Flowsight

Access Controls Policy

Effective: 2026-04-29 · Owner: hugocodes1997@gmail.com

This document defines the access controls Flowsight operates over its production environment, source code, and consumer financial data. The principle is least privilege: every actor — human or system — receives the minimum access needed to do its job, and that access is reviewed continuously.

1. Scope

This policy covers production assets (Vercel deployments, Supabase production database, GitHub repository), API credentials (Plaid, Anthropic, Resend, Google OAuth, Supabase keys, NextAuth secret, cron secret), and consumer financial data received via Plaid, the Apple Card CSV uploader, and the Gmail receipt parser.

2. Access tiers

- End user — signed-in account holder. Sees only their own data, scoped by user_id derived from a verified NextAuth session.
- Operator (developer) — single individual responsible for the service. Has access to Vercel deployments, the Supabase production project, the private GitHub repository, and provider dashboards (Plaid, Anthropic, Resend, Google Cloud).
- Service principals — Vercel runtime, cron schedulers, sub-processors. Each holds only the credential it needs (e.g. the Vercel runtime holds the Supabase secret key but not the Anthropic key for clients).

3. Application-layer access control (RBAC)

- Every API route in the Next.js app validates the NextAuth session before any database read or write. Routes return 401 on missing or invalid sessions.
- All database queries filter by user_id from the verified session — never from request input. This prevents cross-user data access (IDOR) even if a route handler is misconfigured.
- AI chat tools are factory-bound to the signed-in user's ID at request time, so the LLM cannot query other users' data through tool inputs.
- Cron endpoints (/api/cron/sync, /api/cron/daily-brief) are gated by a Bearer token matching CRON_SECRET; they cannot be triggered from a browser session.

4. Database access

- Production data lives in a managed Supabase Postgres project. Disks are encrypted at rest by the provider (AES-256).
- Two-tier API key model: a publishable key (sb_publishable_...) is exposed only for client-safe operations and grants no direct table access; a secret key (sb_secret_...) is held server-side only

and never sent to the browser.

- The secret key is stored as an encrypted env var in Vercel and is not committed to source control.
- The operator has admin access to the Supabase dashboard, protected by MFA (see §6).

5. Production asset access

- Hosting (Vercel): only the operator's Vercel account can deploy, view logs, or modify environment variables. MFA enforced.
- Source code (GitHub): private repository. Only the operator has push access. MFA enforced via GitHub's account security settings.
- Database (Supabase): only the operator's Supabase account can read or modify data via the dashboard. MFA enforced.
- Provider dashboards (Plaid, Anthropic, Resend, Google Cloud): each accessible only to the operator with MFA enforced.
- No SSH access. No bastion host. Production is a managed serverless platform with no direct shell access required.

6. Authentication and MFA

- End users authenticate via Google OAuth (NextAuth v5). Flowsight does not store passwords. Phishing-resistant MFA is supported by the Google Sign-In flow (passkeys, hardware security keys, platform biometrics).
- Operator authentication to admin tools (Vercel, GitHub, Supabase, Google Cloud, Plaid, Anthropic, Resend) requires multi-factor authentication on each provider account.
- Sessions are stateless JWTs signed with NEXTAUTH_SECRET (256-bit random, generated via openssl rand -base64 32) and have a finite lifetime.

7. Secret management

- All secrets are stored as encrypted environment variables in Vercel: PLAID_CLIENT_ID, PLAID_SECRET, ANTHROPIC_API_KEY, RESEND_API_KEY, GOOGLE_CLIENT_ID, GOOGLE_CLIENT_SECRET, SUPABASE_SECRET_KEY, NEXTAUTH_SECRET, CRON_SECRET.
- Secrets are scoped per environment (Production, Preview, Development) and are not shared across environments.
- No secret is ever written to source control. The .gitignore excludes .env, .env.local, and any local secret artifacts.
- Secrets are rotated by replacing the corresponding env var and redeploying; no application code change is required for rotation.

8. Onboarding and offboarding

- Flowsight is operated by a single individual; there are no employees to onboard or offboard.
- If additional operators are added in the future, access will be granted by adding them to the relevant provider teams (Vercel, GitHub, Supabase) under their existing accounts; offboarding will mean removing them from those teams and rotating shared secrets.

9. Access review

As a single-operator service, the operator's access list is reviewed continuously by the operator. Should additional operators be added, a quarterly review will be added to the operations cadence covering all provider dashboards and the GitHub repository.

10. Audit and logging

- Vercel logs all incoming requests with paths, status codes, and identifiers. Logs are accessible only to the operator.
- Supabase logs all administrative dashboard actions and SQL operations (within retention windows).
- GitHub logs all repository access and modifications.
- Provider dashboards (Plaid, Anthropic, Resend, Google Cloud) each maintain their own audit logs accessible to the operator.

11. Incident response

If unauthorized access is suspected or confirmed, the operator immediately rotates all relevant secrets via the Vercel dashboard, redeploys, revokes any compromised provider tokens, and notifies affected users by email within 72 hours. See the Information Security Policy for the full incident response procedure.

12. Contact

Questions or access requests: hugocodes1997@gmail.com

This document is reviewed continuously and updated as Flowsight's access model evolves. Generated programmatically and served as a static asset from flowsight-delta.vercel.app/access-controls-policy.pdf.