

Information Security Policy

The top-level policy: scope, roles, and the requirements every other policy expands on.

Version 1.1 · Last reviewed 22 October 2026 · Owner: Security Lead, security@etropo.com · Current version at <https://trust.etropo.com/resources/information-security-policy>

1. Purpose and scope

This policy sets the framework for protecting the information Etropo holds: customer budget data, the personal data of the people who use the product, and the credentials and keys that protect both. It applies to everyone who works for or with Etropo, to every system that supports the service (production, preview and development), and to every vendor that processes customer data on Etropo's behalf.

The policies listed under Resources expand on specific areas. Where this policy and a specific policy differ, the specific policy applies.

2. Commitments

Etropo commits to:

- protect the confidentiality, integrity and availability of customer data;
- store customer data in the European Union;
- apply the principle of least privilege to every person and system;
- ship changes only through reviewed, tested, reversible deployments;
- tell customers about security incidents that affect them, and about new vendors before they process their data;
- say publicly which controls are in place and which are not.

3. Roles and responsibilities

Security Lead. The founder responsible for engineering owns this policy, approves exceptions, owns incident response and reports on security to the other founders at least quarterly. The Security Lead is reachable at security@etropo.com.

Engineering. Everyone who writes or deploys code implements the controls in the Secure Development Policy, keeps dependencies current, and reports suspected incidents immediately.

All personnel and contractors. Follow this policy and the Acceptable Use Policy, protect their credentials, use customer data only for the task at hand, and report anything that looks wrong.

4. Access control

Summarised here; the Access Control Policy has the detail.

- Customer accounts are protected by Supabase Auth: bcrypt-hashed passwords with a 12-character minimum, screened against known breaches (Have I Been Pwned), one-hour access tokens with rotating refresh tokens, a Cloudflare Turnstile check on sign-in and sign-up, and optional two-factor authentication with an authenticator app. Once a user enrolls a second factor, the proxy, the API layer and the database each refuse a session that has not presented it. Idle browsers are signed out after 15 minutes, and authentication cookies expire after at most 14 days.
- Within an organisation there are two roles, admin and user. Admins can limit users to specific budget categories. Both checks run in the database through Row Level Security, which is enabled on every table.
- Access to production consoles (Vercel, Supabase, GitHub, Stripe, the domain registrar) requires an individual account with multi-factor authentication. There are no shared logins. Access is reviewed quarterly and removed on the day a person leaves.

5. Data protection

Summarised here; the Data Management Policy and the Cryptography Policy have the detail.

- Data is classified as Highly Confidential, Confidential, Internal or Public, and handled according to its class.
- All traffic is encrypted in transit with TLS and HSTS. Data at rest is encrypted by the provider. OAuth tokens for connected services are additionally encrypted at the application level with AES-256-GCM.
- The production database and file storage run in AWS eu-central-1 (Frankfurt); serverless functions run in Vercel's fra1 region.
- Customers can export their budgets at any time. Deletion requests are completed within 30 days.
- Vendors that process customer data are listed publicly with the data they receive, and changes are announced before they take effect.

6. Application and infrastructure security

- Etropo operates no servers of its own. The application runs on Vercel and the database on Supabase; both hold SOC 2 Type II reports and patch their platforms.
- Every response carries a Content Security Policy and the standard browser security headers.
- Sensitive endpoints are rate-limited. Webhooks are verified against their signing secrets. Cron jobs require a secret.

- Secrets live in environment variables, separated between production and preview, and are never committed to source control.
- Preview deployments require a Vercel team login.

7. Secure development and change management

Every change is a pull request with automated type checking, linting and tests, a preview deployment, and an atomic production deployment on merge that can be rolled back in one click. Dependencies are monitored by GitHub Dependabot. See the Secure Development Policy.

8. Monitoring and logging

Application errors are captured by Sentry in its EU region and alert the engineering channel. Integration syncs, token operations and webhook deliveries are written to audit tables. Platform logs are kept by Vercel and Supabase for their plan retention periods. See the Data Management Policy for retention.

9. Incident response

Incidents are classified P0 to P3 with response targets from 15 minutes to 24 hours. Personal data breaches are notified to affected customers without undue delay and to supervisory authorities within 72 hours where required. See the Security Incident Response Plan.

10. Business continuity

Recovery objectives: application within 1 hour with no data loss (rollback), database within 4 hours with at most 24 hours of loss (daily backup). See the Business Continuity and Disaster Recovery Plan.

11. Personnel

- Everyone with production access completes security awareness training on joining and annually.
- Personnel and contractors sign a confidentiality agreement before they receive access to customer data.
- Laptops used for production access have full-disk encryption and automatic screen lock. Customer data is not stored on personal devices.

The Controls page states honestly which of these are in place today.

12. Vendors

Vendors that process customer data are chosen with a preference for SOC 2 Type II or ISO 27001 reports, are covered by a data processing agreement, and are reviewed annually. See the Vendor Management Policy.

13. Risk management

Risks to customer data are assessed at least annually and whenever the architecture changes, rated for likelihood and impact, and assigned an owner and a treatment. See the Risk Management Policy.

14. Compliance

Etropo processes personal data under the GDPR as a processor for its customers' budget data and as a controller for account and billing data. The programme described on this site is run against the SOC 2 Trust Services Criteria (Security, Availability, Confidentiality) in preparation for a Type II audit.

15. Exceptions

Exceptions to this policy need the Security Lead's written approval, a business reason, a compensating control and an expiry of at most 90 days. Nothing required by law can be excepted.

16. Review

This policy is reviewed at least once a year and after any P0 or P1 incident, major architectural change or change in law. Versions are kept in Git.

Version	Date	Change
1.0	September 2025	First version
1.1	May 2026	Two-factor enforcement at proxy, API and database layers
1.1 (public)	October 2026	Published on the Trust Center; wording aligned with the supporting policies