

# # GigWallet Information Security Policy

**\*\*Document Title:\*\*** Information Security Policy

**\*\*Organization:\*\*** DNR Corp (DBA GigWallet)

**\*\*Version:\*\*** 1.0

**\*\*Effective Date:\*\*** February 20, 2026

**\*\*Next Review Date:\*\*** February 20, 2027

**\*\*Classification:\*\*** Internal — Confidential

**\*\*Approved By:\*\*** Sagar Patel, Founder & CEO

---

## ## 1. Purpose & Scope

### ### 1.1 Purpose

This Information Security Policy establishes the administrative, technical, and physical safeguards that GigWallet implements to protect the confidentiality, integrity, and availability of all information assets, with particular emphasis on consumer financial data accessed through third-party integrations including Plaid.

### ### 1.2 Scope

This policy applies to:

- All GigWallet production systems, applications, and infrastructure
- All personnel (employees, contractors, consultants) with access to GigWallet systems
- All consumer data collected, processed, stored, or transmitted by GigWallet
- All third-party integrations including Plaid, Firebase, and payment processors

### ### 1.3 Policy Ownership

The Founder & CEO is responsible for the approval, implementation, and enforcement of this policy. This policy is reviewed and updated at least annually or when significant changes occur.

---

## ## 2. Risk Management

### ### 2.1 Risk Assessment

GigWallet conducts risk assessments to identify, evaluate, and mitigate information security risks. Assessments are performed:

- Annually as part of policy review
- When significant system changes are made
- When new third-party integrations are added
- Following any security incident

### ### 2.2 Risk Mitigation

Identified risks are categorized by severity (Critical, High, Medium, Low) and addressed with appropriate controls. Risk acceptance decisions are documented and approved by leadership.

---

## ## 3. Data Classification & Handling

### ### 3.1 Data Classification

| Classification | Description | Examples |

|---|---|---|

| **\*\*Highly Sensitive\*\*** | Financial data, authentication credentials | Plaid access tokens, bank account data, transaction data, API keys |

| **\*\*Sensitive\*\*** | Personal identifiable information (PII) | User names, email addresses, phone numbers, tax information |

| **\*\*Internal\*\*** | Business operational data | Application logs, analytics, configuration |

| **\*\*Public\*\*** | Information intended for public access | Marketing content, published app store listing |

### ### 3.2 Consumer Financial Data Handling

- Consumer financial data obtained via Plaid is treated as Highly Sensitive
- Financial data is collected only with explicit user consent via Plaid Link
- GigWallet does **\*\*not\*\*** sell, rent, or share consumer financial data with third parties for marketing or advertising purposes
- Data is used solely for the purpose of providing the GigWallet service (earnings tracking, tax estimation, expense categorization)

### ### 3.3 Data Minimization

- Only data necessary for app functionality is collected
- No third-party tracking is implemented (NSPrivacyTracking = false)
- Financial calculations and ML analysis are performed on-device

---

## ## 4. Data Encryption

### ### 4.1 Data in Transit

- All client-server communications use HTTPS with TLS 1.2 or higher
- API requests between the GigWallet iOS app and backend servers are encrypted via TLS
- Plaid API communications use HTTPS exclusively
- Firebase Authentication uses TLS for all token exchanges

### ### 4.2 Data at Rest

- **\*\*iOS Application:\*\*** User data stored via SwiftData (SQLite) is protected by iOS Data Protection (hardware-level AES-256 encryption tied to device passcode)
- **\*\*Keychain Storage:\*\*** Authentication tokens are stored in the iOS Keychain with `kSecAttrAccessibleAfterFirstUnlock` protection class
- **\*\*Backend Database:\*\*** Plaid access tokens and consumer data stored in the backend database are protected by volume-level encryption on the hosting infrastructure
- **\*\*No plaintext credentials:\*\*** API keys, Plaid secrets, and JWT signing keys are stored as environment variables, never hardcoded in source code

### ### 4.3 Cryptographic Standards

- SHA-256 hashing via Apple CryptoKit for authentication nonces
- Cryptographically secure random number generation via `SecRandomCopyBytes`
- JWT tokens signed with industry-standard algorithms

---

## ## 5. Access Control

### ### 5.1 Principle of Least Privilege

Access to production systems, source code, and consumer data is restricted to authorized personnel with a legitimate business need. Permissions are granted at the minimum level required.

### ### 5.2 Authentication Requirements

- Multi-factor authentication (MFA) is required for all access to:
  - Production servers and infrastructure
  - Cloud service consoles (Firebase, Plaid Dashboard, App Store Connect)
  - Source code repositories (GitHub)
  - Backend administration
- End-user authentication is managed via Firebase Authentication supporting:
  - Sign in with Apple (native `ASAuthorizationController` with nonce verification)
  - Sign in with Google (OAuth 2.0)
  - Email/password with Firebase-managed password hashing

### ### 5.3 Access Reviews

- Access to production systems is reviewed quarterly
- Access is revoked immediately upon personnel separation
- Unused accounts are disabled after 90 days of inactivity

### ### 5.4 API Authentication

- All API requests require a valid Bearer token in the Authorization header
- Firebase ID tokens have a 1-hour expiry with automatic refresh
- Backend JWT tokens expire after 30 days
- Plaid access tokens are stored server-side only and never exposed to the client application

## ## 6. Application Security

### ### 6.1 Secure Development Lifecycle

- Code is developed following secure coding practices for Swift and Node.js
- All code changes undergo review before merging to production branches
- Testing is performed before production deployment
- Dependencies are monitored for known vulnerabilities

### ### 6.2 Architecture Security

- **\*\*Client-side:\*\*** SwiftUI + SwiftData on iOS 18+ with Apple's security frameworks
- **\*\*Server-side:\*\*** Node.js + Express with security middleware (CORS, rate limiting, input validation)
- **\*\*Plaid Integration:\*\*** Link tokens are created server-side; public tokens are exchanged for access tokens on the backend only; access tokens never reach the client
- **\*\*Request Validation:\*\*** JSON body size limited to 1MB; input fields are validated and whitelisted

### ### 6.3 Rate Limiting

- API rate limiting is enforced at 60 requests per minute per IP address
- Exceeding the limit returns HTTP 429 (Too Many Requests)

### ### 6.4 CORS Policy

- Cross-origin requests are restricted to a whitelist of approved origins
- Requests from unknown origins are rejected

---

## ## 7. Infrastructure Security

### ### 7.1 Hosting

GigWallet uses cloud-based hosting infrastructure with industry-standard security controls including:

- Network firewalls and access control lists
- Automated security patching
- Encrypted storage volumes

### ### 7.2 Network Security

- Production environments are logically segmented from development and testing
- Only necessary ports and protocols are exposed
- Administrative access requires MFA and is logged

### ### 7.3 Endpoint Security

- Development machines run current operating systems with automatic security updates
- Endpoint protection software is installed on all development machines
- Full-disk encryption is enabled on all development machines

---

## ## 8. Vulnerability Management

### ### 8.1 Vulnerability Scanning

- Application dependencies are monitored for known vulnerabilities

- npm audit and Swift package security advisories are reviewed regularly

### ### 8.2 Patching SLAs

| Severity | Remediation Timeline |

|---|---|

| Critical | Within 48 hours |

| High | Within 7 days |

| Medium | Within 30 days |

| Low | Next scheduled release |

### ### 8.3 Dependency Management

- Third-party packages are sourced from verified repositories (npm, Swift Package Manager)
- Package versions are pinned to prevent unauthorized changes
- Major dependency updates are tested before production deployment

---

## ## 9. Monitoring, Logging & Audit Trails

### ### 9.1 Logging

- Authentication events (sign-in, sign-out, failed attempts) are logged
- API requests are logged with timestamp, endpoint, and response status
- Database operations on sensitive data are tracked

### ### 9.2 Monitoring

- Server health and availability are monitored

- Unusual access patterns and potential security threats trigger alerts
- Error rates and response times are monitored for anomalies

### ### 9.3 Log Retention

- Security logs are retained for a minimum of 12 months
- Logs are stored in a separate, access-controlled location
- Logs are reviewed regularly for security-relevant events

---

## ## 10. Incident Response

### ### 10.1 Incident Classification

| Level | Description | Response Time |

|---|---|---|

| **\*\*Critical\*\*** | Active breach, data exfiltration | Immediate (within 1 hour) |

| **\*\*High\*\*** | Confirmed vulnerability exploitation | Within 4 hours |

| **\*\*Medium\*\*** | Suspected unauthorized access | Within 24 hours |

| **\*\*Low\*\*** | Policy violation, minor anomaly | Within 72 hours |

### ### 10.2 Incident Response Process

1. **\*\*Detection & Identification:\*\*** Identify and confirm the incident through monitoring, alerts, or reports
2. **\*\*Containment:\*\*** Isolate affected systems to prevent further damage
3. **\*\*Eradication:\*\*** Remove the root cause of the incident
4. **\*\*Recovery:\*\*** Restore systems to normal operation with verified integrity
5. **\*\*Post-Incident Review:\*\*** Document lessons learned and implement improvements

### ### 10.3 Breach Notification

- Plaid will be notified promptly at [security@plaid.com](mailto:security@plaid.com) upon discovery of any security breach involving consumer financial data accessed through the Plaid API
- Affected users will be notified in accordance with applicable state and federal breach notification laws
- Regulatory bodies will be notified as required by law

---

## ## 11. Data Retention & Deletion

### ### 11.1 Retention Periods

| Data Type | Retention Period | Rationale |

|---|---|---|

| User account data | Duration of account + 30 days | Service delivery |

| Financial transactions | Current tax year + 3 years | IRS record-keeping requirements |

| Plaid access tokens | Duration of active bank connection | Service functionality |

| Authentication logs | 12 months | Security monitoring |

| Application logs | 6 months | Troubleshooting |

### ### 11.2 Data Deletion

- Users may request deletion of their account and associated data at any time
- Upon account deletion, personal data and financial records are permanently removed within 30 days
- Plaid access tokens are revoked and deleted when a user disconnects a bank account or deletes their account

- Backup copies are purged according to the backup retention schedule

### ### 11.3 Data Portability

- Users can export their financial data in CSV, TXF, or Schedule C summary formats
- Export functionality is available within the application

---

## ## 12. Consumer Consent & Privacy

### ### 12.1 Consent Collection

- Users provide explicit consent before any bank account data is accessed via Plaid Link
- Users are presented with Terms of Service and Privacy Policy before account creation
- Consent is obtained through affirmative user action (tapping "Connect" in Plaid Link flow)

### ### 12.2 Privacy Compliance

- GigWallet's privacy practices comply with applicable federal and state privacy laws including CCPA
- The Apple Privacy Manifest (PrivacyInfo.xcprivacy) accurately declares all data collection
- No consumer financial data is sold to third parties — this is strictly prohibited
- Users are informed of what data is collected and how it is used

### ### 12.3 On-Device Processing

- Tax calculations, earnings analysis, expense categorization, and ML-based insights are processed entirely on-device
- Financial data does not leave the user's device unless the user explicitly initiates a sync or export

---

## ## 13. Third-Party Vendor Management

### ### 13.1 Approved Vendors

| Vendor | Purpose | Security Review |

|---|---|---|

| Plaid | Bank account linking & transaction sync | SOC 2 Type II certified |

| Firebase (Google) | Authentication & user management | SOC 2 Type II, ISO 27001 |

| Apple | App distribution, StoreKit, Sign in with Apple | ISO 27001, SOC 2 |

| Google Sign-In | OAuth authentication | SOC 2 Type II |

### ### 13.2 Vendor Assessment

- Third-party vendors handling consumer data are assessed for security posture before integration
- Vendor security certifications and compliance reports are reviewed
- Vendor agreements include data protection obligations

### ### 13.3 Vendor Monitoring

- Vendor security advisories and updates are monitored
- Vendor access is limited to the minimum required for service delivery
- Vendor integrations are reviewed during annual policy review

---

## ## 14. Personnel Security

### ### 14.1 Background Checks

Background checks are conducted on personnel with access to production systems and consumer data prior to granting access.

### ### 14.2 Security Awareness

- All personnel receive security awareness training upon onboarding
- Ongoing security awareness is reinforced through regular communications
- Training covers: phishing awareness, secure coding practices, data handling, incident reporting

### ### 14.3 Acceptable Use

- Production credentials must not be shared or stored in plaintext
- Sensitive data must not be transmitted via unencrypted channels
- Security incidents must be reported immediately to leadership

---

## ## 15. Business Continuity & Disaster Recovery

### ### 15.1 Backup Policy

- Backend database backups are performed regularly
- Backup integrity is verified periodically

- Backups are stored in a separate location from production data

### ### 15.2 Recovery Objectives

| Metric | Target |

|---|---|

| Recovery Time Objective (RTO) | 24 hours |

| Recovery Point Objective (RPO) | 4 hours |

### ### 15.3 Recovery Testing

- Disaster recovery procedures are tested at least annually
- Recovery test results are documented and deficiencies are remediated

---

## ## 16. Policy Compliance & Enforcement

### ### 16.1 Compliance Monitoring

- Compliance with this policy is monitored through regular reviews
- Non-compliance is addressed through corrective action

### ### 16.2 Policy Violations

Violations of this policy may result in disciplinary action up to and including termination of employment or contract, and may be reported to relevant authorities if required by law.

### ### 16.3 Policy Review

This policy is reviewed and updated:

- At least annually
- Following any significant security incident
- When material changes occur to systems, infrastructure, or regulatory requirements

---

## ## 17. Contact Information

For security concerns, incident reports, or questions about this policy:

**\*\*Security Contact:\*\*** [security@gigwallet.app](mailto:security@gigwallet.app)

**\*\*Plaid Incident Reporting:\*\*** [security@plaid.com](mailto:security@plaid.com)

---

*\* This document is the property of DNR Corp. Unauthorized distribution is prohibited.\**

*\* Last reviewed: February 20, 2026 / Next review: February 20, 2027\**