Information Security Policies – PMSOX LLC (Last updated: January 26, 2026)

1. Information Security Policy (ISP)

This policy outlines the approach and controls in place to ensure the confidentiality, integrity, and availability of data handled by our application.

Owner / Founder: Omar El Mghari
Company: PMSOX LLC

1. Systems & Hosting
- Infrastructure is hosted on Vercel (frontend) and Firebase (auth, database).
- Monitored via GitHub-based CI pipelines.

2. Authentication
- Clerk handles user authentication with strong password policies.
- Internal tools (GitHub, Stripe, Plaid, etc.) use multi-factor authentication (MFA).

3. Access Control
- Only Omar has access to production systems.
- Secrets are stored via Vercel's secret manager and secured `.env` files.
- Source code resides in private GitHub repositories.

4. Encryption
- HTTPS (TLS 1.2+) for all data in transit.
- Firebase and Vercel encrypt data at rest.

5. Change Management
- Version-controlled production code deployed through CI/CD (GitHub Actions).
- Security updates are applied within 24–48 hours.

6. Incident Response
- Errors and failures are logged; manual incident response playbook in place.

7. Privacy
- No Plaid bank data is stored. Users can delete data anytime.

2. Access Control Policy

This policy governs how access to systems and data is controlled and reviewed.

Owner: Omar El Mghari

1. Least Privilege Principle
- Only Omar has access to production systems, code, and secrets.

2. Authentication
- 2FA is enforced on all systems including GitHub, Firebase, Clerk, Vercel, Stripe, and Plaid.

3. Access Review
- Access logs are reviewed every 6 months on GitHub, Vercel, and Firebase.

4. Offboarding / Termination
- No current employees. If team members are added, access will be provisioned and revoked via GitHub and Vercel org controls.

Last updated: January 26, 2026

3. Data Deletion & Retention Policy

This policy outlines how PMSOX LLC handles the retention and deletion of user and system data.

1. Data Retention
- User activity logs and financial metadata (non-PII) are retained for audit purposes for up to 7 years.
- Plaid and Stripe transaction references are retained for 1 year unless otherwise required for compliance.

2. Data Deletion
- End-users may request account or transaction deletion at any time.
- All user requests are handled within 7 days, with full purging from Firebase and Stripe-linked metadata.

3. Data Scope
- We do not store bank credentials or transaction-level data pulled from Plaid.
- Minimal metadata (e.g., Plaid item ID, access token reference) is encrypted and deleted upon disconnection.

4. Secure Deletion
- Firebase data is removed using the Admin SDK.
- All deletions are logged for audit and verified post-deletion.

4. Security Practices Summary

This summary outlines our key security practices to comply with data access partners such as Plaid.

1. Authentication
- All accounts require 2FA (enabled via GitHub, Clerk, Firebase, and Stripe).

2. Secure Storage & Secrets
- All secrets are stored in Vercel's encrypted secret manager and never committed to Git.

3. Encryption
- Data in transit uses TLS 1.2+.
- Data at rest in Firebase and Stripe is encrypted by default.

4. Least Privilege & Auditing
- Only the founder has admin access. GitHub, Firebase, and Stripe logs are reviewed monthly.

5. Data Access & Deletion
- Users can revoke Plaid or Stripe access at any time.
- Data deletion is handled programmatically and logged.

6. Infrastructure
- All infrastructure is hosted in the cloud (Firebase, Vercel), with managed patches and uptime monitoring.

7. Incident Response
- Errors are logged and critical failures trigger alerts.
- Incident playbook is in place to address webhook or financial sync errors.

5. Zero Trust & Encryption Policy

This policy defines our approach to identity-first security using zero trust architecture and encryption.

1. Zero Trust Principles
- All access is denied by default unless explicitly granted.
- Authenticated sessions are validated continuously.

2. Identity Verification
- Users are authenticated using Clerk and Firebase JWT tokens.
- Internal services check claims and roles for every sensitive operation.

3. API Gateways
- API access is restricted via secure tokens and IP limitations when feasible.

4. Encryption
- HTTPS is enforced across all endpoints.
- Firebase encrypts all data at rest using AES-256.
- Secrets are injected at runtime from Vercel's environment store.

5. Device Trust (Future-proofing)
- Will evaluate secure device ID validation and user-agent checks as the team grows.