Information Security Policy (Sole Proprietor)

Last updated: 2026-02-17

1. Purpose
This policy defines how the Spending Tracker sole proprietorship identifies, mitigates, and monitors information security risks for systems that process consumer financial data.

2. Scope
- All production and non-production systems used by the Service.
- All application code, secrets, logs, databases, backups, and third-party integrations (including Plaid).
- Applies to the owner/operator and any future contractors.

3. Governance
- Policy owner: business owner (sole employee).
- Review cadence: at least annually and after major incidents or architecture changes.
- Security decisions and exceptions are documented in project records.

4. Asset and Data Classification
- Sensitive data includes authentication credentials, financial account/transaction data, Plaid tokens, and security logs.
- Sensitive data is handled using least privilege and encryption controls.

5. Access Control
- Production access is limited to the owner.
- Unique accounts are required for infrastructure and source-control providers.
- MFA is required on critical systems (code hosting, deploy platform, Plaid dashboard, database provider).
- Secrets are stored in managed environment variable systems; no hard-coded production secrets in source.

6. Authentication and Session Security
- End-user sessions use secure HTTP-only cookies.
- CSRF protections are enforced for state-changing requests.
- Passwords are hashed and never stored in plaintext.
- MFA support is being implemented for end users; rollout is phased and documented.

7. Cryptography
- Data in transit uses TLS 1.2+.
- Plaid access tokens and sensitive credentials are encrypted at rest.
- Encryption keys and JWT secrets are rotated periodically and after exposure.

8. Vulnerability and Patch Management
- Operating systems and dependencies are patched regularly.
- Dependency updates and security advisories are reviewed routinely.
- Endpoint/device security controls (OS updates, disk encryption, anti-malware) are maintained on operator machines.
- Vulnerability scans and remediation tracking are performed and documented.

9. Logging, Monitoring, and Alerting
- Security-relevant events are logged via structured logs and audit events.
- Health, error-rate, and latency alerts are configured.
- Uptime monitoring is active for public health endpoints.

10. Incident Response
- Incidents are triaged using the documented runbook.
- Containment, recovery, and communication steps are followed.
- Post-incident review is completed with corrective actions tracked.

11. Data Retention and Deletion
- Retention and deletion controls exist for user-scoped data.
- Data deletion requests are honored according to applicable law.
- Retention policy is reviewed periodically and updated as needed.

12. Vendor and Third-Party Management
- Third-party services are limited to required providers (hosting, database, Plaid, monitoring).
- Security settings are reviewed before enabling new providers.
- Access scopes and credentials are minimized.

13. Change Management
- Production-affecting changes are version-controlled.
- Deployments follow runbook checks and rollback readiness.
- Security-impacting changes are reviewed before release.

14. Compliance and Policy Exceptions
- Applicable privacy/security laws and Plaid requirements are considered during operations.
- Exceptions must be documented with business justification, risk assessment, and remediation timeline.