

# Finance Guru Information Security Policy

**Effective Date:** December 22, 2025

**Last Reviewed:** December 22, 2025

**Next Review Date:** June 22, 2026

**Policy Owner:** Finance Guru Development Team

**Classification:** Internal

## 1. Purpose

This policy establishes the information security framework for Finance Guru, defining procedures to identify, mitigate, and monitor information security risks. It ensures the confidentiality, integrity, and availability of user financial data accessed through Plaid and other integrations.

## 2. Scope

This policy applies to:

- All Finance Guru application components and infrastructure
- All data processed, stored, or transmitted by the application
- All development, deployment, and operational procedures
- Third-party integrations (Plaid, hosting providers, etc.)

## 3. Security Governance

### 3.1 Roles and Responsibilities

Role	Responsibilities
Policy Owner	Maintain policy, conduct reviews, approve changes
Development Team	Implement security controls, secure coding practices
Operations	Monitor systems, respond to incidents, maintain infrastructure

### 3.2 Policy Review Cycle

- **Quarterly:** Security control effectiveness review
- **Semi-annually:** Full policy review and update
- **Annually:** Third-party security assessment
- **Ad-hoc:** Following security incidents or significant changes

## 4. Risk Identification

### 4.1 Risk Assessment Process

Finance Guru conducts ongoing risk identification through:

#### 1. Threat Modeling

- Identify assets (user data, credentials, tokens)
- Identify threat actors (external attackers, insider threats)
- Map attack vectors (API abuse, injection, credential theft)
- Document in threat model registry

#### 2. Vulnerability Scanning

- Automated dependency scanning (npm audit, Snyk)
- Static code analysis on each commit
- Dynamic application security testing (DAST) monthly

#### 3. Third-Party Risk Assessment

- Evaluate security posture of integrations (Plaid, hosting)
- Review SOC 2 reports and security certifications
- Monitor vendor security advisories

### 4.2 Risk Registry

All identified risks are documented in a risk registry containing:

Field	Description
Risk ID	Unique identifier
Description	Nature of the risk
Likelihood	Low / Medium / High
Impact	Low / Medium / High / Critical
Risk Score	Likelihood x Impact
Mitigation Status	Open / In Progress / Mitigated / Accepted
Owner	Responsible party
Review Date	Next review date

### 4.3 Key Risk Categories

1. **Data Breach** - Unauthorized access to financial data
2. **Token Compromise** - Plaid access token exposure
3. **Injection Attacks** - SQL/NoSQL injection, XSS
4. **Authentication Bypass** - Unauthorized account access

- 5. **API Abuse** - Rate limiting, unauthorized endpoints
- 6. **Supply Chain** - Compromised dependencies

## 5. Risk Mitigation Controls

### 5.1 Technical Controls

#### *Authentication & Access Control*

- Multi-factor authentication for administrative access
- Session management with secure, rotating tokens
- Principle of least privilege for all system access
- Role-based access control (RBAC)

#### *Data Protection*

- **Encryption at Rest:** AES-256 for stored data
- **Encryption in Transit:** TLS 1.3 for all communications
- **Token Security:** Plaid tokens encrypted, never exposed to clients
- **Key Management:** Secure key storage with rotation schedule

#### *Application Security*

- Input validation on all user inputs
- Output encoding to prevent XSS
- Parameterized queries to prevent injection
- CSRF protection on all state-changing operations
- Security headers (CSP, HSTS, X-Frame-Options)

#### *Infrastructure Security*

- Firewall rules limiting network access
- Regular security patches and updates
- Containerized deployment with minimal attack surface
- Secrets management (environment variables, not code)

### 5.2 Operational Controls

#### *Secure Development Lifecycle*

1. Security requirements in design phase
2. Secure coding training for developers
3. Code review with security checklist
4. Automated security testing in CI/CD
5. Security sign-off before deployment

*Change Management*

- All changes tracked in version control
- Code review required for all merges
- Staging environment testing before production
- Rollback procedures documented

*Incident Response Plan*

1. **Detection:** Automated alerting on anomalies
2. **Triage:** Assess severity and impact
3. **Containment:** Isolate affected systems
4. **Eradication:** Remove threat
5. **Recovery:** Restore normal operations
6. **Lessons Learned:** Post-incident review

5.3 Administrative Controls

- Background checks for personnel with data access
- Security awareness training
- Acceptable use policy
- Data classification guidelines
- Vendor security requirements

6. Security Monitoring

6.1 Continuous Monitoring

Monitoring Type	Frequency	Tool/Method
Application logs	Real-time	Centralized logging
Error rates	Real-time	Application monitoring
API usage patterns	Real-time	Rate limiting & analytics
Dependency vulnerabilities	Daily	Automated scanning
Access logs	Real-time	Authentication service
Infrastructure health	Real-time	Health checks

6.2 Security Metrics

Key security indicators tracked:

- Number of security vulnerabilities (by severity)
- Mean time to remediate vulnerabilities

- Failed authentication attempts
- API error rates and anomalies
- Dependency update currency
- Security training completion rate

## 6.3 Alerting Thresholds

Event	Threshold	Response
Failed logins	5 in 5 minutes	Account lockout, alert
API errors	10% increase	Investigate immediately
New critical CVE	Any	Patch within 24 hours
Unusual data access	Anomaly detected	Review and investigate

## 7. Plaid-Specific Security Controls

### 7.1 Token Management

- Access tokens stored encrypted in database
- Tokens never logged or exposed in error messages
- Token refresh handled server-side only
- Immediate revocation on user disconnect

### 7.2 API Security

- All Plaid API calls authenticated with client credentials
- Webhook signature verification enabled
- Rate limiting to prevent abuse
- Request/response logging (excluding sensitive data)

### 7.3 Data Handling

- Financial data accessed on-demand, not bulk stored
- Transaction data retention limited to 24 months
- No storage of bank credentials (handled by Plaid)
- Data minimization: only collect what's needed

## 8. Compliance

### 8.1 Regulatory Alignment

This policy aligns with:

- **SOC 2 Type II** principles (Security, Availability, Confidentiality)
- **CCPA** requirements for personal data protection
- **PCI DSS** guidance for handling financial data
- **OWASP Top 10** application security standards

## 8.2 Audit Trail

All security-relevant events are logged:

- Authentication events (success/failure)
- Authorization decisions
- Data access events
- Administrative actions
- Security configuration changes

Logs retained for 12 months minimum.

## 9. Exception Handling

Security policy exceptions require:

1. Written justification
2. Risk assessment
3. Compensating controls identified
4. Time-bound approval (max 90 days)
5. Documented in exception registry

## 10. Policy Enforcement

- Violations investigated promptly
- Remediation required within defined SLAs
- Repeat violations escalated
- Policy compliance audited quarterly

## 11. Contact

**Security Inquiries:** support@unifiedental.com

**Incident Reporting:** support@unifiedental.com (Subject: SECURITY)

## 12. Version History

Version	Date	Changes	Author
1.0	2025-12-22	Initial policy creation	Finance Guru Team

## Appendix A: Security Checklist

### Pre-Deployment Checklist

- ☐ All dependencies scanned for vulnerabilities
- ☐ No secrets in codebase
- ☐ Input validation implemented
- ☐ Authentication/authorization tested
- ☐ Security headers configured
- ☐ Error handling doesn't leak information
- ☐ Logging configured (no sensitive data)
- ☐ HTTPS enforced
- ☐ Rate limiting configured

### Quarterly Review Checklist

- ☐ Review and update risk registry
- ☐ Verify monitoring alerts functioning
- ☐ Review access permissions
- ☐ Update dependencies
- ☐ Review incident log
- ☐ Test backup restoration
- ☐ Review third-party security status

*This policy demonstrates Finance Guru's commitment to protecting user financial data through comprehensive security practices.*