

**CRYPTOCURRENCY
POLICY
LUCKLAND GROUP
B.V.**

1. Purpose

The purpose of this Cryptocurrency Policy is to define the principles, controls and procedures governing the acceptance and processing of cryptocurrencies transactions within Luckland Group B.V (the "Company").

This policy ensures that all crypto-related activities are conducted in compliance with the regulatory expectations of the Curaçao Gaming Authority (CGA) as well as applicable Anti-Money Laundering (AML) and Counter-Terrorist Financing (CFT) laws.

Additionally, this policy aims to:

- Mitigate risks associated with anonymity and decentralization of crypto assets.
- Prevent the use of the Company's platform for illicit financial activities.
- Ensure transparency, traceability and accountability in all crypto transactions.

2. Scope

This policy applies to all cryptocurrency-related operations conducted by the Company, including but not limited to:

- Customer deposits and withdrawals using crypto assets.
- Internal handling of crypto wallets and payment flows.
- Integration and use of third-party crypto payment service providers.
- Monitoring, investigation and reporting of crypto transactions.

It applies to:

- All customers (retail and VIP).
- All employees, especially Compliance, Risk, Finance and Customer Support teams.
- All external partners and service providers involved in crypto processing.

3. Accepted Cryptocurrencies

The Company adopts a conservative and risk-based approach when determining which cryptocurrencies are accepted.

3.1 Approved Assets

Only cryptocurrencies that:

- Are widely recognized and transparent
- Have sufficient blockchain traceability
- Are supported by reliable analytics tools

Examples include:

- Bitcoin (BTC)
- Ethereum (ETH)

3.2 Prohibited Assets

The following are not accepted:

- Privacy-focused cryptocurrencies (e.g., Monero, Zcash) due to lack of traceability
- Tokens designed to obscure transaction origin
- Assets linked to high fraud, scams or regulatory concerns

3.3 Ongoing Review

The list of accepted cryptocurrencies is reviewed periodically based on:

- Regulatory developments
- Risk exposure
- Market stability

4. Risk-Based Approach

The Company applies a risk-based approach (RBA) to all crypto-related activities, ensuring that resources are allocated efficiently to higher-risk areas.

4.1 Risk Factors

Each customer and transaction is assessed based on:

- Geographic risk (high-risk or sanctioned jurisdictions)
- Customer profile and behavior
- Transaction size, velocity and frequency
- Wallet exposure and blockchain history

4.2 Risk Categorization

Customers are categorized into:

- Low risk
- Medium risk
- High risk

4.3 Enhanced Controls

Higher-risk profiles triggers:

- Enhanced Due Diligence (EDD)
- Increased transaction monitoring
- Manual compliance review

5. Customer Due Diligence

5.1 Standard Due Diligence

Before enabling crypto transactions, customers must complete Know Your Customer (KYC) verification, including:

- Full legal name, date of birth and nationality
- Valid government-issued identification
- Proof of residential address

Verification must be conducted using reliable and independent sources.

5.2 Enhanced Due Diligence (EDD)

EDD is required in cases such as:

- High-value transactions
- Suspicious activity
- High-risk jurisdictions

EDD measures include:

- Source of Funds (SoF) verification
- Source of Wealth (SoW) analysis
- Additional identity verification
- Ongoing monitoring of activity

6. Wallet and Blockchain Monitoring

The Company utilizes advanced blockchain analytics tools to monitor and assess crypto transactions.

6.1 Wallet Screening

All wallet addresses are screened prior to transaction approval to identify exposure to:

- Sanctioned entities
- Darknet marketplaces
- Fraudulent or stolen funds

6.2 Risk Scoring

Each wallet is assigned a risk score based on:

- Transaction history
- Known associations
- Behavioral patterns

6.3 Action for Alerts

- Low risk → processed automatically
- Medium risk → flagged for review
- High risk → blocked and escalated

7. Monitoring Scenarios

Continuous monitoring systems are implemented to detect unusual or suspicious activity.

7.1 Monitoring Scenarios

Including:

- Structuring transactions to avoid thresholds
- Rapid movement of funds (in/ out)
- Inconsistent activity related to customer profile
- Multiple wallets used to obfuscate flows

7.2 Alert Handling

All alerts are:

- Reviewed by Compliance Officers
- Documented and assessed
- Escalated where necessary

8. Source of Funds Verification

Customers must be able to demonstrate the legitimate origin of their crypto assets.

8.1 Acceptable Documentation

- Exchange account statements
- Trading history
- Salary or business income proof

- Investment records

8.2 Trigger Events

SoF checks are required when:

- Transaction thresholds are exceeded
- Risk level increases
- Suspicious patterns are detected

8.3 Non-Compliance

Failure to provide adequate documentation may result in:

- Account restrictions
- Refusal of withdrawals
- Reporting to authorities

9. Suspicious Transaction Reporting (STR)

The Company is obliged to report suspicious activities in accordance with applicable laws and CGA expectations.

9.1 Red Flags

- Use of mixers/ tumblers
- Links to illicit services
- Sudden spikes in activity
- Attempts to bypass controls

9.2 Reporting Process

- Internal escalation to Compliance
- Investigation and documentation
- Filing of STR with competent authorities

10. Travel Rule Compliance

Where applicable, the Company complies with the Travel Rule requirements

This includes:

- Collecting sender and beneficiary information
- Ensuring data transmission between Virtual Asset Service Providers (VASPs)
- Refusing transactions with non-compliant entities

11. Third-Party Crypto Providers

All third-party crypto service providers must undergo strict due diligence.

11.1 Requirements

Provider must:

- Be licensed or regulated
- Have robust AML/ CFT controls
- Provide transaction monitoring capabilities
- Comply with applicable laws

11.2 Ongoing Monitoring

- Periodic reviews
- Performance and compliance checks
- Immediate action in case of deficiencies

12. Record Keeping

The Company maintains comprehensive records of all crypto-related activities.

12.1 Records Include

- Transaction data
- Wallet addresses
- KYC documentation

- Risk assessments
- Any other document as required by applicable laws

12.2 Retention Period

- Minimum of five (5) years or as required by the Curaçao Gaming Authority.

13. Sanction Compliance

All crypto transactions are screened against international sanctions lists.

13.1 Lists include

- OFAC
- EU
- UN

13.2 Actions

If a match is detected:

- Transaction is blocked immediately
- Funds are frozen if required
- Authorities are notified

14. Staff Training

Employees receive ongoing training to ensure awareness of crypto risks and compliance obligations.

14.1 Training Topics

- AML/ CFT risks in crypto
- Blockchain fundamentals
- Red flag identification

- Reporting obligations

14.2 Frequency of training

- At onboarding
- Annually thereafter
- Upon regulatory updates

15. Internal Controls and Audit

Strong governance is implemented to ensure effectiveness of this policy.

15.1 Controls

- Segregation of duties
- Dual approval processes
- Access controls

15.2 Audit

- Regular internal audits
- Independent compliance reviews
- Remediation of identified gaps

16. Policy Review

This policy is reviewed:

- At least annually
- Upon regulatory updates
- Following significant risk events

All updates must align with the expectations of the Curaçao Gaming Authority.

We may change this policy, at our sole discretion, from time to time in compliance with the Company's decision and/or the dynamic applicable laws and regulation framework, without the need to provide any notice.