Flowsight

Information Security Policy

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

Flowsight is a personal financial dashboard that consolidates data from accounts the user explicitly connects. This document describes our information security program: the controls we operate, how data flows through the system, and how we respond to incidents. The principle is least privilege — every component sees only the data it needs, credentials are isolated by environment, and no secret ever leaves the server.

1. Authentication

- All sign-in is handled via Google OAuth using NextAuth (v5). Flowsight never sees, stores, or transmits user passwords.
- Sessions are stateless JWTs signed server-side with a high-entropy secret (NEXTAUTH_SECRET, 256-bit, generated with openssl rand -base64 32).
- Bank credentials are entered into Plaid Link, an iframe served directly by Plaid. They never enter Flowsight servers.
- Plaid Link OAuth flows for OAuth-required institutions (Chase, BofA, etc.) are routed through Plaid's redirect URI mechanism, not through Flowsight.

2. Authorization

- Every API route validates the NextAuth session before any database read or write. Routes return 401 on missing or invalid sessions.
- Database queries always filter by user_id derived from the verified session — never from request input. This prevents IDOR even if route handlers are misconfigured.
- Cron endpoints (/api/cron/sync, /api/cron/daily-brief) require an Authorization: Bearer token matching CRON_SECRET. Stored as encrypted env var; never logged.
- AI chat tool definitions are factory-bound to the signed-in user's ID at request time, so the LLM cannot query other users' data even if its tool inputs were manipulated.

3. Data in transit

- All client connections use HTTPS / TLS 1.2 or higher, terminated at Vercel's edge.
- Server-to-Plaid, server-to-Supabase, server-to-Anthropic, and server-to-Resend calls all use HTTPS with certificate validation.
- Sensitive views are server-rendered. Sensitive data is computed on the server and rendered into HTML rather than fetched by client-side JavaScript, reducing the surface area where data could be intercepted.

4. Data at rest

- Production database is managed Postgres on Supabase. Disks are encrypted at rest by the provider (AES-256).
- Database access uses the new Supabase secret-key API scheme (sb_secret_...). Held only on Vercel servers as an encrypted env var. The publishable key is scoped for client-safe operations only and never grants direct table access.
- Plaid access tokens are stored server-side in the plaid_items table and never sent to the browser.
- No fields are stored in plaintext that should not be — credentials, OAuth tokens, and Plaid access tokens are protected by access-control rather than column-level encryption (acceptable given single-key-per-database model).

5. Secret management

- All secrets — Plaid client/secret, Anthropic API key, Resend API key, Google OAuth client secret, Supabase secret key, NextAuth secret, cron secret — are stored as encrypted env vars in Vercel.
- No secret is ever committed to source control. The repository is private. .gitignore excludes .env files and any local secret artifacts.
- Secrets are scoped per environment (Production / Preview / Development) so non-production environments cannot access production keys.
- Rotation: secrets can be rotated by replacing the env var and redeploying; no application code changes required.

6. Network and infrastructure

- Hosted on Vercel's managed serverless platform. No self-managed servers, no SSH access, no shared infrastructure.
- Database is in a private network managed by Supabase; only the Vercel server is authorized to connect.
- No public database endpoint exposed; no SSH-accessible bastion.
- DDoS and WAF protections inherited from Vercel and Supabase platform defaults.

7. Logging and monitoring

- We do not log raw transaction descriptions, account numbers, balances, OAuth tokens, or other sensitive content.
- Operational logs (request paths, status codes, error messages) are retained by Vercel for 24 hours by default and accessible only to the developer.
- Errors include enough context to debug without exposing PII.

8. Sub-processor security

- Plaid (account aggregation) — SOC 2 Type 2 and ISO 27001 certified. Bank credentials never reach Flowsight.
- Supabase (database) — SOC 2 Type 2 certified; daily encrypted backups.

Vercel (hosting) — SOC 2 Type 2 certified; managed serverless platform.

- Anthropic (AI chat + receipt parsing) — SOC 2 Type 2 attestation; does not train on API data by default.
- Resend (email) — used only for opt-in transactional email (daily brief).
- Google (auth + optional Gmail) — Google Identity Platform; OAuth scopes narrowed to the minimum required.

9. Vulnerability management

- Dependencies monitored continuously via npm audit and GitHub Dependabot security advisories.
- Critical-severity advisories are patched as a priority; moderate-severity advisories are evaluated for exploitability and patched on a normal cycle.
- Application is rebuilt and redeployed on every commit to main, so dependency updates ship as soon as merged.
- Security issues can be reported privately by email to hugocodes1997@gmail.com.

10. Incident response

- In the event of a confirmed security incident, the developer is the responder. Initial acknowledgment within 48 hours of discovery.
- Affected users notified by email within 72 hours of confirming the incident, with description of what was affected and remediation status.
- Post-incident review documents root cause and prevention measures.

11. Data minimization and retention

- We collect only data the user explicitly grants (Google profile, Plaid-provided account/transaction data, optional Gmail receipts, optional Apple Card CSVs).
- Data is retained while the account is active and deleted on user request. Disconnecting a Plaid institution cascades-deletes its transactions and accounts.
- Account deletion: user emails the contact address; all rows associated with the user_id are removed within 30 days.

12. Continuous improvement

This program is reviewed and updated as the application evolves. New sub-processors are added to the Privacy Policy before being put into production. Significant changes to the security model are reflected in the Security page on the website and in this document.

Contact

Security questions, vulnerability reports, or compliance review: hugocodes1997@gmail.com

---

This document reflects Flowsight's information security program as of the effective date and is reviewed continuously. Generated programmatically and served as a static asset from flowsight-delta.vercel.app/security-policy.pdf.