Security and compliance

OPEREX is built for continuous-process, hazardous (Seveso-class) sites — where data confidentiality, audit trail and data residency are not optional. The following are measured, enforced properties of the product.

Data isolation and access

- Tenant isolation enforced at the database level (Row-Level Security, FORCE), not just in the app.
- Role-based access per organisation, with custom roles and a permission matrix.
- Site-level access list — a user only sees the sites entrusted to them.

Audit trail (in the spirit of ISO 45001 §10.2)

- Append-only audit log: entries recorded with timestamp, author, immutably.
- The diary and reports produce a canonical, versioned PDF artifact (old versions retained).
- User login history; sensitive operations logged.

Data residency and deployment

- EU data residency; self-hosted, even air-gapped (Docker) deployment on Enterprise.
- Portable data layer (standard PostgreSQL) — no vendor lock-in; your own identity provider (SSO) can be wired in.
- Object storage (S3/MinIO) for diaries/images, with authenticated access.

Platform hardening

- HTTPS everywhere (HSTS), content security policy (CSP), security response headers.
- Login/password-reset/API rate-limited; invite-only registration.
- Secrets in environment variables (never in code); firewall + least-privilege DB role.

> Compliance statements are verifiable technical properties. An external pentest can be scheduled before the first Enterprise rollout. Contact us for details.