CLOUD DOCUMENTS SECURITY WHITE PAPER

WHITE PAPER

TABLE OF CONTENTS

Introduction 3

Account Security 3

Product Security 3

- Development Practice 4
- Foxit Cloud Documents Security Architecture 4
- Acquired Certification 5

Data Security 6

- Static Storage Security 6
- Transport Security 6
- Data Isolation 6
- Data Backup and Failure Recovery 6
- Data Retention Policy 6

Operational Security 9

- Management of Operational Authority 9
- Monitoring and Incident Response 10

Cloud Documents - Q&A 10

INTRODUCTION

We have a professional and leading security team to ensure the security of your data stored in Foxit Cloud Documents. Our security policy mainly covers the following aspects: product security, data security, account security, transmission security, operational security, etc. The security team directs our employees to report suspicious activity by implementing a security incident response mechanism within the company. Our Security Incident Response team has procedures and tools in place to respond to security incidents, and continuously update technology to improve security protection capabilities. We regularly review infrastructure and applications that may affect user data security. Our security team iteratively evaluates new tools to increase the coverage and depth of reviews. We will update the content of this overview while we constantly improve our product security and upgrade product security performance.

ACCOUNT SECURITY

Foxit stores user passwords in encrypted storage with salt, and user login credentials are encrypted in transit using TLS. User passwords must meet complexity requirements as well. Meanwhile, login attempts of the same account are limited to reduce the risk of brute force cracking.

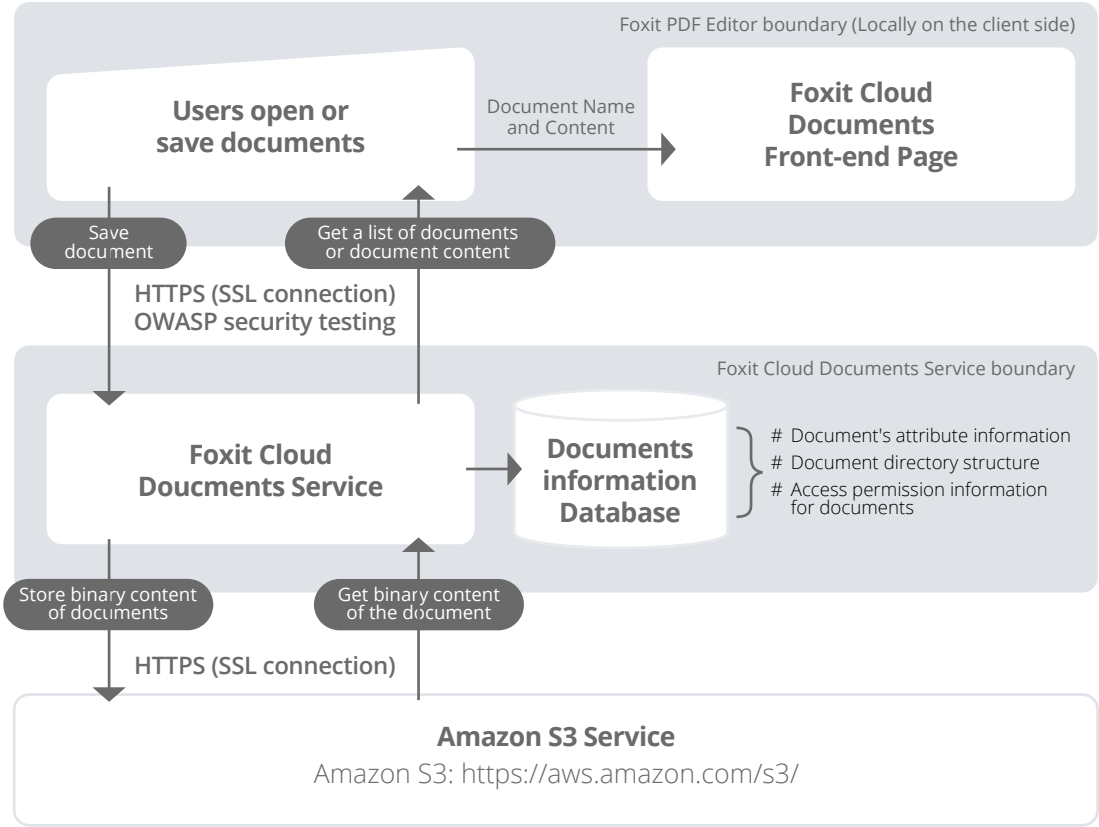
Foxit provides multi-factor authentication for all accounts, which can be enabled in user center. User has options to receive a two-step verification code by email or generated by a local password through time-limited one-time password (TOTP) algorithm applications on their mobile devices. At the same time, we also support universal third-party account (such as Google, Microsoft, Facebook, and LinkedIn) logins to our product.

PRODUCT SECURITY

DEVELOPMENT PRACTICE

Foxit adheres to the security concept of "shifting left", and continuously intensifies the implementation of S-SDLC (Secure Software Development Life Cycle). We improve our product security by introducing necessary and appropriate security activities at all stages of the software development life cycle. These security activities include but not limited to architecture design review, threat modeling, static code scanning, software component analysis, penetration testing, web application vulnerability scanning, image scanning, etc.

FOXIT CLOUD DOCUMENTS SECURITY ARCHITECTURE



The subsequent steps outline the workflow within the Foxit Cloud Documents Security Architecture:

1. Users open documents from Cloud Documents; or save documents to Cloud Documents.

2. The front-end web page (which is embedded in Foxit PDF Editor) calls the Foxit Cloud Documents Service API, obtain the user file directory list and document information (including document binary content) from Cloud Documents; or save the client document to the specified user folder in Cloud Documents.

3. Foxit Cloud Documents Service is a document management system developed by us based on the open-source Apache Chemistry that complies with the OASIS Content Management Interoperability Services (CMIS) specification, which includes data model (Data Model) and service (Services), it also defines the binding of Atom Pub, binding of

Web Services and binding of browser, and includes the protocol of multipart uploading of files in massive size. Cloud Documents service stores user document information in MySQL database, and binary contents are stored in AWS S3 service. Storage is encrypted both in transit (via HTTPS protocol) and at rest.

a. Get user file directory list:
   Based on the user document metadata stored in MySQL, a user file directory list is constructed and returned.

b. Get document binary content:
   First, query the corresponding Amazon S3 storage key from the document ID, then obtain the document binary content from the Amazon S3 service based on the key, and return it to the caller.

c. Save document:
   Based on the incoming directory information and document information (including document binary content), the user document is first created in the corresponding directory and the relevant information is stored in the MySQL database, and then the document binary content is uploaded to the Amazon S3 service through the Amazon S3 service API.

4. Data, privacy, and security

   a. The development of Foxit Cloud Documents complies with OWASP, a rigorously secure programing framework. And it took anti-virus, penetration, and vulnerability tests before releases.

   b. All web APIs are called via the HTTPS protocol, including calls to the Foxit Cloud Documents Service API and the Amazon S3 service API. This ensures the security of document and user's data transmission.

   c. The MySQL databases used in the service are not exposed to the public. It is protected by a firewall and can only be accessed within the internal network.

   d. The Amazon S3 service has its own security standards. For details, refer to: https://aws.amazon.com/s3/.

Microsoft 365 Certified

ACQUIRED CERTIFICATION

Foxit PDF Editor Cloud is certified by Microsoft 365 Teams Apps Security and Compliance program (which demonstrates the application is reviewed with controls from leading industry standard frameworks and has strong security and compliance practices in place to protect customer data) and is SOC2 certified.

DATA SECURITY

We use the AWS S3 service as the storage solution for user uploaded files. Amazon S3 provides a highly durable storage infrastructure for mission-critical and primary data storage. AWS S3 provides 99.999999999% durability and 99.99% availability. We ensure data security with the following specifications:

STATIC STORAGE SECURITY

Amazon S3 encrypts objects before saving them to disk in the data center by default. Objects are then decrypted during download.

TRANSPORT SECURITY

We use industry standard encryption to protect user data in transit, commonly referred to as Transport Layer Security (“TLS”) or Secure Sockets Layer (“SSL”) technology while in transit.

DATA ISOLATION

Cloud documents uploaded by users in each region are stored in S3 buckets corresponding to their specific region. For example, files uploaded by European users are stored in S3 buckets in the European region. Data between regions is isolated.

DATA BACKUP AND FAILURE RECOVERY

The Cloud Documents service is resilient to failures. We have version control to save, retrieve, and restore various versions of documents, which readily recovers data from false operations and application failures. There are complete life cycle rules and backup rules in place.

DATA RETENTION POLICY

Our product holds many different types of documents containing a variety of data, including user details, orders information as well as files. These documents are a vital part of our business, and it is important that we ensure that we protect the documents and information contained in them in order to ensure the smooth running of the business and also to comply with the requirements laid down by law.

The purpose of this policy is to ensure that we only hold documents for as long as necessary and that once they are no longer required they are destroyed in accordance with the procedures laid down in this policy.

This policy supplements our privacy policy and was last reviewed on March 17, 2023.

Who does this Policy apply to?

This policy applies to all users of Foxit Editor Cloud.

What is a Document?

It contains data such as recorded data and uploaded files generated by users using our product.

Retention of Documents

The retention schedule below lists the types of documents that our product holds. We are required by law not to hold documents for any longer than necessary, and therefore we have set retention periods below.

The retention periods are based on time limits set by law for some documents, and where there is no statutory period, we have set the time based on how long we think the document will be required. Once the statutory period has been reached, then the documents should be destroyed unless there is a good reason to keep them (e.g., ongoing legal proceedings). In such events, the Responsible Person should make the final decision on whether documents are retained beyond the minimum retention period.

Destruction of Documents

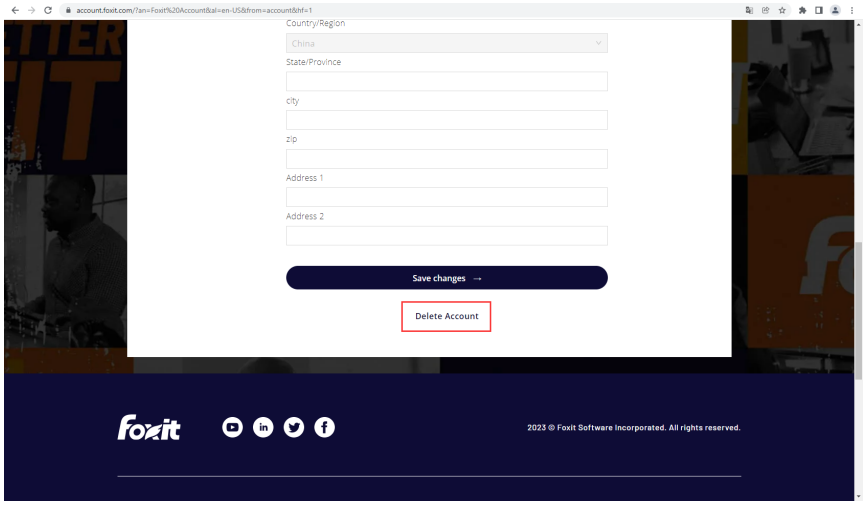
Once the documents have reached their minimum retention period, then they must be permanently destroyed unless there is a good reason to keep them. and the Responsible Person has agreed on a further retention period.

Schedule of Documents

Type of Documents	Description of Document	Retention Period
Foxit Accounts	Online accounts created by the user, contains the name and email of the Microsoft Teams user.	Permanent, unless you actively delete the account.
Orders Database	Order details, including user contact details, credit card information, etc.	Permanent, unless you actively delete the order or account.
Cloud Documents	Files and collaborative content uploaded through the collaboration or cloud documents feature.	Permanent, except in the following cases: 1. You actively delete the document or account. 2. When an enterprise user is removed by the administrator from the enterprise or when the enterprise administrator deletes the enterprise. 3. If the enterprise user's authorization is revoked and the total document size exceeds the 1G limited space, the document will be automatically cleaned up to within 1G after 30 days. 4. When the enterprise subscription expires, the total document size of a single enterprise user exceeds the 1G limit space, the document will be automatically cleaned up to within 1G after 30 days. 5. If your personal subscription expires and the total document size exceeds the 1G limited space, the document will be automatically cleaned up to within 1G after 30 days.
Temporary Documents	Files uploaded by conversion features.	It is executed regularly every day, and files older than two days will be deleted.

Account deletion

To delete your account, go to My Account Profile and scroll down to the bottom of the page.



If you click the 'Delete Account' button to submit a request for account deletion, we will process your request asynchronously in the background. First, we will delete all your data, documents, and subscription records in our system, and finally, we will delete your account information. Once the process is complete, we will notify you via email. After the deletion is completed, the action cannot be reversed.

OPERATIONAL SECURITY

MANAGEMENT OF OPERATIONAL AUTHORITY

All S3 storage buckets are private using ACL-based access policies. We have least-privileged access to allow only specific IPs and IAMs to access bucket resources.

MONITORING AND INCIDENT RESPONSE

S3 protection and Amazon Guard Duty is in place to allow monitoring of object-level API operations, which will identify potential security risks. Amazon CloudTrail is also integrated to record actions taken by users, roles, or other Amazon services.

CloudTrail captures a subset of API calls to Amazon S3 as events, including calls from the Amazon S3 console and code calls to the Amazon S3 API.

CloudTrail events can be delivered to S3 buckets (including Amazon S3 events) continuously for further review if a trail is created. Latest events are still available in CloudTrail console event history even a trail is not created. Information collected by CloudTrail can be used to analyse events such as what requests are made, source IP address of the request, who made the request, when it was made etc.

CLOUD DOCUMENTS - Q&A

Q1 **Data Retention Policy** (how long do we keep documents in the cloud for example when one of the modules that require document upload is used, for example - conversion). What data is being stored and what data is not being stored?

A1 Document uploaded to the Cloud Documents will be kept permanently unless users actively delete the document or account. For details, please refer to Foxit PDF Editor Cloud Data Retention Policy.

However, for those features like Conversion, the original document will be deleted immediately once the conversion is over. The converted documents could also be determined by users whether to be uploaded to Cloud Documents.

Q2 Once a file is deleted from Cloud Documents storage, if there is a backup of that file (on our servers) when is that backup deleted?

A2 Files deleted from Cloud Documents cannot be retrieved or recovered.

Files are backed up daily, and after a day the backed-up files on the server are also synchronized with the user's deletion actions.

Q3 If an account does not renew the subscription, do they instantly lose access to Cloud Documents, or do we allow access for a limited time to the files so they can download/back them up?

A3 Freemium Users - 1GB, Premium Users - 20GB.

When an account subscription expires, if the user's total document size exceeds 1G, we will email the user to renew the subscription or download his documents.

If the user does not renew the subscription within 30 days, the total document size will be cleared to less than 1G (The earliest uploaded documents will be cleaned up first).

Q4 Where is an uploaded document being stored / if it is even stored? Where are our backup servers?

A4 AWS S3, the backup data is in AWS S3. The standby server is in a different region of AWS.

Q5 Can you describe the document **workflow** within the cloud? What happens to the document exactly when it is being uploaded, worked at, sent, and stored?

A5 Refers to Cloud Documents Security White Paper.

Q6 Does data leave the EU zone? If so, which data and why? Are documents stored in the US only?

A6 The file uploaded by the user at which instance will be transferred to the local area of Amazon, which means the data from the EU will be kept in AWS S3 EU. However, the Account Information is stored in the US to support global account login.

Q7 Is this a paid service? What's the document retention policy from the client's standpoint?

A7 No. It is part of the subscription and not an extra add-on.

Q8 Can we turn off the automatic uploads feature for enterprise customers? Otherwise, each employee would need to turn it off.

A8 Enterprises can configure whether to turn Cloud Documents on or off via the Admin Console.

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

© Foxit Software Incorporated. All Rights Reserved.