Tapify Security Overview

This document provides an overview of Tapify's hosting infrastructure and security practices, to demonstrate compliance readiness for integration with Plaid and Dwolla.

Hosting

Tapify uses fully cloud-hosted infrastructure:

1. Frontend & API Routes: Hosted on Vercel (Next.js framework).
2. Database & Authentication: Hosted on Supabase (PostgreSQL + Row-Level Security).
3. No on-premises infrastructure is used.
4. Both Vercel and Supabase provide SOC 2 Type II compliant infrastructure.

Security Practices

1. All data in transit is encrypted via TLS 1.2+.
2. All data at rest is encrypted using AES-256.
3. Supabase Row Level Security (RLS) is enabled on all sensitive tables.
4. Access to project resources is restricted to authorized team members with Multi-Factor Authentication (MFA).
5. Source code and deployments are managed via GitHub + Vercel with role-based access control.

Monitoring & Logging

1. Supabase provides audit logs for database access and modifications.
2. Vercel provides analytics, error tracking, and deployment history.
3. System-level events are logged in the Tapify `logs` table for audit and debugging purposes.

Compliance Alignment

Tapify aligns its practices with industry standards for cloud-hosted applications. This includes encryption, access control, monitoring, and the principle of least privilege. Tapify does not store sensitive bank credentials directly. All account authentication and payments are handled securely via Plaid and Dwolla APIs.