

Access Control Policy

Who gets access to what, how it is granted, reviewed and removed, for customers and for Etropo personnel.

Version 1.0 · Last reviewed 22 October 2026 · Owner: Security Lead, security@etropo.com · Current version at <https://trust.etropo.com/resources/access-control-policy>

1. Purpose

Access to customer data and to the systems that hold it is limited to the people and services that need it for a specific task, for as long as they need it, and no further. This policy says how that is done for customers using the product and for Etropo personnel operating it.

2. Customer accounts

Identity. A user signs in with an email address and password, or with a Google account. Supabase Auth stores passwords as bcrypt hashes; Etropo never sees or stores a plain-text password.

Password policy. New passwords — at sign-up and on every password change — must be at least 12 characters and are screened against known breach corpora (Have I Been Pwned); a password that appears there is rejected. Both checks are enforced server-side by Supabase Auth; the sign-up form mirrors the length rule.

Sessions. Access tokens expire after one hour. Refresh tokens rotate on every use, so a stolen refresh token stops working as soon as the legitimate client refreshes. Authentication cookies carry a rolling 14-day maximum age, and an automated test fails the build if any client would issue a longer-lived cookie.

Idle sign-out. A browser left without user activity for 15 minutes is signed out automatically, with an on-screen warning two minutes before. Activity in any tab of the browser resets the clock, so someone actively working is never interrupted — only an unattended machine locks itself. The sign-out ends the session on that browser only; the user's other devices are unaffected.

Bot protection. Sign-in and sign-up require a Cloudflare Turnstile challenge, verified by Supabase Auth on the server.

Two-factor authentication. Any user can enrol up to two authenticator-app (TOTP) devices. Once one is enrolled, every access path requires it:

- the proxy redirects a session without the second factor to the verification step;
- organisation-scoped API routes refuse the request;

- Row Level Security policies in the database return no rows until the session carries the second factor;
- the OAuth consent page for MCP clients requires it before consent.

Removing a device, adding a second one and changing a password require the second factor again.

Sign-up controls. A database hook runs before any account is created, on every path including Google sign-in and invitations, and refuses email domains on the blocklist (disposable-email providers and domains blocked after abuse).

3. Authorisation inside an organisation

- Each organisation has **admins** and **users**. Admins manage members, billing, integrations, budget structure and the deletion of budgets and categories. Users work within the budgets they are given.
- Admins can restrict a user to specific **budget categories**. The restriction is evaluated by database functions bound to the organisation, so a category from another organisation can never be granted.
- Every table in the application schema has **Row Level Security** enabled. Policies tie each row to its organisation and check the caller's membership on every statement.
- Server-side code that must bypass Row Level Security (scheduled syncs, the Slack and Teams assistants) is restricted in TypeScript to the organisation it acts for, and reads are filtered to the user's category access. Those paths are covered by tests that fail if the filter is removed.
- AI features read data through the same access rules as the user who asks.

4. Personnel access to production systems

Systems in scope. Vercel (hosting, environment variables, logs), Supabase (database, authentication, storage), GitHub (source code), Stripe (billing), the domain registrar and DNS, and the consoles of every vendor on the Subprocessors page.

Rules.

- One account per person. No shared logins.
- Multi-factor authentication on every system that offers it. All systems in scope do.
- Least privilege: the lowest role that lets the person do their job. Owner or admin roles are limited to the Security Lead and the Infrastructure Lead.
- Access to the production database outside the application is limited to the Security Lead and is used for support and operations only. Queries that change data are made through migrations kept in Git.
- Secrets are read from the environment of the system that needs them. They are not copied into chat, email, documents or personal devices.

Provisioning. Access is granted on joining, per role, using a checklist that names every system in scope. The checklist is kept with the person's onboarding record.

Removal. On the day a person leaves, their access to every system on the checklist is removed, and any shared secret they could have seen is rotated.

5. Access review

Every quarter the Security Lead lists every person with access to each system in scope, confirms each is still needed, removes what is not, and records the review. Reviews have run since the third quarter of 2026.

6. Customer-connected integrations

When a customer connects Google Ads, LinkedIn, Meta, TikTok, Google Sheets, Notion, HubSpot, Attio or Slack, the connection uses OAuth 2.0 with a cryptographically random state value, requests the minimum scopes for the feature, and stores the tokens encrypted. Any admin of the organisation can disconnect an integration at any time, which revokes Etropo's access.

7. Review

Reviewed annually with the Information Security Policy. Version 1.0, October 2026.