Standard Policies & Procedures

Information Security

Beam HR

October 2020

Contents

Beam Information Security

This document describes how Beam manages the security and integrity in relation to the provision of its hosted Workforce Management Services.

Hosting Partner

Beam has selected Google Cloud Platform (GCP) as its Hosting partner. Primary region is `europe-west1` which servers are located in St. Ghislain, Belgium, Europe. Secondary regions for Disaster recovery are XXXX (IRELAND??) and YYYY (USA???).

Every internal service is active in at least two Availability Zones and load balanced using proxies. All services can handle failure of a single zone. Beam offers a highly redundant and scalable platform and product.

Solution Security

Physical Security

Beam hosting environment is a fully redundant and scalable solution hosted in CPG hosting environment fulfilling ISO IEC 27001 for security requirements, and ISO IEC 27017 for cloud security and ISO IEC 27018 for cloud privacy ensuring GDPR compliance. You can read more about CGP hosting security policy in terms of Compliance, Infrastructure, Security Products and Transparency here and specifically Google Cloud Platform Security Whitepaper.

Operating System Security

We have a conservative upgrade policy where we receive and analyze security advisories and decide whether they pose an actionable attack vector to us or our customers using the platform before upgrading. All servers are running Linux operating systems that are hardened to the usage of the specific server.

Application Security

Access to the application and its stored data, regardless of user role, is secured using a personal identifier such as email address or user ID or phone number and password. The Data that can be used to access customer and user data, such as passwords, are stored in encrypted format. The customer has also the option to require to Beam's technical team to implement for their users a heightened password security level which requires that passwords:

- Are at least 8 characters long, containing at least two numeric and two alphabetic characters
- Are changed at least once every three months and are not reused during a 30-month period or 10 consecutive password changes

Access to the full data set is only given to Beam representatives who absolutely require it to perform their work and Beam routinely reviews this access to determine whether, depending on the representative's current needs, there are grounds for revocation.

All Beam representatives are subject to confidentiality agreements and are instructed in best practice data security procedures as part of their onboarding. All digital work environments are safeguarded with a central authentication mechanism which ensures that users only have access to data in each respective software application that is crucial to their´ability to fulfill Beam' agreement with the customer.

The application is guarded by server side validations based on the user's actual and stored role and access rights. Only data valid and allowed for the specified user is transmitted to the´client application layer ensuring that no data is leaked by investigating the data sent out from the server environment. All communication between client software and third-party applications is encrypted using SSL using SHA-256 (512 bits) with RSA encryption.

Mobile Security

Access to the mobile application, in addition to the above stated Application Security measures, is protected by both - TLS (Transport Level Security) and Application Security. Application Security of mobile application is based on the latest security standards for authentication and authorization of user access. Authentication rules applicable as described above in Application Security section, and authorization is based on OAuth2 standard combined with JWT (Json Web Tokens). Any authorization details passed via network are:

- Digitally signed (JWS) with SHA-256 (2048 bits RSA algorithm key)
- And encrypted (JWE with 256 bits AES algorithm key)
- All of the above is in addition to protection on transport level using encryption methods stated above in the Application Security section.

API Security

One of the data channels provided by Beam is access through API. API access is highly secured with multiple levels of protection, including TLS (Transport Level Security), Network Security, Application Security and Security Gateways. Efficient components of such architecture guarantee a high level of customer data safety. API Security implementation is based on the latest security standards.

API Authentication Controls

API Security requires stronger policies around the length and complexity (at least 2 times stronger) of credentials than those described above in the Application Security section. Customer client (API integrator) credentials are never stored as plain text within systems of Beam, instead those are hashed using strong hashing techniques - which eliminates the possibility of unauthorized access from internal Beam systems.

API Authorization Controls

Strong controls around API access authorizations are in place to support management of access - so access could be efficiently enabled and revoked when needed. API Authorization uses various techniques, including OAuth2 standard combined with JWT (Json Web Tokens). In this scenario the authorization details passed via network are:

- Digitally signed (JWS) with SHA-256 (2048 bits RSA algorithm key)
- And encrypted (JWE with 256 bits AES algorithm key)
- All of the above is in addition to protection on transport level using encryption methods stated above in the Application Security section.

API Security Gateways

API Gateways provide an extra layer of security in combination with other measures, such as Network Security. API Gateways support secure routing of authorized traffic towards the internal services, so the internal systems of Beam would not be exposed. Those also guarantee the additional protection for the whole API layer as such, effectively providing protection against unexpected load (circuit breakers, throughput limits) - improving the overall state of API layer defence mechanisms.

Network Security

Beam uses a centralised authentication mechanism for all servers including test environments. It is group based with minimal rights to users granted on a need-basis.

Customer Data Security

Database

Access to production databases is only permitted for Systems Administrators to complete their mandatory work duties and read-only access is allowed on a need to have basis for representatives for the purposes such as error finding and support.

Block-Level Data

Data at rest is encrypted using mechanisms built into the hosting provider's platform with keys on an HSM (Hardware Security Module) which the provider does not have more than physical- and log-access to.

Environment Separation

Development, staging (pre-production) and production environments are separated on different servers and network segments and are not connected in any logical way. All environments listed are hosted using the same security levels as if it were a production environment.

Logging of Data Changes

Any changes to critical application data such as access rights, agreement templates, individual agreements, users, planning units, schedule and time punch-clocks are logged, regardless if they are performed by Beam representatives on behalf of the customer or by the customer's users themselves.

General Security Audit

On an annual basis, Beam invites an external security company to perform an audit and penetration test of our environments. These audits and tests are summarised in reports highlighting vulnerabilities, if any, which in such a case are addressed immediately.

Backup

Beam takes full automated backups of configuration, code and data every 3 hours to both a local storage and a secondary site. Data is also copied in real-time to a database replica on a secondary site to not lose any data in the unlikely event of a full disaster in both availability zones of the main site. This gives us a current RPO (Recovery Point Objective) of maximum 3 hours. Backups are stored for at least 30 days.

Disaster Recovery and Contingency

Beam main hosting is shared over at least two different availability zones at the Primary site and all components of the environment have at least one instance in each availability zone. In the unlikely event of full malfunction in both availability zones at the Primary site, Beam will effectuate the Beam Disaster Recovery Process. The disaster recovery time is currently estimated to be a maximum of 24 hours.

Service Availability

Service Level Agreement

Beam offers a highly redundant and scalable platform and product. Service availability is very high and is guaranteed to be at least 99,5% over 24 hours 7 days a week outside planned maintenance windows. Historical SLA is 99.98% Beam updates the platform and the product at least every 30 days and all customers are notified at least 7 days ahead of maintenance windows that might disrupt service availability.