

Crypto Security Policy 2024

Purpose

This Crypto Security Policy establishes guidelines for the secure handling, storage, and use of cryptocurrency assets within “Groove Technologies”. The policy is designed to comply with Curaçao Gaming Control Board (GCB) requirements, safeguard client and company funds, and prevent unauthorized access, misuse, or fraudulent activities.

Scope

This policy applies to all employees, contractors, third-party vendors, and any individual or entity authorized to handle cryptocurrency on behalf of “Groove Technologies”. It covers all cryptocurrency-related activities, including deposits, withdrawals, transactions, storage, and security.

Definitions

- **Cryptocurrency:** Digital assets based on blockchain technology (e.g., Bitcoin, Ethereum, USDT).
 - **Cold Wallet:** An offline wallet used for secure long-term storage of cryptocurrency.
 - **Hot Wallet:** An online wallet used for day-to-day operations with minimal balances.
 - **Private Key:** A cryptographic key granting access to cryptocurrency wallets.
 - **AML:** Anti-Money Laundering procedures in compliance with Curaçao regulations.
 - **KYC:** Know Your Customer requirements to verify client identity and eligibility.
-

Policy Objectives

1. Ensure secure storage and handling of cryptocurrency assets.
 2. Maintain full compliance with Curaçao GCB licensing requirements.
 3. Mitigate risks related to hacking, theft, fraud, and money laundering.
 4. Establish clear roles and responsibilities for crypto security.
-

1. Governance and Compliance

1.1 Regulatory Compliance

- Comply with Curaçao GCB license requirements, ensuring full adherence to all applicable laws and regulations, including AML and KYC obligations for crypto transactions.

1.2 AML and KYC Procedures

- Perform KYC verification for all clients before processing cryptocurrency transactions.

1.3 Internal Audits

- Retain records of all cryptocurrency transactions for a minimum of 5 years.
-

2. Wallet Management

2.1 Cold Wallets

- Store the majority of cryptocurrency holdings in cold wallets to minimize exposure to online threats.
- Cold wallets must be encrypted, backed up, and stored in a secure physical location, such as a bank vault.

2.2 Private Key Security

- Private keys must be securely generated, stored offline, and accessible only to authorized personnel.
 - Use hardware security modules (HSM) or equivalent tools for private key management.
 - Perform regular key rotation and revoke compromised keys immediately.
-

3. Security Measures

3.1 Encryption and Authentication

- Encrypt all wallet credentials, private keys, and sensitive transaction data using industry-standard encryption protocols (e.g., AES-256).
- Implement multi-factor authentication (MFA) for access to crypto wallets, platforms, and systems.

3.2 Access Control

- Limit access to wallets and cryptocurrency systems to authorized personnel only, based on their roles and responsibilities.
 - Maintain an access control to only one authorized person in the company for all cryptocurrency systems.
-

4. Transaction Security

4.1 Transaction Authorization

- Require multi-signature approvals for all cryptocurrency transactions above a predefined threshold.
- Validate all transactions against AML and fraud detection systems before execution.

4.2 Transaction Limits.

- Notify management of any exceptions to limits, which require explicit approval.
-

5. Employee Training and Awareness

5.1 Training Program

- Provide mandatory training for employees handling cryptocurrency on security best practices, fraud prevention, and regulatory compliance.

5.2 Confidentiality Agreement

- Require employees to sign confidentiality agreements covering cryptocurrency-related responsibilities.
-

6. Business Continuity.

6.1 Business Continuity

- Develop and maintain a business continuity plan to ensure operational resilience in the event of crypto-related incidents.
-

7. Policy Review and Updates

7.1 Periodic Review

- Review this policy annually or as required by changes in regulatory requirements or company operations.

7.2 Approval Process

- Policy updates must be approved by senior management and documented for audit purposes.
-

8. Violations and Disciplinary Action

8.1 Non-Compliance

- Violations of this policy may result in disciplinary action, up to and including termination of employment or contracts.
 - Severe violations will be reported to regulatory authorities as required by law.
-

Acknowledgment

All employees and stakeholders must acknowledge and agree to comply with this Crypto Security Policy by signing the acknowledgment form.

Signed: 
Groove Technologies N.V
154475
Curacao

Date: 13.1.2025