GWP Security Overview

Growing Wealth Platform · Last updated: June 11, 2026

1. Purpose

This document describes the security architecture and data handling practices of GWP for compliance and vendor review purposes.

2. Platform overview

GWP is a wealth intelligence platform for licensed financial advisors. It is not a financial advisor, broker-dealer, or bank.

3. Infrastructure (US-hosted)

Component	Provider
Web application	Vercel
Database	Neon PostgreSQL
Plaid/metrics service	Fly.io (US: sjc)
Authentication	Clerk
Email	Resend
File uploads	UploadThing
Error monitoring	Sentry

4. Data encryption

- Industry-standard encryption at rest and in transit via infrastructure vendors
- HTTPS enforced on all production endpoints
- Plaid access tokens stored server-side; never exposed to client application

5. Access controls

- Clerk authentication on all protected routes
- Consumer data scoped to authenticated user profile
- Advisor access requires org membership, workspace permissions, client linkage
- No cross-client data access

6. Plaid integration

Enabled products: Transactions, Liabilities, Auth (depository).

Not enabled: Payment Initiation, Transfer, Identity Verification.

GWP does not initiate money movement or modify financial accounts. Bank credentials are handled by Plaid Link and not stored by GWP.

7. Subprocessors

- Plaid — financial account connectivity
- Clerk — authentication
- Neon — database hosting
- Vercel — application hosting
- Fly.io — Plaid/metrics backend
- Resend — email delivery
- Sentry — error monitoring
- UploadThing — document storage

8. Data retention and deletion

Data retained only as necessary to provide services or meet legal obligations. Deletion requests: help@joingwp.com or security@joingwp.com. Plaid disconnect removes tokens and associated records.

9. Contact

security@joingwp.com