KAOSHI SECURITY POLICY

Introduction

KAOSHI aims to be a one-stop shop for all immigrant financial needs in their home country - remittance, mortgage, loans, investment, financing, insurance, etc. It connects immigrants to the financial needs of their family members in their home country.

Being entrusted with user data demands a high level of diligence in securing said data and this becomes even more important when dealing with financial information.

To this effect KAOSHI takes a great deal of care in ensuring that the data of our users is kept as secure as is possible in accordance with industry accepted standards.

There are also strict security measures in place on KAOSHI's infrastructure. This serves to protect against unauthorized access, alert the right teams in the event of a breach and prevent possible misuse of access within the company.

This document details the measures which have been put in place to ensure that KAOSHI continues to deliver on its promise to provide the best service to its customers in the most secure means possible.

Organizational Security

KAOSHi recognizes the need to enforce strict observances of industry acceptable security measures within the organization as part of its larger aim of ensuring that all services provided to its users are as secure as possible. This section details the steps which have been put in place to minimize the chances of security breaches from within the company.

Employee Orientation

All KAOSHI employees are properly briefed on protocols to follow when working with company property including but not limited to KAOSHI servers, processing user data, application code and company related communication.

KAOSHI employs secure platforms for handling intra organizational communication. This cental communication hub limits the chances of sensitive information being leaked to non-privileged parties.

As with every part of KAOSHI's processes, the employee security protocol in place is constantly being evaluate and modifications are made in areas which either fall short or are no longer sufficient to meet KAOSHI's security compliance levels.

Infrastructure Security

KAOSHI utilizes reputable cloud service providers for providing the infrastructure to run its services. The deployment team responsible for provisioning resources with selected cloud service vendors ensures that the provisioning process meets the stipulated security measures suggested by the cloud vendors. This serves as the first layer of security in KAOSHI infrastructure.

Infrastructure Hardening

KAOSHI does not stop at implementing vendor suggested security measures. Company security policies for provisioned servers list out guidelines which are followed after services are provisioned.

These policies ensure privileged access to KAOSHI servers is allowed only via provisioned virtual private networks and also that only employees who need access to the servers to carry out their designated functions are granted access.

In the case of its servers, KAOSHI sets up default firewall policies that block all non functional ports. Where possible non-default ports are used to discourage attackers.

Traffic monitors are also setup on the servers to send alerts in the event of detection of suspicious traffic patterns.

Development Best Practices

KAOSHI treats all application code as intellectual property and ensures that it is securely stored.

Private version control systems from trusted and reputable vendors are used to store code securely. Great care has also been taken to ensure that the deployment pipelines from development to staging and finally the production environments are made as secure as possible.

A team within KAOSHI is responsible for auditing all newly added features to the platform to

ensure that no security breach is introduced into the system.

Within the application code itself sensitive data is never stored. All sensitive data required to deploy and run the application are bundled as environment variables stored in secure storage and injected into the application during the deployment phase.

Access Control

Provisioning

To minimize the risk of data exposure KAOSHI adheres to the principles of least privilege and role-based permissions when provisioning access.

Employees are only authorized to access data and resources that they reasonably require in order to fulfill their current job responsibilities.

All production access to data, infrastructure and other resources is reviewed at least quarterly.

Authentication

To further reduce the risk of unauthorized access to data, KAOSHI employs multi-factor authentication for all access to systems with highly classified data, including our production environment, which houses our customer data.

Where possible and appropriate, KAOSHI uses public key encryption methods for authentication, in addition to the previously mentioned multi-factor authentication on a separately configured device.

System Monitoring, Logging and Alerting

KAOSHI monitors servers, workstations and mobile devices to retain and analyze a comprehensive view of the security state of its corporate and production infrastructure.

Administrative access, use of privileged commands, and system calls on all servers in KAOSHI's production network are logged and retained for at least two years. Analysis of logs is automated to the extent practical to detect potential issues and alert responsible personnel.

All production logs are stored in a separate network that is restricted to only the relevant security personnel.

It should be noted that care is taken to ensure that only information required to sufficiently evaluate compliance with company security policies are logged.

Data Encryption

Data in Transit

Data transmission between KAOSHI clients i.e mobile applications, web applications and KAOSHI servers as well as server-to-server communication employs industry recommended security protocols.

All KAOSHI services (clients and servers) are fully TLS 1.3 compliant. Also, where required and supported by the services, KAOSHI encrypts data being transferred between services using AES256 encryption and utilizes SHA256 signatures for payload verification.

KAOSHI also ensures that all third party providers with whom data might be exchanged also provide guarantees on the security of data in transit.

Data at Rest

Data at rest on KAOSHI's production infrastructure is encrypted using FIPS 140-2 compliant encryption standards. This applies to all data stored in relational databases, file stores, database backups, etc.

The encryption keys are stored in a secure server on a segregated network with access granted only to a specially designated personnel. This ensures that even in the event of a breach, intruders would not be able to decipher the stored data without also getting access to the keys.

Appropriate safeguards which protect the creation, storage, retrieval, and destruction of secrets such as encryption keys and service account credentials have also been implemented.

KAOSHI carefully evaluates the security policies of selected third party vendors with whom data might be stored to ensure that at no point in time within the storage time frame is the data security compromised.

Data Retention and Disposal

KAOSHI Customer data is removed immediately upon deletion by the end user or upon expiration of message retention as configured by the customer administrator.

However, as required by Anti Money Laundering regulation, KAOSHI is required to retain certain data for a specified period before they are eventually deleted.

Kaoshi hard deletes all information from currently running production systems (excluding and search terms embedded in URLs in web server access logs) and backups are destroyed within 14 days.

When selecting vendors for cloud storage, KAOSHI ensures that the vendors remove data from disks in a responsible manner before they are repurposed. Vendors who do not meet this requirement are not considered in the selection process.

Handling Security Breaches

Despite best efforts, it might happen that a security breach is identified by a non-contracted party. In the event of such reports reaching KAOSHI, all necessary action required to remediate the breach is taken.

KAOSHI has a well defined escalation policy for all identified breaches from the first point of contact to the teams which have responsibility over affected parts of KAOSHI infrastructure. KAOSHI's security team is also notified in the event of such a breach.

All affected parties including but not limited to users, vendors, and service providers are notified of the breach within 48 hours at most.

The initial notification details the cause of the breach and the steps taken to remediate it. If the remediation process is still ongoing then all affected parties are updated at least on a daily basis until the breach is closed.

External Validation

Security Compliance Audits

KAOSHI is continuously monitoring, auditing, and improving the design and operating effectiveness of our security controls. These activities are regularly performed by both third party credentialed assessors and KAOSHI's internal risk and compliance team (contracted).

Audit results are shared with senior management and all findings are tracked to resolution in a timely manner.

Penetration Testing

In addition to our compliance audits, KAOSHI engages independent entities to conduct application-level and infrastructure-level penetration tests at least annually.

Results of these tests are shared with senior management and are triaged, prioritized, and remediated in a timely manner.

Third-Party Security Notification

KAOSHi takes all non-contracted 3rd party identifications of security breaches very seriously and treats such reports with the same level of severity as it would for internally reported breaches.

The notification policy mention in the section on *Handling Security Breaches* also applies in this case as well as for security breaches identified during compliance audits and penetration testing.

Vendor Management

To run efficiently, KAOSHI relies on sub-service organizations (also called vendors). Where those sub-service organizations may impact the security of KAOSHI's production environment, appropriate steps are taken to ensure that KAOSHI's security posture is maintained by establishing agreements that require service organizations to adhere to confidentiality commitments which have been made to users.

KAOSHI monitors the effective operation of the organization’s safeguards by conducting reviews of all service organizations’ controls before use and at least annually.

Below is a list of our sub-service organizations:

1. Amazon Web Services - Data storage and cloud servers
2. Twilio - Email and SMS Notifications
3. ShuftiPro - Identity Management and Anti-Money Laundering Checks
4. Plaid - For Financial Data Aggregation
5. VoPay - For Payment APIs in Canada
6. Token - For Payment API in the UK and Europe