OBEDIENCE GLOBAL LTD

Security Overview

The concrete measures protecting your data, and the certification roadmap we are on.

Version 1.2 | Effective 28 July 2026 | Security

Owner Obedience Global Ltd board | Approved by Obedience Global Ltd board on 28 July 2026
Approval state company-approved | Next review 28 October 2026

01 Architecture

- Structured customer project records use Neon Postgres in London; file objects use a Cloudflare R2 bucket reporting Western Europe (WEUR) automatic location, which is not a single-country jurisdiction guarantee
- Tenant isolation enforced in the database itself with row-level security: one practice can never read another's rows, even if application code fails
- Fail-closed access control: an unset secret or unreachable dependency denies access, it never falls open
- Encryption in transit (TLS) everywhere, and at rest for the database, file storage and backups
- Least-privilege service roles: the application connects with a restricted database role, not an owner role

02 Operations

- Daily encrypted off-site backups with restore testing (a backup that has not been restored is a hope, not a backup)
- Key-only SSH on our servers, brute-force protection, host firewalls allowing only required ports
- Automatic security patching on platform servers
- Secrets held in environment configuration, never in source control; repository history is scanned
- Audit logging of security-relevant events in the product

03 Where we are honest about the roadmap

We are a startup, and we say so. We do not hold ISO 27001, SOC 2 or Cyber Essentials certification today, and we will never display a badge we have not earned. The near-term roadmap is Cyber Essentials first, then Cyber Essentials Plus, with ISO 27001 as the longer-term ambition. This page will change the day each one is real.

Canonical online record: https://obedience.global/policies/security