gabi.

Gabi Solutions Security Overview

Document version: 06-18-18.1

Gabi Solutions is committed to providing a highly secure and reliable services to its clients. We maintain the confidentiality of its customers' information and ensure that customers' information will be available when it is needed.

To achieve best-in-class security, we design all our Applications with security in mind. We use tools, technologies, practices and methods to minimize the use and storage of customer personally identifiable information (PII) on Gabi Solutions data servers.

Application Development

Gabi Solutions utilizes a comprehensive software development lifecycle process that incorporates the security by design. Many of our applications are designed to process data in a manner that does not involve the capture or storage of PII on Gabi Solutions data servers. All applications are regularly scanned for common security vulnerabilities.

In addition, we provide regular training on security best practices for our engineers. Regular security tests are conducted, including the use of scanning and fuzzing tools to check for vulnerabilities.

Network Security

At Gabi Solutions, all information is encrypted in transit and at rest.

Gabi Solutions services are accessible only over HTTPS. Traffic over HTTPS is encrypted and is protected from interception by unauthorized third parties. Gabi Solutions follows current best practices for security, including the use of strong encryption algorithms with a key length of at least 128 bits.

For on-premise systems, access requires the installation of a on premises agent behind the firewall. All communication between Gabi Solutions and the on premises agent is over an encrypted link (TLS 1.2).

Administrative access to Gabi Solutions servers is over VPN or other secure protocols. Administrative access is granted only to select employees of Gabi Solutions, based on role and business need. Multi-factor authentication is required for access.

Gabi Solutions uses a multi-tier architecture that segregates internal application systems from the public Internet. All network access, both within the datacenter and between the datacenter and outside services, is restricted by firewall and routing rules. Network access is recorded into a centralized secure logging system.

Application access to databases used in the Gabi Solutions service is over an encrypted link (TLS).

Transaction Data Retention and At-Rest Protection

Gabi Solutions stores transaction related data only to enable customers to have better insight and control over their transactions and in cases where transactions take a long time to finish. Specifically, Gabi Solutions stores transaction data to support transaction logging, testing and debugging, re-running transactions, and in support of long running transactions. All transaction data is always encrypted in transit and when stored in Gabi Solutions's platform. Gabi Solutions stores transaction data on the Google cloud.

Customers have control over the retention period of the transaction data. In addition Gabi Solutions provides the ability to mask out sensitive data in the transaction logs for additional security.

Hosting Environment and Physical Security

Gabi Solutions is hosted on public cloud infrastructure from Amazon Web Services (AWS) and Google Cloud Platform. Both Amazon and Google servers and databases run on servers in secure data centers and have a broad set of certifications.

You can read further about AWS and Google security and certifications here:

aws.amazon.com/security/

cloud.google.com/security/

PCI

Gabi Solutions uses PCI Compliant Level 1 audited payment processor for processing credit card payments for the Gabi Solutions services.

Data Privacy

Gabi Solutions has a privacy policy, which details the steps we take to protect clients' information. You can view the privacy policy here at https://www.Gabi Solutions.com/terms-privacy/ .

User Authentication

Clients login to Gabi Solutions using a password which is known only to them. Password length and complexity standards are enforced. Passwords are not stored; instead, as is standard practice, only a secure hash of the password is stored in the database. Because the hash is relatively expensive to compute, and because a "salting" method is used, brute-force guessing attempts are relatively ineffective, and password reverse-engineering is difficult even if the hash value were to be obtained by a malicious party.

Connections to remote systems are done only over secure (HTTPS) connections.

Gabi Solutions supports automatic session logout after a period of time. Enterprises can set the appropriate timeout period according to their security needs.

When Gabi Solutions connects to remote systems using user-supplied credentials, where possible this is done using OAuth2, and in those cases, no credentials need to be stored in the Gabi Solutions system. However, if a remote system requires credentials to be stored, they are encrypted using a 256-bit key.

Gabi Solutions systems can be configured to require Multi-factor Authentication as well as other security features.

High Availability

Gabi Solutions ensures continuous availability of its service and protects against the risk of disruptions by implementing a Business Continuity and Disaster Recovery program. This includes continuous backup to a standby database.

Personnel Security Practices

All employees are subject to background checks that cover education, employment and criminal history. Employment at Gabi Solutions requires written acknowledgement by employees of their roles and responsibilities with respect to protecting user data and privacy.

Gabi Solutions maintains an information security training program.

Knowledgeable full-time security personnel are on staff.

Incident Response

While we don't anticipate there ever being a breach of our systems, we know that no computer system is perfectly secure.

In the event of a breach of a Gabi Solutions information system, we have a detailed Incident Response Plan in place, and there is periodic testing of the response plan.

Gabi Solutions has 24x7 monitoring of the security status of its systems and automated alerts for security and performance issues.