Flattnd

Bank Data, Distilled.

Security & Compliance Brief

Confidential — April 2026

Prepared for: Prospective Evaluation Partners

1. Executive Summary

Flattnd is a specialized financial data extraction platform built for Treasury Management. We convert commercial bank account analysis PDFs into structured, pivot-ready Excel files. This document outlines our security architecture, data handling practices, and compliance posture.

2. Infrastructure

Layer	Provider	Certification
Edge Security & DNS	Cloudflare	SOC 2 Type II, ISO 27001
Application Hosting	Vercel	SOC 2 Type II
Database	Supabase (PostgreSQL on AWS)	SOC 2 Type II, AES-256 at rest
Email Delivery	Resend	DKIM + SPF verified

- All traffic encrypted via TLS 1.3
- Cloudflare WAF enabled with SQL injection and XSS protection
- HSTS enforced on all domains
- AI training bots blocked at the edge

3. Data Handling

"The Vault" Architecture

- Source PDFs are processed entirely in-memory — they are never written to disk and never stored
- Only the structured extraction output (Excel format) is persisted in the encrypted database
- PDF data exists in memory only during the extraction process (typically 2–5 seconds)
- No PDF content is logged, cached, or retained after processing
- Extracted Excel files are subject to a 30-day automated retention policy — records older than 30 days are purged from the database at each deployment cycle
- Users may manually delete individual extraction records at any time

Data at Rest

- PostgreSQL database encrypted with AES-256
- Hosted in AWS us-east-1 (N. Virginia)
- Automated backups managed by Supabase

4. Authentication & Access Control

- Passwordless authentication via magic link email (no passwords stored)
- Single-use, time-limited tokens (15-minute expiry)
- Double-click protection: prevents email scanners from consuming login tokens
- Invite-only — users must be explicitly whitelisted by an administrator
- Per-user data isolation — users can only access their own extractions
- 7-day session expiry with manual sign-out

5. Audit Trail

Attribute	Details
User Identifier	Email address
Action Type	Login, upload, export, sign-out
Source IP Address	IPv4 / IPv6 of requesting client
Timestamp	UTC, per event

Logs retained in database and available for compliance review.

6. Organizational Controls

- Code hosted in private GitHub repository with restricted access
- CI/CD deployment via Vercel with automatic builds on code push
- No third-party analytics or tracking scripts
- No client-side data storage (localStorage / cookies not used)
- Domain verified with DKIM and SPF for email authenticity

7. Current Scope & Roadmap

Current (Private Beta)

- Commercial bank Account Analysis Statement extraction
- User-level data isolation with full audit trail
- 30-day automated retention policy with user-initiated deletion

Planned

- Multi-bank support across major commercial banks
- Organization-level multi-tenancy with role-based access control
- SOC 2 Type II certification
- Configurable retention windows per organization