

Howwe security overview

Version 2026-10-22 · Last updated 22 October 2026

Howwe holds some of our customers' most important information: their strategy, goals and execution. This page describes how we protect it. Customers can ask for more detail, including a summary of our latest penetration test, at contact@howwe.io.

Hosting and data location

- The Howwe application and its data are hosted on Google Cloud Platform in the EU (Eemshaven, the Netherlands), with the database run by ArangoDB in the EU.
- Login runs on Auth0 in the EU.
- Traffic to the service passes through Cloudflare for encryption, protection against attacks and performance.
- All vendors that process customer data are listed, with location, on our [sub-processor list](#).

Encryption

- Data in transit is encrypted with TLS 1.2 or higher.
- Data at rest, including backups, is encrypted with AES-256. Keys are managed in Google Cloud.
- Secrets are kept in Google Secret Manager.

Access control

- Customers decide who has access and with which roles. Users only see what their role allows.
- Single sign-on with Microsoft, Google and SAML through Auth0.
- Multi-factor authentication is required for all administrative access to production systems.
- Howwe staff get access to production on a least-privilege basis, and access is removed when it is no longer needed.
- Development, test and production environments are separated.

Backup and recovery

- Automated backups run daily, are stored in the EU and are kept for up to 90 days.
- Restores are tested regularly, and recovery is practised at least twice a year.
- Recovery targets: recovery time under 4 hours, data loss under 24 hours.

Testing and monitoring

- Automated vulnerability scanning against the OWASP Top 10 runs continuously.
- An independent penetration test is carried out at least once a year and after major changes. Findings are fixed in order of severity and retested.

- The service is monitored around the clock for errors, availability and unusual activity.
- Dependencies are kept up to date, and code is reviewed before release.

Incidents

- We have a documented incident response process with clear roles.
- If a personal data breach affects a customer's data, we notify the customer without undue delay and no later than 48 hours after we become aware of it, with the information the customer needs for its own reporting.

People and vendors

- All employees and consultants sign confidentiality agreements.
- Security and data protection training is mandatory at onboarding and every year.
- Vendors that process customer data are assessed before use and bound by data processing agreements.

Standards

Howwe's security work follows the structure of ISO/IEC 27001. Howwe is not certified. Google Cloud, Auth0 and our other main vendors hold ISO 27001 and SOC 2 reports, which they publish in their trust centers.

Report a security issue

If you believe you have found a vulnerability, email contact@howwe.io with "Security" in the subject. Please give us reasonable time to fix it before you share it.

Howwe Technologies AB (publ), Grev Turegatan 30, 114 38 Stockholm, Sweden.