forced to abide by our network's strict security rules. Foxit eSign provides end-to-end protection by encrypting the data in rest and in motion.

# VISIBILITY

Foxit eSign offers customers full visibility controls so that you can decide who can see and access your organization's documents. This includes the following controls:

- Customize visibility features to limit document viewing to only those designated recipients you choose.
- Restrict account user visibility with features like Secured Field Access, which gives only approved users access to information in secured fields.
- Control access to information by designating different user levels and sharing settings.
- Assign managers to regular users and admins, ensuring easy monitoring and subordinate document usage.

# AUDITING

Knowing exactly where your documents are and where they've been is a crucial component of security and compliance. Foxit eSign provides detailed auditing reports and features so customers can stay informed about their document workflows.

- Detailed audit trails track each document by IP address and timestamp, so you have full knowledge of where, when, and who is viewing your documents at all times.
- Certificate of completion provided for every document with the associated IP address, email address, timestamp, and name of signer.
- Track the deletion of documents and folders each step of the way. Our delete folder history allows you to see where, when, and by whom any folder was deleted.

# DATA CENTERS

It's important that our customers understand where their documents are being stored. We also understand the importance of local data residency for our customers. To that end, Foxit eSign uses Amazon Web Services (AWS) data centers. Our data centers are designed to anticipate and tolerate failure while maintain service levels and access to data centers is regularly reviewed.

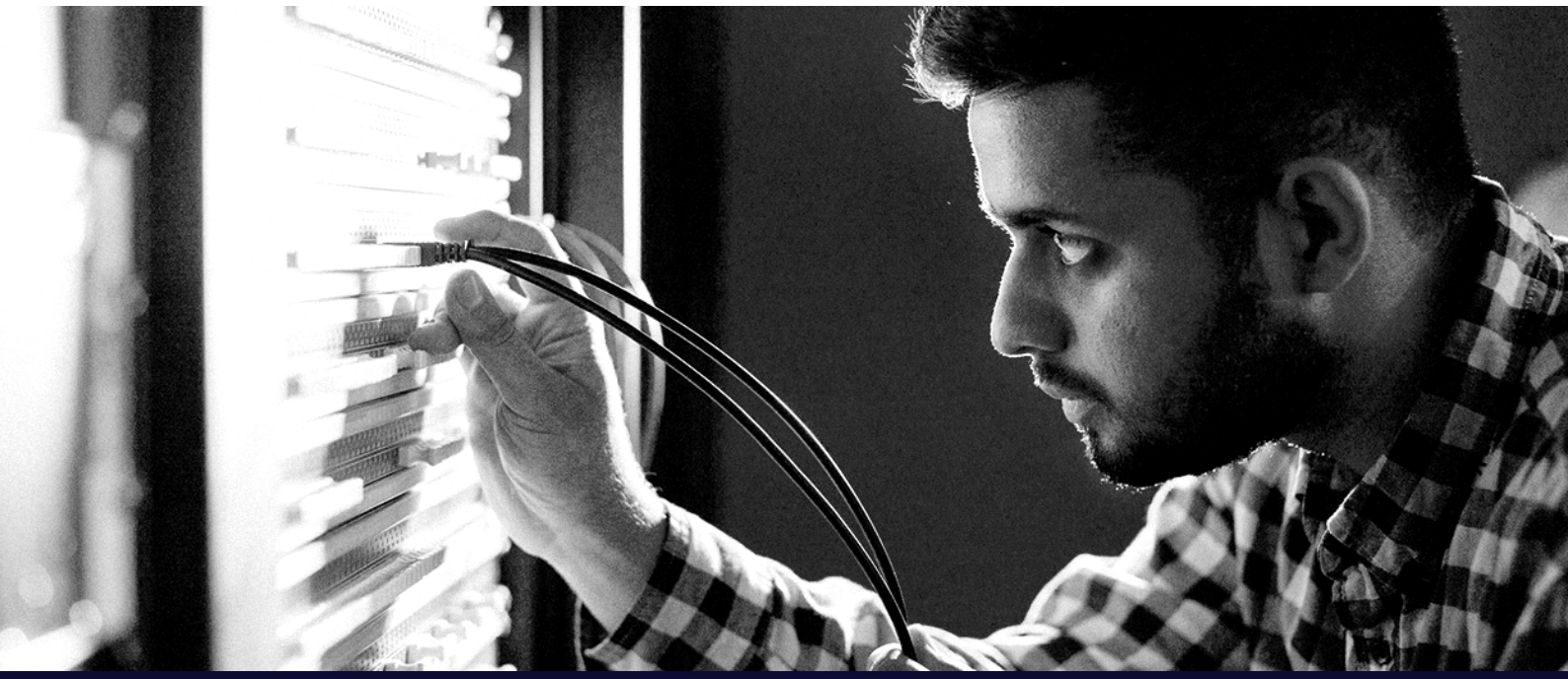
**Data Location** – Foxit eSign maintains trusted US and European data centers with SSAE16 facilities that are SOC 2 Type 2 compliant and PCI compliant. In the United States, applications are hosted on the AWS platform and primarily operate in facilities located in N. Virginia (US East), Ohio (US East), and Northern California (US West). In Europe, data centers are located in Frankfurt, Germany. In Canada, data centers are located in Montreal. These facilities are locked and monitored around the clock to ensure that your data is only stored on the safest and most secure servers.

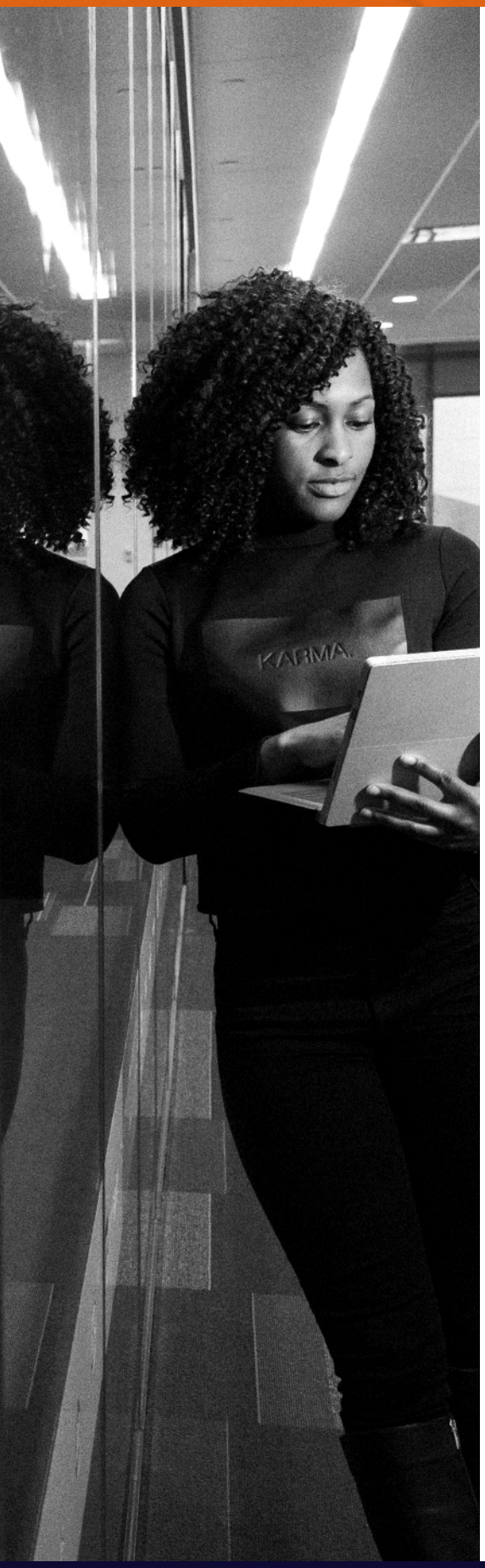
**Data Residency** – When signing up for a Foxit eSign account, your account will be assigned to your local region for server storage. We also provide our customers with the option to choose which data center they would like to store their documents. Finally, customers are given full control over who accesses their documents.

# BUSINESS CONTINUITY/DISASTER RECOVERY

Foxit eSign data and files is stored in high availability servers and managed databases and is also synced real time to the reporting and backup encrypted databases and file servers. In case of emergency, systems can be brought online from the backup or from another availability zone.

Additionally, Foxit eSign maintains robust system capacity and infrastructure monitoring for performance and availability. Backups are performed in near-real-time and are largely a continuous process. Business continuity and disaster recovery planning at Foxit eSign takes into consideration a Business Impact Analysis (BIA), incident handling, contingency, and business continuity plans, which collectively make up the framework for maintaining a continuity and contingency strategy, management and operational plans. Foxit eSign has designed policies and procedures that cover a partial or complete failure of cloud service providers (CSPs).






# DATA RETENTION POLICY

Our data retention policy outlines important guidelines for how long we track and keep your information, and when it is disposed of. Retention policies differ based on the account type. Account type policies are defined as follows:

**Trial Accounts** – Non-paid account documents and related data will be deleted after 30 days unless the account is converted into a paid account by the user.

**Paid Accounts** – Paid account draft documents will be stored in the system for 45 days unless the documents are sent for signing. Paid account users can also configure their own document retention policies for each type of document, including shared, partially signed, executed, canceled and/or expired documents.

Foxit
39355 California Street, Suite 302
Fremont, CA 94538, USA

Sales: 1-866-680-3668
Support: 1-866-693-6948
Or 1-866-MYFOXIT

Support Center
www.foxit.com