FLUIX

Security White Paper

March 2023

Table of Contents

Introduction

Fluix Limited is committed to keeping data secure at all times. Businesses and government organizations all over the world trust their everyday workflow to Fluix. Protecting the integrity of the corporate network and the privacy of sensitive data is of utmost concern to any company. **We recognize that security and stability are the two most important choice making factors for our customers.**

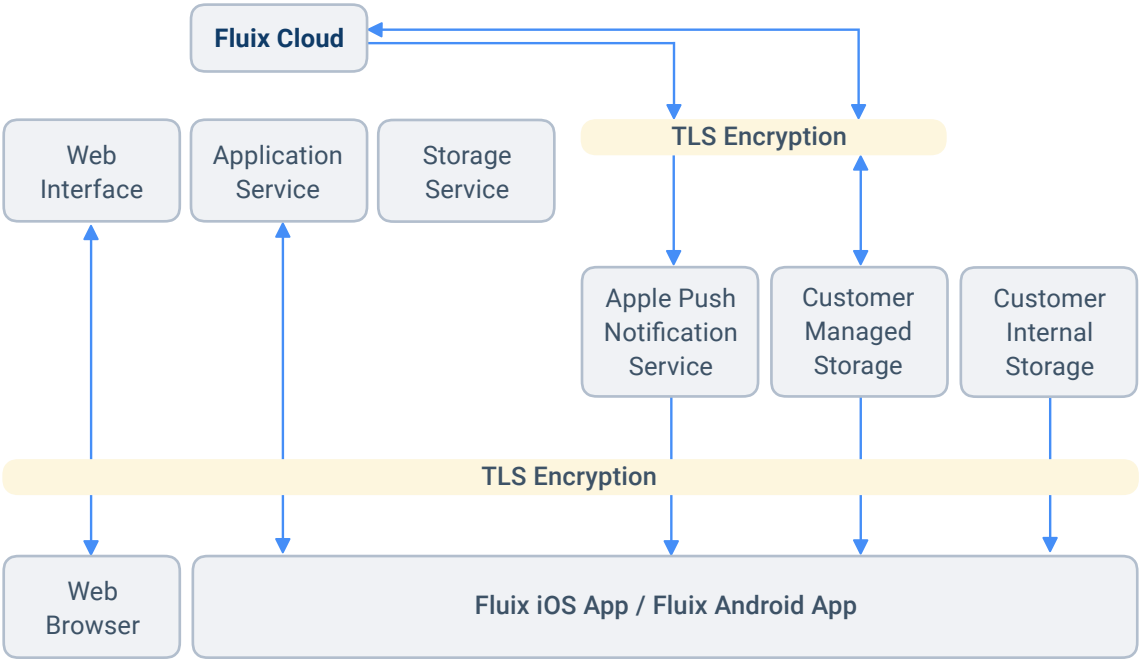
This document dwells on Fluix security infrastructure and policies. In case further questions regarding our security policies arise, please feel free to get in touch with us.

Productivity today literally means the ability of company employees to easily and quickly access and share data from any place, device, and environment. In today's era of globalization and mobility, work is not performed from a single location or computer anymore; rather it takes place anywhere and on any device available. Projects and processes today involve people operating from organizations and locations around the globe. And company IT infrastructure in place should allow data to flow freely where necessary—without sacrificing compliance with corporate policies, control, and overall security.

Using a mobile solution like Fluix involves cloud solutions to make data available on the go and an iOS and Android applications that allows data access. Security is a crucial requirement for both parts of this solution.

The Solution

With the above mentioned taken into consideration, Fluix offers a reliable and manageable solution for document distribution, form filling, data collection, and collaboration.



The Fluix architecture consists of two key components:

1. **Fluix Cloud**
2. **Fluix iOS Application**
3. **Fluix Android Application**

The application communicates with cloud infrastructure to provide secure access to data and take part in the document workflow.

Fluix Cloud

The Cloud infrastructure consists of the following services:

- **Application Service**
  The core cloud component that communicates to the iOS app and handles authentication, authorization, network access configurations, document movement within the workflow, as well as programmatic API access. All operations with data or metadata require prior authentication and authorization.

- **Storage Service**
  Highly durable distributed storage service (AWS S3) which is used to store documents within a workflow, sent via push directly to the application or stored inside built-in storage. Storage service employs strong multi-factor encryption. Each document is encrypted using a unique key. As an additional safeguard, the key itself is encrypted with a master key, which is rotated regularly. All requests to the storage service need to be signed previously by the Application Service.

- **Web Administration Portal**
  Handles user provisioning, user management, policy creation, workflow configuration, sending push messages,& reporting. Company account administrators are authorized to access Web Administration Portal and could create special role-scoped users for specific actions. There are different sets of user permissions that may restrict certain action-specific features.

All data transfers between these services are encrypted in transit, both across the services and between the services as well as the iOS application. See the Encryption section below for information on the types of encryption used.

Fluix iOS Application

Here are some of the highlights of security measures for the Fluix iOS application:

- **Application Policies**
  The company account administrator may ensure the iOS application is more secure by restricting user/group sharing options on the administration portal.

- **Access Control**
  In case the iOS device gets stolen or lost, the company account administrator can revoke access to the application on the web admin portal in real-time.

- **Data Storage**
  The iOS version of Fluix leverages Apple iOS data protection. All data within the Fluix app is constantly encrypted using the AES-256 cipher. Following the principle of least privilege, the application assigns different protection classes to the files, ranging from **Protected Until First User Authentication** (similar properties to desktop full-volume encryption) to **Complete Protection** (encrypting data within 10 seconds after device locked). See the iOS Security Guide for details.

- **Data Transfer**
  All data moved between the server and the application are encrypted. See the Encryption section below for information on the types of encryption used.

- **Software Development Process**
  Changes in various stages of development are tested on a daily basis. The testing process includes both positive and negative testing to ensure the stable and secure operation of the app.

- **Security Testing**
  The application is being regularly tested against mobile OWASP top vulnerabilities and hardened against running on jailbroken devices and decrypting traffic using user-installed TLS certificates.

Fluix Android Application

Here are some of the highlights of security measures for the Fluix Android application:

- **Application Policies**
  The company account administrator may ensure the Android application is more secure by restricting user/group sharing options on the administration portal.

- **Access Control**
  In case the Android device gets stolen or lost, the company account administrator can revoke access to the application on the web admin portal in real-time.

- **Data Storage**
  The Android version of Fluix leverages Android 10+ data protection. All data within the Fluix app is constantly encrypted using the file-based encryption mechanism (FBE). Android application runs in an Application Sandbox. By default, an Android application can only access a limited range of system resources. See the Android Security Guide for details.

- **Data Transfer**
  All data moved between the server and the application are encrypted. See the Encryption section below for information on the types of encryption used

- **Software Development Process**
  Changes in various stages of development are tested on a daily basis. The testing process includes both positive and negative testing to ensure the stable and secure operation of the app.

- **Security Testing**
  The application is being regularly tested against mobile OWASP top vulnerabilities and hardened against running on jailbroken devices and decrypting traffic using user-installed TLS certificates.

Customer Managed Storage

Fluix may be configured to use customer-managed storage (located either on-premises or in the cloud) to store data for online access, two-way synchronization folders, and for the repository with templates.

Fluix supports customer-managed storage that operates industry-standard WebDAV via HTTPS and SFTP protocols.

Additionally, Fluix supports proprietary protocols for connecting to Dropbox, Box, Google Drive, and OneDrive for Business and Sharepoint.

The most recent and secure TLS 1.2 standard is used when connecting to HTTPS resources and cloud services.

Customer Internal Storage

Using the “Internal Workflow” feature, it is possible to configure access to customers’ storage (over WebDAV or SFTP) directly from iOS devices over a VPN.[1]

In this case, the data on customer internal storage is completely inaccessible to the Fluix Cloud. While advanced workflow mechanics are not possible in this case, this solution makes it possible to deploy Fluix for the most data-sensitive use cases.

Server credentials are transferred to mobile devices using 256-bit TLS encryption and the latter is connected to external data storage directly.

Apple Push Notification Service

Apple Push Notification service (APNs for short) is a robust and highly efficient service for propagating information to iOS devices. Each device establishes an accredited and encrypted IP connection with the service and receives notifications over this persistent connection.

Fluix leverages Apple Push Notification Service to notify users about new document arrival or to trigger synchronization within the iOS application.

Being the only way to deliver push notifications to iOS devices, the service is operated by Apple. On the device side of the connection, APNS validates that the connection is with a legitimate device and application.

APNS is never used to deliver documents from the system. Only the text of a push message and the fact that the app requires synchronization get delivered.

[1] setup and configuration of VPN infrastructure is performed by the customer

Product Security & Compliance

Fluix SaaS solution, including Fluix Cloud, Fluix iOS Application and APIs, is one of the main business assets that require robust protection and minimization of cyber security risks.

In this section we provide an overview of different technical and administrative security measures to protect the main business assets.

Fluix Information Security Management System

Fluix has implemented an Information Security Management System based on ISO 27001 to ensure that we properly address information security risks and protect our assets. The ISMS at Fluix is being constantly improved and is getting more mature.

Policies and Procedures

We established a framework of information security policies and procedures to promote principles and guidelines to our employees and third parties. The documents are reviewed at least annually and updated if needed. All of them are approved by top management and shared with the employees who should be aware of them.

Below are some of the core policies:

- Information Security Policy
- Information Classification and Handling Policy
- Access Control Policy
- Business Continuity Policy
- Backup and Data retention Policy
- Security Procedures for IT
- Technical Vulnerabilities Policy
- Password Policy
- Risk Assessment and Risk Treatment Methodology (Standard)
- Information Security Incident Management Policy
- Servers and Cloud Configuration Policy
- Policy on the Use of Encryption
- Secure Development Policy

- Change Control Procedure
- Internal Audit Procedure
- Physical Security Policy
- Supplier Security Policy

Compliance

ISO 27001

Fluix is ISO 27001:2013 compliant and we continually improve our technical, administrative and physical security controls to meet industry best practice.

HIPAA

Fluix meets the requirements from HIPAA standard and in case of requirement from our client, we will be able to sign Business Associate Agreements (BAAs).

Vulnerability Management

Fluix Security and Technical Operations Teams perform regular activities to make sure we eliminate all known technical vulnerabilities in our system components, both exposed to the public and "under the hood". Below are some of the ongoing operations we perform.

Application Security

Fluix developers get regular secure development training on the technologies used for development. We use SAST/DAST tools as well as manual code review to eliminate vulnerabilities and possible logic flaws in our source code.

Infrastructure Security

Since we use AWS as our cloud provider the responsibility for patching is shared between the cloud provider which is responsible for providing us up-to-date services and components without vulnerabilities; and the Fluix team for running vulnerabilities-free servers and other custom components on it. From our side, all infrastructure components that are under our management we patch on a regular basis ensuring we have the latest and supported versions.

Checking Libraries and Software Components

We understand that despite perfect and safe code, an issue in one of the libraries or components our code depends on might lead to compromise of the whole system. Thus within our CI/CD process, we have a series of security checks. And one of the checks is to ensure that there are no vulnerabilities within libraries or other software components we use while developing our application. All findings are timely addressed.

Penetration Tests

Fluix passes regular penetration tests from trusted independent providers to ensure we do not have any security issues in our products. In case of findings, technical teams ensure to have timely follow-up to mitigate them.

Responsible Disclosure Program

To improve overall product security, and to allow a big number of security researchers to analyze Fluix from a security perspective, we launched Fluix Responsible Disclosure Program. As a result, we receive security reports from the ethical hackers regarding the product. Some of the reports pass internal PoC and we take care of them with the highest priority.

Technical Compliance

We check our products' components over best practices and ensure we meet them. We use trusted open-source and commercial tools (as well as native for AWS) to check relevant criteria and benchmarks.

Access Control

When granting access to our employees we strictly follow the 'least privilege' principle. All requested accesses are thoroughly reviewed and if approved, granted to an employee.

Access to Production

Access to the production environment is strictly limited to the minimum number of employees. Access to production is secured with two-factor authentication with the help of a hardware token.

Access Review

Every six months we review existing accesses to Fluix systems and services in use. Production servers, databases, access to cloud service providers, internal and external business services, and systems are in scope of the review.

Two-factor Authentication

All services which we consider critical, mainly systems and services that have access or might impact access to clients' data are protected with two-factor authentication along with advanced password policies. We use hardware tokens from YubiKey as a second factor for those services.

Cloud Environment

Fluix Cloud is deployed at Amazon Web Services (AWS) cloud platform.

AWS operates the global cloud infrastructure that Fluix uses to provide a variety of basic computing resources such as processing and storage. The AWS global infrastructure includes the facilities, network, hardware, and operational software (e.g. host OS, virtualization software, etc.) that support the provisioning and use of these resources. The AWS global infrastructure is designed and managed according to security best practices as well as a variety of security compliance standards.

For more information about AWS security see “Amazon Web Services: Overview of Security Processes” whitepaper at http://aws.amazon.com/security/.

Cloud Environment Compliance

The IT infrastructure that AWS provides to Fluix is designed and managed in alignment with security best practices and a variety of IT security standards, including SOC1/2/3, PCI DSS, FedRAMP, ISO 27001, FIPS 140-2, MTCS Level 3, and others. In addition, the flexibility and control that the AWS platform provides allow customers to deploy solutions that meet several industry-specific standards, including HIPAA, CSA, MPAA.

AWS provides a wide range of information regarding its IT control environment to customers through white papers, reports, certifications, accreditations, and other third-party attestations. More information is available in the Risk and Compliance whitepaper available on the website: http://aws.amazon.com/compliance/.

Data Transfer

To protect transferred data, Fluix uses Transport Layer Security (TLS) for data transfer between Fluix App and Fluix Cloud. The secure tunnel for data transfer is protected by up to 256-bit Advanced Encryption Standard (AES) encryption. Our servers are configured to use strong cryptography ciphers (**Elliptic Curve Cipher Suites**), have support for **perfect forward secrecy**, and **HTTP Strict Transport Security** with a long duration.

The server requires clients to use TLS 1.2 protocol with the following cipher suites in server-preferred order (as of November 2020):

TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 (0xC0, 0x2B)	128
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xC0, 0x2F)	128
TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256 (0xC0, 0x23)	128
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 (0xC0, 0x27)	128
TLS_RSA_WITH_AES_128_GCM_SHA256 (0x00, 0x9C)	128
TLS_RSA_WITH_AES_128_CBC_SHA256 (0x00, 0x3C)	128
TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 (0xC0, 0x2C)	256
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (0xC0, 0x30)	256
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384 (0xC0, 0x24)	256
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 (0xC0, 0x28)	256
TLS_RSA_WITH_AES_256_GCM_SHA384 (0x00, 0x9D)	256
TLS_RSA_WITH_AES_256_CBC_SHA256 (0x00, 0x3D)	256

Data Storage

Fluix Storage Service is based on AWS S3 storage and uses 256-bit Advanced Encryption Standard (AES) encryption for data at rest. Storage service employs strong multi-factor encryption. Each document is encrypted using a unique key. As an additional safeguard, the key itself is encrypted with a master key, which is rotated regularly.

Fluix production customers can access their documents stored in the built-in cloud repository (Fluix storage) at any time in the course of their active subscription. Completed workflow documents can also be viewed (managed) by dedicated company employees with special permissions to access the Fluix admin portal. These can be found in Document Status and will be stored there for up to 999 days. Afterward, these documents can be accessed at any time only from the Fluix storage if they were submitted there.

Network Security

- **The Fluix production network** is segregated from the Fluix corporate network and requires a separate set of credentials for logical access.
- **Virtual Private Cloud (VPC)** is used to provision a logically isolated section of the Amazon Web Services (AWS) Cloud. Fluix VPC employs rule sets, access control lists (ACL), and configurations to enforce the flow of information to specific information system services.
- **Firewall configuration** is strictly controlled and limited to a small number of services and administrators.

Testing

Fluix Limited has established a specialized team to conduct security tests against Fluix to ensure that the security incident response process is technically sound and effective. Fluix Limited also regularly invites third-party teams to perform penetration tests to evaluate the effectiveness of the security protections in place and the smoothness of the incident response process.

Data Breach Practices

In general, the Fluix Incident Response Team handles any security incidents.

If despite all other protections in place, your data is accessed without authorization, we will notify you.

Reliability

- Fluix offers a 99.9% uptime guarantee. Our record shows we are performing above this level of availability.
- All stateful Fluix Cloud instances are backed up nightly and backups are retained for two weeks.
- The AWS S3 storage service we are using is designed for 99.99% availability and an extremely high amount of durability. The service redundantly stores data in multiple facilities and on multiple devices within each facility.
- Fluix undergoes annual disaster recovery testing during which we are able to deploy the latest version of Fluix infrastructure in a new environment in a matter of hours.

Privacy

Fluix takes the privacy of its users and their business data very seriously. Our privacy policy is available at https://fluix.io/privacy.

EU General Data Protection Regulation (GDPR)

Fluix is committed to the security and protection of our clients' data including PII in line with legal requirements of the EU GDPR. Before going into effect on May 25, 2018 Fluix has added several features to its application to comply with the requirements and improve data security.

Fluix has an appointed Data Protection Officer who will be able to reply to any GDPR and data privacy inquiries, please contact them at dpo@fluix.io.

Summary

With the above security principles built into Fluix architecture, Fluix mobile document management solution provides a reliable environment for a paperless workflow.

About Fluix Limited

Fluix was spun out of award-winning productivity app company, Readdle, in 2014. Over the years our technology has developed into a robust platform that helps bridge the gap between remote teams and offices. Companies using Fluix are now more efficient at collecting and processing data in the field – saving time, money, and effort, overall.

Despite the hundreds of mobility-focused software solutions out there today, our team recognizes that not only is this market relatively new, but also there are a variety of unique challenges each company faces across the globe.

To learn more visit www.fluix.io.