DigitWallet Information Security Policy

Purpose

DigitWallet is committed to delivering robust security measures to protect customer assets, private information, and operational systems from threats. This policy outlines the security standards, controls, and processes implemented to ensure confidentiality, integrity, and availability across our cryptocurrency custody and services.

Our mission is to set the benchmark for secure digital asset management by adhering to internationally recognized security standards, ensuring compliance with regulatory frameworks, and providing customers peace of mind when entrusting DigitWallet with their assets.

Scope

This policy applies to:

- **All Personnel**: Employees, contractors, vendors, and third-party service providers.
- **All Assets**: Cryptocurrency holdings, sensitive data, IT infrastructure, physical equipment, and customer information.
- **All Locations**: On-premises facilities, cloud environments, physical vaults, and any third-party integrated systems.
- **All Activities**: Processes involving data processing, storage, retrieval, and cryptocurrency transactions.

Compliance Framework

Cryptocurrency Security Standard (CCSS) Level 3
DigitWallet adopts CCSS Level 3, the highest standard for securing cryptocurrency systems.

Implementation Details:

Multi-Signature Wallet Setup:

- Each client's assets are stored using a multi-signature (multi-sig) wallet system.
- Multi-sig wallets require two of three private keys to authorise any transaction. This ensures that no single party (client, DigitWallet, or backup recovery) can control the

funds.
- DigitWallet uses Ledger hardware wallets to implement and secure this system.

Distributed Key Storage:

- The private keys are stored securely in ISO 27001-certified physical vaults located in geographically distinct locations.
- Backup recovery keys are securely encrypted and stored in a separate region, reducing risks from regional disasters.

Access Control:

- Only authorised personnel with verified credentials and multi-factor authentication (MFA) can access key management systems.
- Client keys are encrypted with AES-256 encryption before storage.

Audit Trail:

- Every transaction, key generation event, and authorization is logged, timestamped, and subject to internal and external audit.
- Logs are tamper-proof and stored securely for 10 years.

Penetration Testing and Risk Assessment:

- Regular penetration tests are conducted on wallet infrastructure.
- Risks are identified, mitigated, and logged quarterly.

Third-Party Custody and Wallet Infrastructure

DigitWallet partners with industry-leading third-party wallet infrastructure providers to ensure best-in-class security and scalability.

- Fireblocks is used to provide secure, Multi-Party Computation (MPC) institutional-grade custody infrastructure for clients' long-term and cold storage assets.
- BCB Group is our primary wallet provider for trading wallets, allowing for seamless liquidity and operational efficiency.

All wallet solutions provided by our partners are audited, certified, and comply with relevant security and compliance standards (eg., SOC 2, ISO 27002, CCSS).

We conduct due diligence and continuous monitoring on all partners to ensure they meet our internal cybersecurity standards and regulatory expectations. The use of these providers allows DigitWallet to maintain a high level of operational resilience while delegating infrastructure security to battle-tested industry leaders.

Both BCB and Fireblocks maintain robust insurance coverage, audit processes, and compliance with applicable global cybersecurity and regulatory standards.

Distributed Key Storage

The private keys are stored securely in ISO 27001-certified physical vaults located in geographically distinct locations. Backup recovery keys are securely encrypted and stored in a separate region, reducing risks from regional disasters.

Access Control

Only authorized personnel with verified credentials and multi-factor authentication (MFA) can access key management systems. Client keys are encrypted with AES-256 encryptoon before storage.

Audit Trail

Every transaction, key generation event, and authorisation is logged, timestamped, and subject to internal and external audit. Logs are tamper-proof and stored securely for 10 years.

Penetration Testing and Risk Assessment

Regular penetration tests are conducted on wallet infrastructure. Risks are identified, mitigated, and logged.

3.2 ISO/IEC 27017:2015 (Cloud-Specific Security)
DigitWallet uses Amazon Web Services (AWS) for secure cloud operations, adhering to ISO 27017 standards for cloud security.

Cloud Security Implementation:

1. Shared Responsibility Model:

- AWS secures the physical cloud infrastructure (data centers, servers, etc.).
- DigitWallet is responsible for securing its applications, data, and access control on AWS.

2. Access Control:

- Cloud access requires MFA and is restricted by roles and responsibilities using Role-Based Access Control (RBAC).
- Access logs are continuously monitored and reviewed bi-weekly.

3. Data Encryption:

- All sensitive customer data, including transaction history and PII, is encrypted at rest using AES-256 encryption and in transit using TLS 1.3.

4. Intrusion Detection:

- AWS GuardDuty is deployed for real-time detection of unauthorized or anomalous behavior.
- Notifications are sent to the security team within 5 minutes of detection.

Web and DNS Security:

DigitWallet employs Cloudflare to protect the application layer of its web platforms and DNS services.

- Cloudflare WAF (Web Application Firewall) helps filter and block malicious traffic, DDoS attacks, and common exploits (e.g., XSS, SQLi).
- DNS records are managed securely through Cloudflare with 2FA and restricted access protocols.
- CDN caching and SSL termination are used to optimise website performance and ensure encrypted access.

3.3 ISO/IEC 27018:2019 (PII Protection)

ISO/IEC 27018 compliance ensures that DigitWallet protects personal data processed in the cloud.

Implementation Details:

1. Anonymization and Pseudonymization:

- Customer data is anonymized where possible to reduce the impact of a data breach.
- Pseudonymization techniques replace sensitive identifiers with tokens for internal processing.

2. Data Access:

- Only employees with a legitimate business need can access customer data.
- All data access is logged, reviewed, and retained for a minimum of 7 years.

3. Incident Management:

- A 72-hour breach notification protocol is in place to inform customers and regulatory bodies if PII is exposed.

3.4 ISO/IEC 27001:2022 (ISMS)

DigitWallet's ISMS governs all information security management activities.

Core Components:

1. Information Security Objectives:

- Protect customer funds and data from theft, unauthorized access, and operational failures.
- Ensure 99.99% uptime for critical services.

2. Risk Assessment:

- All information assets are assessed for potential risks quarterly.
- Risk treatment plans are documented and implemented promptly.

3. Security Awareness:

- Employees undergo mandatory security training annually, covering threats like phishing and social engineering.

4. Independent Audits:

- An accredited third party audits DigitWallet's compliance annually.
- Internal audits occur semi-annually.

3.5 Amazon Web Services (AWS)

AWS is certified for ISO 27001, SOC 2, and more, providing a reliable backbone for DigitWallet's operations.

AWS Integration Details:

Backup and Disaster Recovery:

- All critical data is backed up daily and replicated across AWS's geographically redundant data centers.

Firewall Protection:

- AWS Web Application Firewall (WAF) filters malicious traffic to web-facing systems.

Security Controls

DigitWallet ensures that client digital assets are held in segregated wallets through Fireblocks' secure custody platform, protected by multi-layer cryptographic controls. Trading-related funds are managed through BCB's institutional-grade infrastructure, ensuring operational efficient without compromising security.

These arrangements ensure that client funds are not co-mingled, auditable, and are protected by robust operational and cybersecurity controls.

Security Controls

Access Control Policy

- All system access is managed using RBAC.
- MFA is enforced for employees, partners, and clients accessing secure systems.
- Periodic access reviews occur every 90 days.

Key Management Policy

- Keys are generated offline using Ledger hardware wallets in secure, controlled environments.
- DigitWallet retains one co-signing key, with the remaining keys distributed between the client and secure backups.
- In case of a lost key, DigitWallet's recovery protocol ensures access restoration within 72 hours.

Encryption Policy

- Data in Transit: Protected by TLS 1.3.
- Data at Rest: Secured with AES-256 encryption.
- Key Encryption: Managed by HSMs (Hardware Security Modules) and audited semi-annually.

Employee Security Training

Mandatory Onboarding:

- Training on phishing, social engineering, and data privacy occurs within the first week.

Ongoing Training:

- Employees participate in quarterly refresher courses.

Signed

Cinell Brown

Director, DigitWallet

30th December 2024