Float

Security White Paper

Introduction

Keeping customer data safe is a key goal for Float. We work hard to maintain and deliver best in class controls for organisational security, data protection and privacy.

Team Security and Access Control

Personnel

We take great care in finding the right people to work with. Our team is the lifeblood of our customers.

- Float as an organization has been operating for 10 years without a single data breach.
- All of our team go through background checks as part of our hiring and onboarding process using a trusted third party service.
- All members of the team are required to sign privacy agreements upon joining the company.

Security is everyone's problem

As a distributed company we have to take security far more seriously than many. We take the view that security is everyone's problem. Everyone in our organisation is trained and made aware of security best practices.

- We run a zero-paper company, in a bid to remove potential security failures in lost or stolen documentation.
- All of our internal communications are labelled and categorised in terms of confidentiality, this way our team knows immediately what level of care and attention a piece of information requires.
- We consistently utilize a centralized SSO for access to all production systems and company documentation. This gives our teams fine-grained control over permissions for the systems and services we use.
- We heavily enforce principles of least privilege across the organisation. This means that individuals can access only the information and resources that are necessary for their work.

- We enforce specific security policies for the individual use of laptops and computers for work.

Security Overview

Security Policies and Standards

We run our infrastructure on Google Cloud. You can find documentation on their security compliance here: https://cloud.google.com/security/compliance/

We regularly run penetration testing and heavily utilize the security offerings of our cloud providers to keep our networks up to date and safe.

Some of our key policies for our engineering and operations teams are:

- We consistently design our software features and updates with security in mind.
- We tackle our engineering and operations debt in specific cycles of work.
- We regularly maintain our systems and keep them up to date, including maintaining OS and framework level patches.
- As a team, we subscribe to and monitor various security publishers to keep ahead of exploits and stay up to date with best practices.
- We design, review, and test our response processes.
- We maintain internal SLO's (Service Level Objectives) in responding to alerts and security events.
- We operate a "follow-the-sun" on-call team who are always available to respond to events.
- We use automated monitoring that alerts for hundreds of potential issues which are then escalated to our Ops team for investigation.
- We utilize public status pages and perform public postmortems where possible to keep our operations as transparent as we can.

Platform

Float as a platform has been evolving and growing over the past 10 years. As its stands in 2021:

- Float is a micro-service software stack comprised of multiple languages including NodeJS and PHP.
- Float utilizes tried and tested database technologies like MySQL, Redis and MongoDB in delivering highly available global software.
- Float's software stack is mostly standalone, although we do rely on these third party providers for some aspects of key functionality:
    - **Recurly**: Payment processing service
    - **Sendgrid**: Email delivery service
    - **Intercom.** Help desk software
    - **Rocket Science Group (MailChimp).** Email newsletter service

Data protection and privacy

Data Centers and Infrastructure

Our primary data centres are located in Google Cloud regions `us-central1`, `us-east1` and `us-west1`. You can see a list of locations for Google Cloud here: https://cloud.google.com/about/locations/

We run our infrastructure across multiple availability zones and regions for redundancy.

Ours and our customers data is backed up in multiple regions so it's always accessible in the event of a region outage.

- We backup our databases and our internal data within Google Cloud.
- Backups are distributed across multiple regions so they're always accessible in the event of a regional outage.
- We don't backup data offline or allow production data outside of Google Cloud Platform.

Our applications are run within secure VPC's which maintain separate links to the outside world by controlled policies.

By using data centers from world class leaders like Google Cloud and AWS, we instantly inherit the extreme level of security they apply to their own systems like biometric locks, round-the-clock interior and exterior surveillance monitoring, and 24/7/365 onsite staff.

Encryption

All traffic to our systems occurs via strong encryption. All web traffic to our systems happens only via TLS, and any non HTTPS traffic is automatically redirected to use TLS.

We use SSL certificates issued by Google. Our connections use `AES_256_GCM` and `AES_128_GCM` for encryption, with `SHA2` for message authentication and `ECDHE_RSA` as the key exchange mechanism.

Our SSL certificates are rotated every 90 days automatically. This means we keep a consistently updated set of encryption protocols facing our customers, and we never degrade a request to our systems from HTTPS to HTTP.

All of our data storage is encrypted at rest by default, and the backups for those systems are encrypted and distributed securely across multiple regions. We use AES-256 encryption for in-use storage like databases.

All passwords are hashed and salted using BCrypt with a cost factor of 10.

General Initiatives

Your data is yours—plain and simple. At Float we live and die by these key principles:

- We will never sell your data to a third party.
- We will not provide access to your account to anyone without your express, written consent.
- The only time a member of the Float team will access your account is to help you solve a problem or to reproduce a software bug, and in all but the most extreme cases (picture the SaaS equivalent of a nuclear meltdown), we will always ask for your permission first.

This policy applies to the personal data of all of our users, regardless of who you are or where you're located.

You can find our full privacy policy here https://www.float.com/privacy

EU-US and US-Swiss Privacy Shield Frameworks

We are officially compliant under the EU-U.S. and Swiss-U.S. Privacy Shield Frameworks. In addition to GDPR compliance, this furthers our ongoing commitment to your privacy and security and the transfer and use of your personal data. Read more about the Privacy Shield program here.

Data deletion

We're dedicated to helping Float customers and users understand and comply with the General Data Protection Regulation (GDPR) that went into effect on May 25, 2018.

Account Owners can delete their customer data at any time during a subscription term by selecting "Delete Team" from the bottom of the Team Settings.

All your content will be deleted from our servers within 30 days on the event of a deletion. Individual people and project data can also be deleted at any time from within the app or via our API.

Conclusion

Security is about trust. Our team is hand-picked to exhibit and apply the ideals of trust as an extension of Float as an organisation.

We consistently work on updating and improving our security processes and procedures with the understanding that security is a never finished goal.

Want to know more?

Submit a support request if you have other security questions and we'll get back to you as quickly as we can.