Beekeeper Security

White Paper

BEEKEEPER

Table of Contents

Statement of Commitment

The Beekeeper product and services are delivered to many companies in a variety of market segments and across the globe. Our customers entrust their data security and privacy to us, and all **Beekeeper employees in return fully commit to maintaining this trust**.

Senior management supports all necessary information security tools and processes. We maintain our commitment without compromising seamless delivery of the Beekeeper product and services, while **ensuring confidentiality, integrity, and availability of our customers' data**.

To achieve the highest level of our customers' trust and to further expand our commitment, we have implemented an Information Security Management System (ISMS) in accordance with **the internationally-recognized information security and data privacy best practices** as outlined by the ISO 27001:2013, ISO 27017:2015 and ISO 27018:2019 certification process.

The enclosed documentation is an attestation to our commitment to customer data protection. Beekeeper will remain vigilant and relentless in continuously improving our ISMS and maintaining our data privacy commitment to our customers and employees in the future.

"We are committed to managing risk with the highest standards of security tools and processes to ensure your right to data protection and privacy."

Cris Grossmann
CEO & Co-Founder

Pillars of Beekeeper's Security

Beekeeper considers data confidentiality, integrity and availability a top priority. We demonstrate our commitment to continuous customer data protection and data privacy processes in the following ways:

1. Beekeeper uses industry-leading data security technologies and follows comprehensive defense-in-depth practices to protect our customers' data

2. Beekeeper operates a highly capable security system to continuously monitor its product and platform for security vulnerabilities

3. Beekeeper's 24/7 on-call technical support ensures rapid response time to detect and respond to any security threats

4. Beekeeper strives to achieve world-class security standards and has fully implemented information security controls as defined by the International Organization for Standardization (ISO) as a minimum requirement

5. Beekeeper is committed to maintaining the highest security standards and continual improvement. As such, Beekeeper undergoes independent internal and external audits and security tests on a regular basis

Beekeeper's security practices are structured in accordance with the six information security pillars to the right. Each pillar contributes to the use of advanced security technology and controls, and in combination, meet the requirements of our ISMS (Information Security Management System). This is congruent with and beyond the requirements of the stringent accreditation process as verified by our ISO 27001:2013 certification in addition to ISO 27017:2015 and ISO 27018:2019 certifications.

Pillars of Beekeeper's Security

Virtual Private Cloud (VPC)

The Beekeeper product and services are deployed in Virtual Private Clouds (VPCs) configured with robust security measures and controls. All of our VPCs are hosted in certified data centers provided by our Cloud Service Providers (CSPs). Our product and services are made available to our customers in various jurisdictions, and customers have the choice to store their data either in Switzerland, in the EU or US.

The customers' tenants within our VPCs are designed to be highly secure and available. Each customer tenant is also fully segregated logically from other customer tenants and data, thus ensuring that each tenant acts as an independent customer environment.

Security Operations

Beekeeper has established leading security operation practices starting with a "shift-left" mentality. Security is factored in right at the beginning of the microservices-based product lifecycle, and automated processes are in place to bring the most recently tested and quality-verified product to the Production Environment, with minimum human intervention. We have implemented robust and modern logging and monitoring capabilities supported by state-of-the-art technologies. Our security audits and testing include a comprehensive vulnerability management program. Beekeeper's Incident Response Plan allows us to handle security incident situations and scenarios in a standardized and consistent way.

Customer Controls Access

Beekeeper was built as an internal communication platform. Access provisioning to their tenant is fully controlled by the customer. Only administrative roles via the Beekeeper dashboard or automated control processes such as the active directory allow control over the identity management.

Full Encryption

Beekeeper utilizes cryptographic measures in various use cases, including encryption of all external communication channels as well as encryption of data at rest, regardless of whether the data is in storage facilities or the end user's mobile device.

Compliance with GDPR and ISO 27001 Regulations

Beekeeper maintains compliance with the General Data Protection Regulation (GDPR) as outlined for the protection of personal data, as well as other jurisdictionally-mandated data privacy requirements. Beekeeper has implemented

Security Pillars

Compliance with GDPR and ISO 27001 Regulations (cont'd)

an ISMS framework in accordance with ISO 27001 control objectives and attained ISO 27001:2013 certification. Beekeeper's data processing agreement is a contractual agreement between Beekeeper and its customers, outlining all requirements of this aspect. In addition, certifications for ISO 27017:2015 and ISO 27018:2019 have been achieved. These latter security standardizations allow Beekeeper to demonstrate compliance as a SaaS offering, both as a Cloud Service Provider as well as when processing personal data in cloud solutions.

High Availability

Beekeeper agrees to a 99.9% availability with customers as part of its commercial subscription agreement contract. Beekeeper fulfills this obligation with multiple redundancy and frequent testing of its service availability.

Beekeeper’s Certification

The International Organization for Standardization is an independent, non-governmental organization consisting of members from the national standards bodies of 164 countries. ISO 27001 is a set of information security and data privacy best practices regarding the management of customer data that adheres to the highest international data security standards. Importantly, ISO standards are the result of a consensus-driven process by experts from all over the world, pooling vast international experience and knowledge from all business sectors.

Data that falls under the risk management controls set in place by ISO 27001 include a customer’s or employee’s details, or any personal information entrusted to us. In addition, ISO 27017 & ISO 27018 certifications establish the framework of control objectives to operate as a Cloud Service Provider as well as process personal data in a cloud-based environment.

Learn more about Beekeeper’s journey to the ISO 27000 series certification and ongoing adherence to ISO 27001, 27017, 27018 information security standards.

Certified Data Centers
Beekeeper only uses certified data center service providers that have obtained internationally-recognized and approved compliance certifications for information security management:

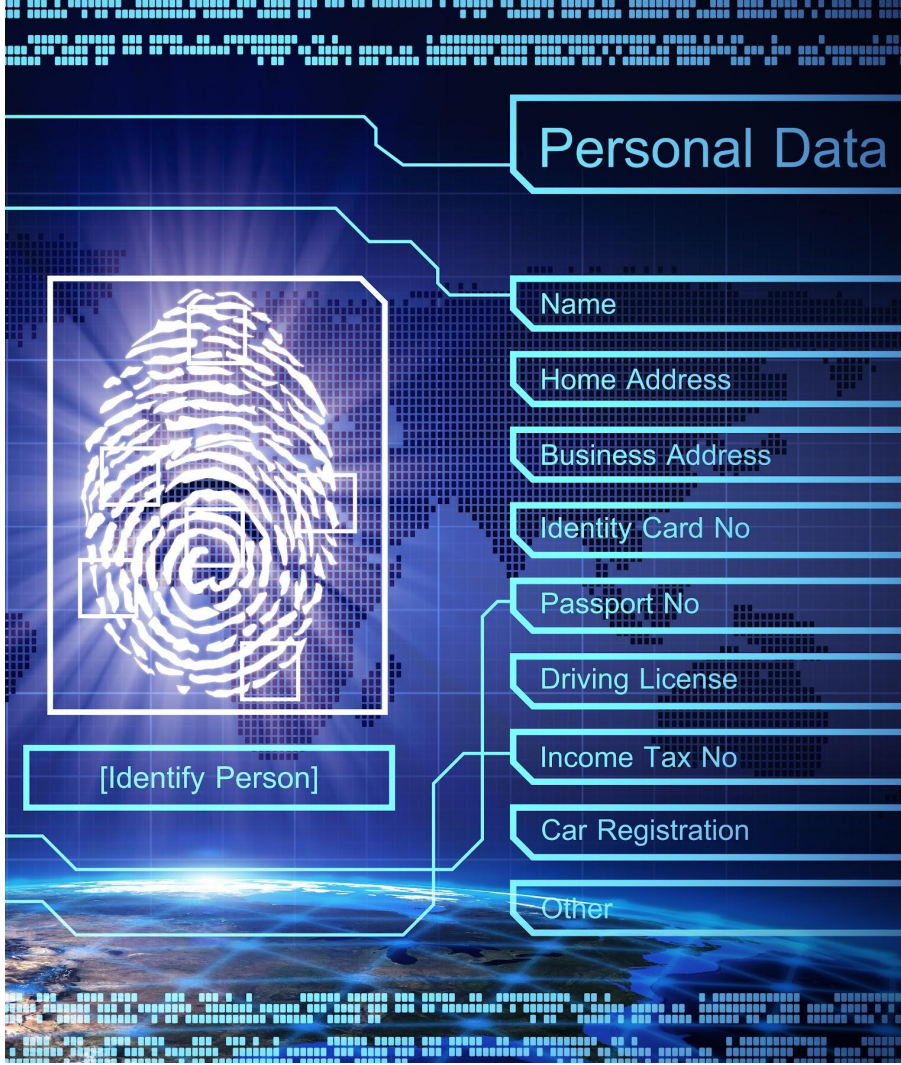
- Amazon Web Services: aws.amazon.com/compliance/
- Google Cloud Platform: cloud.google.com/security/compliance/

Data Privacy

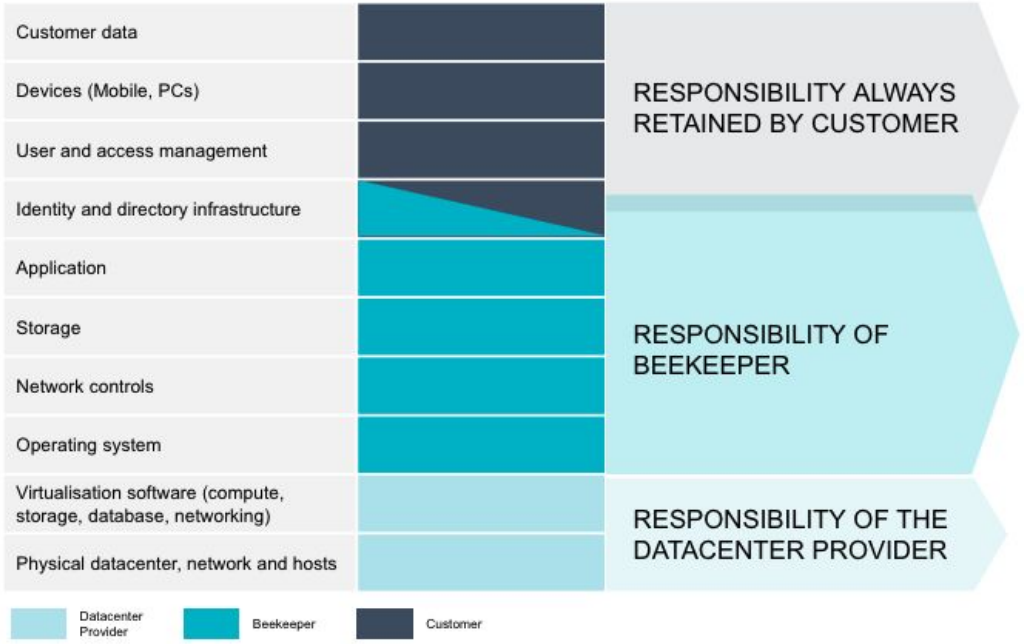
Beekeeper uses the leading and strictest regulatory requirements as outlined in the General Data Protection Regulation (GDPR) and the Swiss Federal Act on Data Protection (FADP) as the umbrella for the data protection requirements on personal data that are stated in our Data Processing Agreement and our Privacy Policy.

Your data is processed in accordance with the seven protection and accountability principles outlined in the GDPR.

Technical measures such as the use of encryption technologies are standard and embedded in Beekeeper's product and service lines. Processes such as the performance of Privacy Impact Assessments before the release of any new product or service line is part of our product and service development lifecycle. The list of organizational and technical measures is available in the Beekeeper Data Processing Agreement (Annex 2).



Our Shared Responsibility Model



- All customer data stored and processed in Beekeeper
- The devices used to access Beekeeper and the way they are being managed and secured
- The level of access accounts and users have to the customer's Beekeeper tenant

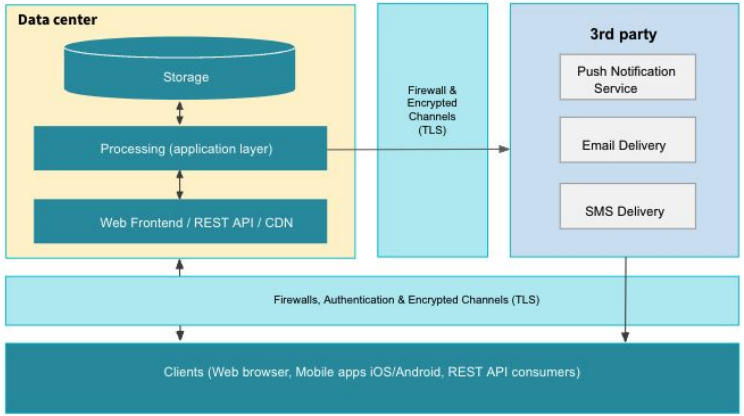
- *The integration of identities and accounts can be a shared responsibility*

- Confidentiality, integrity and availability of the Beekeeper platform and data therein
- Data encryption in transit and at rest
- High-availability, backup and disaster recovery
- Network, cluster and host security including VPC, firewalls, subnets, hardened resources and security tooling

- Beekeeper is responsible for contracting data center providers to handle cloud management & virtualization services
- High-availability datacenter requirements
- Physical and environmental controls

Security Architecture

As a SaaS (Software as a Service) provider, we maximize the security of our cloud platform through a comprehensive defense-in-depth approach, including a high-availability architecture, strong access control, secure segregation, encryption, hardening and frequent backups. Our services are deployed in highly secure Virtual Private Clouds (VPCs) that are monitored continuously for security threats and vulnerabilities.



Storage: Data is stored using state-of-the-art cloud storage services that are highly secure, durable and provide consistent uptime and performance.

Segregation: Each of our customers is defined as an independent tenant, and is logically segregated from other customer tenants and data.

Firewalls: We have configured perimeter firewalls at all our VPCs. Additionally, we have deployed a Web Application Firewall (WAF) for application layer protection.

Third-party connection: Push notifications, emails and SMS text messages are sent via third-party providers. All communication channels with third parties are encrypted with secure protocols.

Encryption & Key Management

Beekeeper has a cryptography and key management policy and procedure to protect the confidentiality, authenticity and integrity of information through encryption.

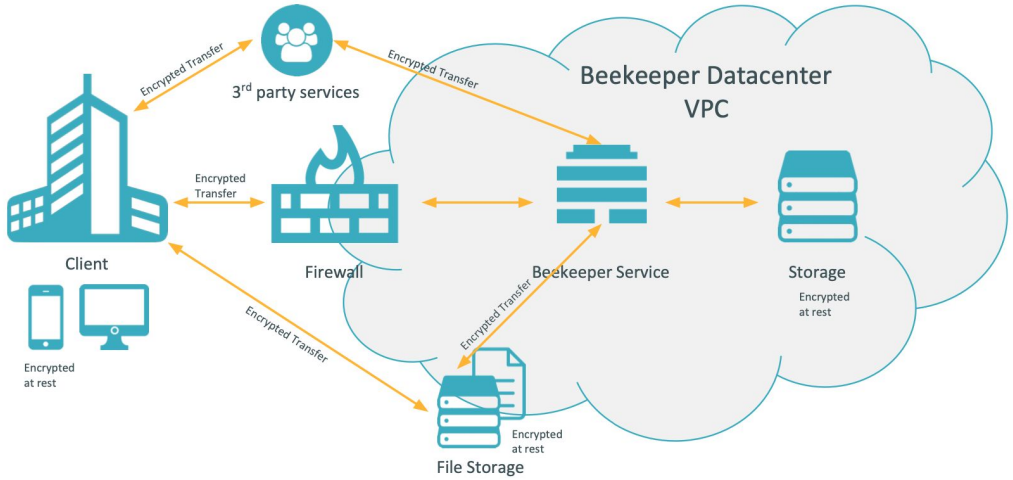
At rest: Data at rest are encrypted. Databases in data centers are encrypted with AES 256. Data on iOS and Android devices are encrypted with AES 256.

In transit: All communications to the Beekeeper platform are through encrypted tunnels using TLS 1.2 and 1.3, utilizing strong cipher suites with a 256-bit AES encryption for secure connections of data transfer over unsecure internet.

Key Management

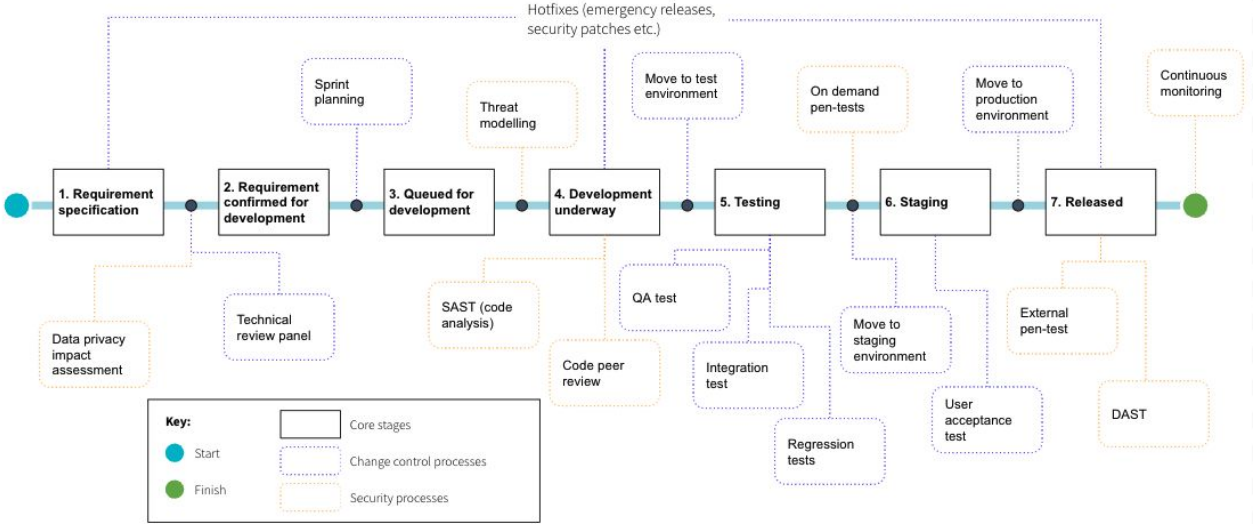
Per the shared responsibility model, all physical infrastructure (i.e. physical data centers) encryption keys are managed by the respective Cloud Service Providers (CSPs). Encryption keys used for connecting and accessing virtual servers, databases, S3/storage buckets and backup are fully managed by Beekeeper.

Data Flow Diagram



Product Development Lifecycle

Beekeeper follows a clearly defined change management process for deploying code changes to the Beekeeper product and services. Our development team employs secure coding techniques and best practices as defined by OWASP or SANS methodologies. Developers are trained in secure application development practices upon hire and further on an ongoing basis. Derived in accordance with ISO 27001 control objectives, the information security policy of Beekeeper mandates a strict segregation of duties as well as separated environments to maximize the confidentiality, integrity, and availability of our information systems.



- Beekeeper has established a formal change management program to ensure changes to formal processes are followed for making any changes to systems/applications
- Development, staging and production environments are separated
- Access for making changes to production systems is restricted to authorized users
- Security processes are fully integrated into the change and product development lifecycle
- Beekeeper has established and implemented a formal security patch management program

Security Testing & Assurance

External Security Testing

Beekeeper's information security policy mandates independent external security firms to perform annual penetration tests of Beekeeper. All findings are recorded in our risk inventory, and mitigation steps are defined and implemented in accordance with our change management processes.

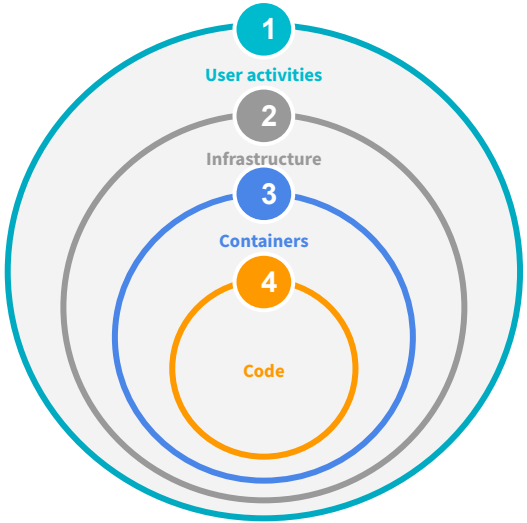
Internal Security Testing

The following internal automated vulnerability checks are performed:

- Independent of code changes:
  - Daily SSL certificate check
  - Weekly configuration scanning, activity monitoring, and reviewing against best practices library
  - Weekly dynamic application security testing
- For every code change:
  - Mandatory peer review
  - Static application security testing
  - Unit and integration test suites focused on access permissions
  - System library vulnerability checks

Logging & Monitoring

At Beekeeper we have designed and implemented robust and modern logging and monitoring capabilities supported by state-of-the-art technologies. We have dedicated tools and strong processes for logs collection, correlation and retention. We deploy WAF in front of all our applications to continuously monitor and filter suspicious traffics. We follow a zero-trust approach and are therefore able to detect suspicious user activities within our network. Our 24/7 support engineers are on duty to respond to any security events outside business hours.



Layers of logging and monitoring at Beekeeper

1. User activities

Among other things, we are logging user activities, including time & date stamp, IP address details, user name & ID, type of activities attempted and systems accessed

2. Infrastructure

In addition to native cloud services (e.g. GuardDuty), we run additional solutions to log and monitor IAM, VPC, DNS and other security related events

3. Containers

We have implemented advanced tools that allow us to log, monitor, aggregate and alert to security events relating strictly to containers

4. Code

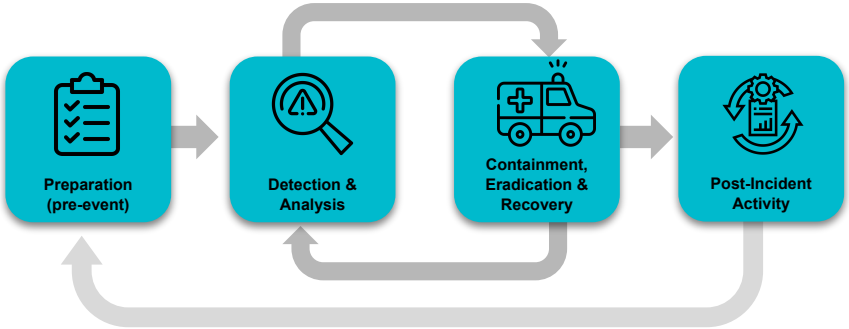
We actively monitor our code base and libraries to identify known/disclosed vulnerabilities. Additionally, we maintain an inventory of our public libraries, repos and dependencies

Incident Response & Notification

We have a defined incident response plan as well as crisis coordination plan in case an incident is escalated as per our incident severity scale. Our Incident Response Plan follows NIST's Computer Security Incident Handling Guide, the industry's best practice standard, is designed to manage cyberattacks in our environment and comprises four phases:

Phase 1: Preparation (pre-event)
Phase 2: Detection and Analysis
Phase 3: Containment, Eradication, and Recovery
Phase 4: Post-Incident

This gives us the required flexibility to handle security incident situations and scenarios in a standardized and consistent way.



In the case of a personal data breach, in line with the applicable data protection regulations (e.g. CCPA, GDPR) Beekeeper will without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to you, following Beekeeper's Incident Management Notification Process.

Our incident management and notification practice is in accordance with the Control Objectives defined by ISO 27001/27017/27018 Incident Management as well as the GDPR Art. 33, 34 requirements. These are both reflected in the Data Processing Agreement.

Disaster Recovery Planning

The purpose of our Disaster Recovery Planning (DRP) is to prepare Beekeeper in the event of extended service outages caused by factors beyond our control (e.g. natural disasters, man-made events), and to restore services to the widest extent possible in a minimum time frame. We have defined a DRP for all our data centers and run quarterly "Disaster days" where we test and evaluate the effectiveness of such plans and make updates based on the learnings of such tests.

Data Preservation and Recovery

In accordance with ISO 27001 control objectives for business continuity and disaster recovery, Beekeeper utilizes data preservation managed services by its certified data center providers. Our solutions are architected with full redundancy capabilities and tested numerous times throughout the year. All availability zones are restricted to the same jurisdiction as the data center used by Beekeeper. Most of our services operate in stateless mode so that in case of disaster we will provide new services, and data will be available from the database.

Our database operates with multi-availability zones to enhance durability and availability (i.e. there is the primary database which also synchronously replicates to a standby instance in a different availability zone). In case of a disaster, Beekeeper relies on the automated backups and database snapshots performed by our data center provider. Encryption at rest is implemented for all backup systems as well.

Access to Beekeeper

Beekeeper can be accessed through a number of digital interfaces. Each interface provides security settings that protect user data while ensuring accessibility.

Web browsers: Browsers only store a secure cookie which authenticates the current user. There is no local storage of customer data via this interface.

Mobile apps: On Android and iOS, access credentials are stored in the encrypted containers that the OS (operating system) provides.

Custom REST API: Beekeeper has developed a REST API and provides documentation to highlight best security practices when programming custom clients.

Connections to Beekeeper

All connections to Beekeeper are over HTTPS (TLS 1.2 and 1.3 only). Any attempt to connect over HTTP is redirected to HTTPS.

Access Control

Beekeeper considers access control as consisting of two key components:

- Authentication
- Authorization

For managing access control requirements, Beekeeper developed systems and interfaces, as well as a control dashboard.

Authentication

For internal processes, as governed by the requirements stated in our Beekeeper product and services access control principles, Beekeeper requires two-factor authentication for its employees.

For customer access, Beekeeper is able to maintain compliance with company policy where two-factor authentication is available through a single sign-on solution (SSO). Beekeeper is also able to connect to the company's identity directory, as well as consider any other type of authentication mechanism.

Authorization

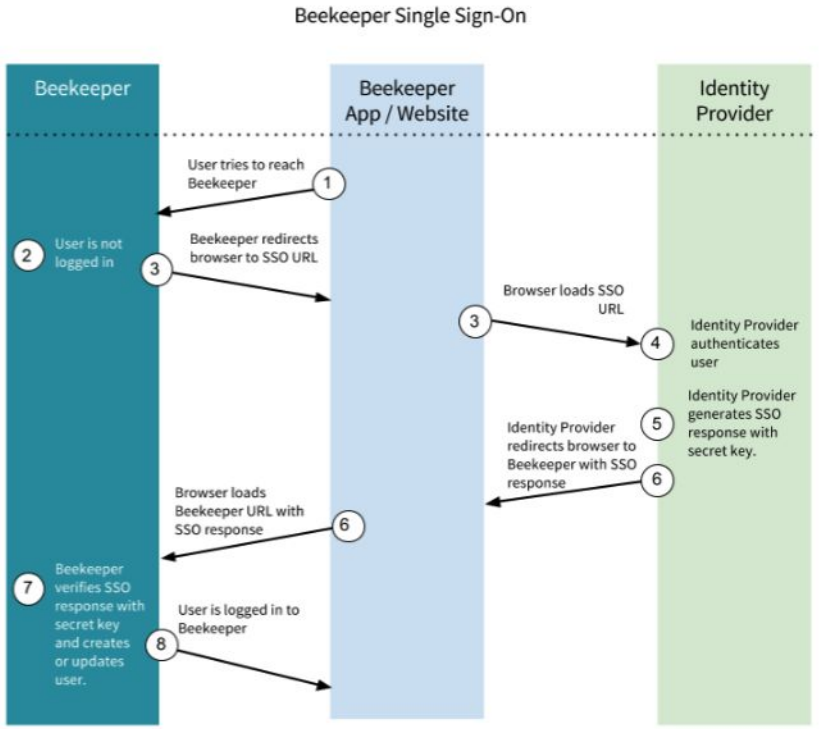
Beekeeper uses an industry standard authorization server, which is utilized for provisioning rights to Beekeeper systems. Some features of Beekeeper's authorization capabilities are available to the customer-defined administrator through the Beekeeper dashboard.

Access Control

Beekeeper Dashboard

Company-defined administrators may use the Beekeeper dashboard via secure internal communication channels to control the following user administrator functions:

- Create, update, or delete a user
- Logout an active user
- Suspend user access
- Configure SAML single sign-on
- Bulk import and update users from an Excel file



Product use Security Features

Authentication

- Login using email, phone number, or username in combination with a password
- Preset password strength (8 or more characters, upper and lowercase letters, and at least one numeric character)
- Admins can reset passwords
- After the first login there is a request to change the password
- When resetting the password, no former password can be used
- Auto logout of users after X days (number is set by administrators)
- Login to mobile app via QR code
- Alert by email about login via a one-time QR code
- Admins can log out users and suspend accounts
- The logout of a user by an admin will log out the user from every single device
- Account is locked after 10 unsuccessful login attempts

Authorization

- Every user has a role assigned, which defines what someone can do within the application (see Admin Help Center)

Product use
Security Features

- Session timeout
  - Session timeouts can be configured in the event users access Beekeeper from public computers.
- User suspension
  - Administrators can suspend users at any point. A suspended user will be immediately logged out of all clients and will lose access to all data. The data of a suspended user is retained and can be made available for forensic investigations.
- Deny- and allow-list to prevent email domains from login
- Single sign-on (SAML)
- Alert by email when logging in on a previously unknown device
- Backup
  - Regular backups of user information and all data are maintained to prevent accidental or malicious destruction.
- Roles
  - Available roles: Global Admin, Org. Unit Admin, Location Admin, Group Admin, Stream Admin, and Content Moderator (see Admin Help Center)
- Activity monitoring available through the Meta Dashboard (customer must request data access to see this information)
  - Possibility to see last login with device information
  - List with devices used to log in
- Antivirus to scan files sent within the Beekeeper app
- Disallow or restrict possibility of embedding the application within another page

Frequently Asked Questions

Q: Can data and messages be exported for internal archiving or reviewing?
A: Yes, based on a defined process, Beekeeper may give access to the data for automated archiving purposes.

Q: Are security penetration test reports available for review?
A: Yes, upon request we can share the reports of previous penetration tests.

Q: Is Beekeeper hosted on a shared cloud infrastructure?
A: Yes, but our certified data centers offer virtual private cloud (VPC) features to guarantee data isolation from other Beekeeper customers.

Q: Do you offer on-premise hosting?
A: We do not offer on-premise hosting.

Q: Is an audit log available?
A: An audit log can be made available in CSV format.

Q: Are Beekeeper's Products and Services HIPAA Security compliant?
A: The Beekeeper product and services meet the requirements outlined by HIPAA Security Controls, by having implemented an ISMS (Information Security Management System) that is certified according to information security best practices outlined by the ISO 27001 accreditation body. It is important to note that Beekeeper is an internal communication platform and not a healthcare data processing platform.

Q: How is Beekeeper's support and maintenance?
A: As a SaaS offering, Beekeeper's product is supported and maintained from Beekeeper's Zurich, Switzerland, and Krakow, Poland, Support Centers. Beekeeper also provides local help desk support services from its offices in the US and Germany, EU.

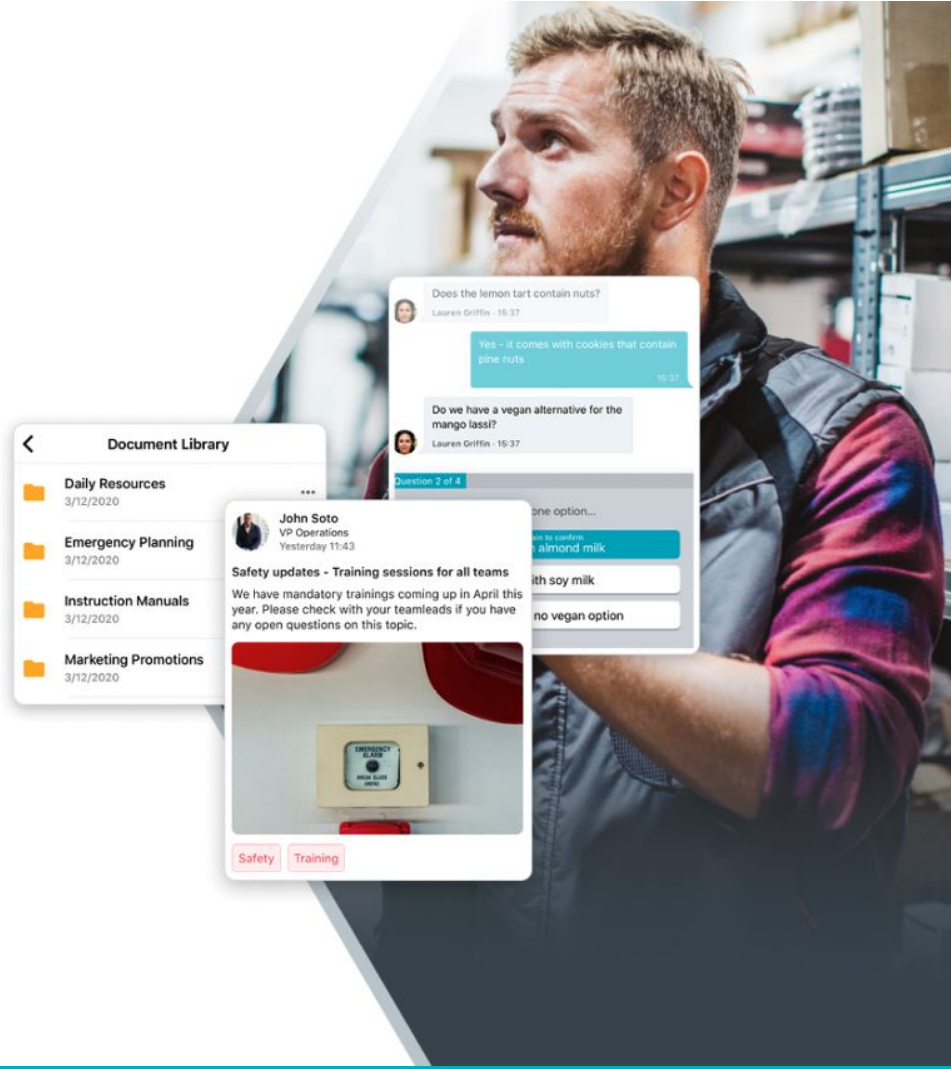
For more detailed information visit beekeeper.io/security

Contact Us
If you have further security related questions, contact us at security@beekeeper.io.

BEEKEEPER

Beekeeper is transforming the way frontline businesses work. Our frontline success system helps companies ditch paper and manual processes to improve employee engagement, retention, and performance.

Empower employees with direct access to the people, processes, and systems they need to do their best work. Companies around the world use Beekeeper to connect their teams, unify their systems and drive their businesses forward.



» Get Started

For more detailed information visit
beekeeper.io/security

Release Date (R3.1): August 2022