Biings Security Overview

Introduction

Biings' mission is to help companies maintain a healthy working climate in their teams through preventive absence management practices. Keeping customer data safe and secure is a huge responsibility and a top priority for Biings Technologies. We work hard to protect our customers from the latest threats. We store our own sensitive absence and HR data on the same server our customers do. We don't want our information compromised, so we're motivated by self-preservation as well. Aligning our goals with your goals is the best way to see eye-to-eye on the need to keep everything as secure as we can.

Organisational security

Access control

All our employees and contractors (workers) sign confidentiality agreements before gaining access to our code and data. Background checks aren't performed on our workers.

Only employees located in our office in Morges are allowed to access client's data.

Everybody at Biings is trained and made aware of security concerns and best practices for their systems (including regular password updates) as well as the way we code and handle support tickets. We log all access to all accounts and servers by IP address. Physical access to our office in Morges is also logged via individual and identifiable key cards.

Our hosting provider (Infomaniak) has no access to the data on our server.

System Monitoring, Logging and Alerting

Biings runs on a dedicated server secured with firewalls and carefully monitored. Our software infrastructure is updated regularly with the latest security patches.

We also have alerts in place for server downtime or excessive resource use. Those alerts escalate to our team for manual investigation.

We use a proven tool to monitor our logs and suspicious activity (including failed server logins).

Development guidelines

Our coding and development practices include special attention to the top 10 security risks published by the OWASP Foundation (https://owasp.org).

Additionally Biings, as a server and web application, is built on top of open source frameworks that already include strong security layers and that are regularly tested and updated to fix known vulnerabilities.

Backups

All data and files are backed up daily, and stored in multiple locations in Switzerland. By default all our backups are kept for a maximum of 30 days.

Server snapshots are performed regularly for rapid disaster recovery.

Data protection and privacy

Data Location

Biings software application runs on a server located in Switzerland and hosted by Infomaniak. For security reasons, the exact location of the server and its data center is not made public.

Biings Account security

While we don't require users to set a complex password, we always ask for a minimum number of character when setting or updating any password in Biings.

We limit and log failed login attempts and disallow user enumeration to slow down password guessing attacks.

Encryption in transit and at rest

Over public networks we send data using strong encryption. We use SSL/TLS certificates issued by GANDI.net. The connection uses AES_128_GCM for encryption, with SHA2 for message authentication and ECDHE_RSA as the key exchange mechanism.

Absence data, follow-up actions and HR data aren't encrypted at rest — they are active in our database and subject to the same protection and monitoring as the rest of our systems. All passwords are hashed and salted using a Blowfish encryption algorithm.

Database backups are encrypted. Only our staff in Morges holds the encryption key to those backups.

Physical Security

Hosted in Infomaniak Tier III+ data center, our server is protected by several airlocks, biometric identification (analysing the vein network of your finger), facial recognition and round-the-clock interior and exterior surveillance monitoring.

Only authorized personnel have access to the data center. 24/7/365 onsite staff provides extra protection against unauthorized entry and security breaches.

Law enforcement

Biings won't hand your data over to law enforcement unless a court order says we have to. We flat-out reject requests from local and federal law enforcement when they seek data without a court order. And unless we're legally prevented from it, we'll always inform you when such requests are made.

Data retention and deletion

All your content will be inaccessible immediately upon cancellation. When you cancel your account, we'll transfer all of your data stored on our server over to you and we'll ensure that everything is deleted from our servers past 30 days. Your data can not be recovered once it has been permanently deleted.

Incident management and disaster recovery

In the event of an incident, we will contact your account owner, and work with you throughout.

When a security breach is detected, by us or our monitoring systems, we would promptly notify you and tell you about the data involved in the event (to the extend of what we can learn from our logs and databases).

We retain a full backup copy of production data in a remote location. Full backups are saved to this remote location at least once per day.

In case of disaster our team is trained to restore all system using the latest server snapshot and backups.

In case of Ransomware attack

If by any chance we fall victim to a ransomware attack, the first thing we will do is to freeze all access to production data and tell every impacted client about what is currently happening. The next step will be to contact the authorities.

We will then setup an entirely new cloud server and restore all data to the latest available backup in order to let our client use their product as fast as possible again.

One of the most important step will be to investigate what went wrong and take action to fix the related vulnerability if possible. Throughout all of this we will keep every impacted client update as the situation progresses.

Conclusion

We've been around since 2013 and we've worked with companies applying high-level security practices. Security isn't just about technology, it's about trust. We've worked hard to earn the trust of our clients over the years. Safeguarding the HR data stored in Biings is a critical responsibility we have to our customers, and we continue to work hard to maintain that trust.

Want to know more?

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

swiss made software
+hosted in switzerland