Cloud Security

Summary of what we do every day to guarantee that your data is safe with Ergobit and that we apply best security practices on our cloud platform.

ERGOBIT GmbH and subsidiaries

Summary

1 Backups / Disaster Recovery

- We keep 25 full backups of each database for at least 3 months: 1/day for 14 days, 1/week for 8 weeks, 1/month for 3 months.
- Backups are replicated in at least 3 different data centers, on at least 2 different countries.
- The actual locations of our data centers are specified in our Privacy Policy.
- You can also send backups of your data to your storage (if it is accessible via internet).

- You can contact our Helpdesk to restore any of those backups on your live database (or on the side).
- **Hardware failover:** for services hosted on bare metal, where hardware failure is possible, we implement local hot standby replication, with monitoring and a manual failover procedure that takes less than 5 minutes.
- **Disaster recovery:** in case of complete disaster, with a data center *entirely down for an extended period,* preventing the failover to our local hot-standby (never happened so far, this is the worst-case plan), we have the following objectives:
    - RPO (Recovery Point Objective) = 24h. This means you can lose max 24h of work if the data cannot be recovered and we need to restore your latest daily backup.
    - RTO (Recovery Time Objective) = 24h for paid subscriptions, 48h for free trials, education offer, freemium users, etc. This is the time to restore the service in a different data center if a disaster occurs and a datacenter is completely down.
    - How is this accomplished: we actively monitor our daily backups, and they are replicated in multiples locations in different countries. We have automated provisioning to deploy our services in a new hosting location. Restoring the data based on our backups of the previous day can then be done in a few hours (for the largest clusters), with priority on the paid subscriptions.
      We routinely use both the daily backups and provisioning scripts for daily operations, so both parts of the disaster recovery procedure are tested all the time.

2 Database Security

- Customer data is stored in a dedicated database - no sharing of data between clients.
- Data access control rules implement complete isolation between customer databases running on the same cluster, no access is possible from one database to another.

3 Password Security

- Customer passwords are protected with industry-standard PBKDF2+SHA512 encryption (salted + stretched for thousands of rounds).
- Ergobit staff does not have access to your password, and cannot retrieve it for you, the only option if you lose it is to reset it.
- Login credentials are always transmitted securely over HTTPS.
- During the configuration of your system, we or your system administrators even have the option to configure the rate limiting and cooldown duration for repeated login attempts.

- *Password policies:* database administrators have a built-in setting for enforcing a minimum user password length. Other password policies like *required character classes* can be configured on customer request.

4 Staff Access

- Ergobit helpdesk staff may sign into your account to access settings related to your support issue. For this they use their own special staff credentials, not your password (which they have no way to know).
- This special staff access improves efficiency and security: they can immediately reproduce the problem you are seeing, you never need to share your password, and we can audit and control staff actions separately!
- Our Helpdesk staff strives to respect your privacy as much as possible, and only access files and settings needed to diagnose and resolve your issue.

5 System Security

- All Ergobit Cloud servers are running hardened Linux distributions with up-to-date security patches.
- Installations are ad-hoc and minimal to limit the number of services that could contain vulnerabilities (no PHP/MySQL stack for example).
- Only a few trusted Ergobit engineers have clearance to remotely manage the servers - and access is only possible using an encrypted personal SSH keypair, from a computer with full-disk encryption.

6 Physical Security

Ergobit Cloud servers are hosted in trusted data centers in various regions of the world (e.g. Hetzner, OVH, Google Cloud), and they must all exceed our physical security criterions:

- Restricted perimeter, physically accessed by authorized data center employees only.
- Physical access control with security badges or biometrical security.
- Security cameras monitoring the data center locations 24/7.
- Security personnel on site 24/7.

7 Credit Card Safety

- We never store credit card information on our own systems.
- Your credit card information is always transmitted securely directly between you and our PCI-Compliant payment acquirers (see the list on our Privacy Policy page).

8 Data Encryption

Customer data is always transferred and stored in encrypted form (encryption in **transit** and **at rest**).

- All data communications to client instances are protected with state-of-the-art 256-bit SSL encryption (HTTPS).
- All internal data communications between our servers are also protected with state-of-the-art encryption (SSH).
- Our servers are kept under a strict security watch, and always patched against the latest SSL vulnerabilities, enjoying Grade A SSL ratings at all times.
- All our SSL certificates use robust 2048-bit modulus with full SHA-2 certificates chains.
- All customer data (database content and stored files) is encrypted at rest, both in production and in backups (AES-128 or AES-256)

9 Network defense

- All data center providers used by Ergobit Cloud have very large network capacities, and have designed their infrastructure to withstand the largest Distributed Denial of Service (DDoS) attacks. Their automatic and manual mitigation systems can detect and divert attack traffic at the edge of their multi-continental networks, before it gets the chance to disrupt service availability.
- Firewalls and intrusion prevention systems on Ergobit Cloud servers help detect and block threats such as brute-force password attacks.
- Customer database administrators even have the option to configure the rate limiting and cooldown duration for repeated login attempts.


ergobit
consulting