

CRYPTOCURRENCY RISK MANAGEMENT AND COMPLIANCE POLICY

LUCKYROO N.V.

Effective Date: 6 August 2026



(SMES) Solutions for Management and Employment Support N.V.
Managing Director
07.08.2026

Document Information

Subject	Cryptocurrency Risk Management and Compliance Policy
Licensee	LUCKYROO N.V.
Company Registration Number	163606
CGA Licence Number	OGL/2024/1371/0694
Registered Address	Abraham Mendez Chumaceiro Boulevard 3, 4750, Willemstad, Curaçao
Involvement	All Departments
Responsibility	Compliance Officer
Approval	Board of Directors
Effective Date	6 August 2026
Review	Annually, or earlier upon: a change in applicable CGA guidance or the LOK; addition or removal of an accepted crypto asset, VASP, or risk threshold; a material incident; or a finding from audit or the regulator. Next scheduled review: 6 August 2027.
Classification	Internal

1. General Provisions

This Policy applies to all crypto-asset workflows of LUCKYROO N.V. (deposit, wagering, withdrawal, and treasury) and to all group entities that support the licensed operation under licence OGL/2024/1371/0694.

Managing Cryptocurrency risk effectively in a Company operating in a continuously changing risk environment requires a strong risk management culture. As a result, LUCKYROO N.V. has established an effective risk oversight structure and the necessary internal organisational controls to ensure that the Company undertakes the following:

- Compliance with the applicable legislation.
- The establishment of the necessary policies and procedures.
- The setting and monitoring of the relevant limits.
- The adequate identification and management of risks.

The Board meets on a regular basis and receives updates on risk and regulatory matters from management. More than that, the Board receives and reviews regularly (at least annually) written reports concerning compliance, Cryptocurrency Risk Management and Internal Audit policies.

Risk culture is a critical element in LUCKYROO N.V.'s Cryptocurrency Risk Management framework and procedures. Management considers risk awareness and risk culture within the Company as an important part of the effective risk management process. Ethical behaviour is a key component of the strong risk culture, and its importance is continuously emphasised by management.

The Company is committed to embedding a strong risk culture throughout the business where everyone understands the risks they personally manage and are empowered and qualified to take accountability for them. The Company embraces a culture where each business area is encouraged to take risk-based decisions, while knowing when to escalate or seek advice.

LUCKYROO N.V. adheres to a comprehensive framework that aligns with national and international cryptocurrency regulations, specifically:

- Curaçao Anti-Money Laundering Ordinances: adherence to reporting obligations under NORUT and NOIS, focusing on unusual and suspicious transactions.
- CGA Crypto Policy Guideline (June 2026): compliance with the Curaçao Gaming Control Board's dedicated crypto-asset guideline for licensed online gaming operators, including its risk-based requirements as set out throughout this Policy.

- FATF Virtual Asset Recommendations: incorporation of FATF Recommendation 15 (definition and treatment of Virtual Asset Service Providers) and Recommendation 16 (the Travel Rule) into the monitoring of virtual assets.
- EU Anti-Money Laundering Directives (AMLD5 & AMLD6): ensuring all customer interactions and transactions meet stringent KYC and risk-based monitoring criteria.

This Policy does not replace or limit any other legal, regulatory, or licensing obligation applicable to LUCKYROO N.V., including any Virtual Asset Service Provider-related laws in Curaçao. LUCKYROO N.V. independently ensures full compliance with all such obligations. The crypto-specific AML/CFT controls referenced in this Policy are detailed further in the Company's AML/CFT Manual submitted on the CGA Portal; this Policy is to be read in conjunction with that Manual.

2. Key Definitions

Virtual Asset Service Provider (VASP): any natural or legal person who conducts one or more of the following activities on behalf of another: exchange between virtual assets and fiat currencies; exchange between one or more forms of virtual assets; transfer of virtual assets; or safekeeping and/or administration of virtual assets or instruments enabling control over virtual assets, in line with FATF Recommendation 15.

Unhosted Wallet (self-hosted or non-custodial wallet): a crypto-asset wallet that is not managed by a VASP and where the private keys, and therefore full control of the assets, are held directly by the user. This distinction affects the risk treatment applied and whether the FATF Travel Rule applies to a given transfer.

Wallet Ownership Verification: the process by which the Company confirms that a customer controls a given wallet address, for example via a test transaction, a signed message, or an equivalent cryptographic proof of control.

Blockchain Analytics Tools: software and/or services used to trace, analyse and risk-assess virtual-asset transactions, including exposure to high-risk or prohibited sources such as sanctioned wallets, mixers, darknet markets and fraud-linked addresses.

FATF Travel Rule: FATF Recommendation 16, requiring that originator and beneficiary information accompany virtual-asset transfers between VASPs, and that such information be made available to competent authorities upon request.

Compliant VASP: a virtual asset service provider that demonstrates AML/CFT compliance, Travel Rule capability, sanctions screening, operational resilience and transparency, assessed on a risk basis rather than by jurisdiction label alone.

3. Governance Structure

To enforce Cryptocurrency Risk Management effectively, LUCKYROO N.V. has created a governance model with dedicated roles across departments:

- The Board of Directors: ultimate oversight, responsible for approving policy changes and monitoring overall compliance.
- Compliance Officer: oversees daily compliance with cryptocurrency usage, regulatory reporting, and submission of audit findings to the Curaçao FIU when necessary.
- Risk Department: this department, comprising cross-functional leaders, assesses risk exposures quarterly, reviewing security controls and compliance benchmarks.
- Internal Audit Team: conducts independent audits quarterly, reviewing policy adherence and reporting directly to the Board of Directors.

This Crypto Policy is signed off by the Compliance Officer of LUCKYROO N.V. and approved by the Board of Directors. It takes effect on 6 August 2026 and is reviewed annually, or earlier upon: a change in applicable CGA guidance or the LOK; addition or removal of an accepted crypto asset, VASP, or risk threshold; a material incident; or a finding from audit or the regulator.

Any change to this Policy is documented and managed. The addition or removal of any accepted crypto asset, virtual asset service provider, or risk threshold requires a documented risk assessment and appropriate sign-off before it takes effect.

The Company undertakes blockchain analytics and transaction-monitoring tools (using Chainalysis and Elliptic) capable of identifying prohibited assets and transaction patterns. Where any part of this capability is outsourced, visibility and accountability remain with the Company.

The Company will reject, freeze, or return funds where prohibited activity is detected, and will report relevant incidents in accordance with Article 5.10 (Incident Reporting) of the National Ordinance on Games of Chance.

The Company maintains documented procedures for identifying and handling prohibited assets, including escalation, freezing, and reporting steps, and ensures relevant personnel are trained in digital-asset risk identification and assessment (see Section 20, Training and Staff Awareness).

4. Not a Financial Institution

LUCKYROO N.V. does not function as an exchange, payment services provider, or Virtual Asset Service Provider (VASP). Crypto-assets are accepted for gambling services only.

LUCKYROO N.V. does not convert crypto to crypto or crypto to fiat on behalf of players, does not offer trading, swapping, or exchange services, and does not offer custody, transfer, or wallet services outside gambling-related transactions.

Players are informed that the Company is not responsible for the services of any third-party exchange used by the player to buy or sell crypto-assets.

5. AML/KYC in a Crypto Context

Crypto is not a carve-out from AML/CFT or Responsible Gambling obligations; the Company's AML policy applies equally to fiat and crypto transactions.

The crypto-specific AML/CFT controls referenced in this Policy are detailed further in the Company's AML/CFT Manual submitted on the CGA Portal; this Policy is to be read in conjunction with that Manual.

6. Risk Identification and Management

6.1 Market and Volatility Risk

Cryptocurrencies are characterized by significant price fluctuations, which can affect both payouts and deposits. To mitigate this risk, the Company treats crypto-assets as high risk, subject to asset-specific risk assessment (see Section 8, Digital Assets and Transaction Sources), and implements the following strategies:

- Preference for Stablecoins: where possible, the Company encourages high-value payouts in fiat-backed, regulated stablecoins to reduce volatility impact.
- Scheduled Payout Intervals: large payouts are distributed across fixed intervals to buffer against sharp market drops.

The Financial Operations Team monitors cryptocurrency valuations daily, adjusting payouts to reflect real-time market values. Transaction values are documented, and any market-driven adjustments are reported to the Compliance Officer.

6.2 Regulatory and Compliance Risks

With the evolving landscape of cryptocurrency regulations, LUCKYROO N.V. is dedicated to maintaining a proactive and thorough compliance framework, including:

- Real-Time Regulatory Monitoring: ongoing analysis of regulatory updates that could affect cryptocurrency operations, especially Curaçao-specific directives, including any update to the CGA Crypto Policy Guideline.

- Comprehensive Documentation: full record-keeping of all transactions and customer interactions is maintained for five years, per Curaçao FIU requirements.

Monthly audits of all crypto records ensure accuracy, while regulatory updates are tracked by the Legal Team. Any gaps in documentation are corrected immediately to ensure compliance.

6.3 Anti-Money Laundering (AML) and Fraud Prevention

To address the pseudo-anonymous nature of cryptocurrencies and prevent fraudulent activities, LUCKYROO N.V. has implemented robust AML/CFT measures, including:

- Enhanced Due Diligence (EDD): customers exceeding transaction thresholds must provide additional documentation for verification.
- Ongoing Monitoring for High-Risk Activity: all crypto transactions are monitored in real time to detect anomalies such as rapid deposits and withdrawals.

If a transaction is flagged for enhanced due diligence, it is escalated to the Compliance Team, who may request additional documents and investigate further using blockchain analytics tools. High-risk transactions are paused pending investigation and, where prohibited activity is confirmed, rejected, frozen, or returned in accordance with Section 3 (Governance Structure).

6.4 Cybersecurity and Asset Security

With heightened cyber risk for digital assets, LUCKYROO N.V. employs extensive security measures, detailed further in Section 16 (Hot, Warm and Cold Wallet Controls):

- Cold Storage for Reserves: the majority of digital assets are stored offline in cold wallets, secured with multi-factor authentication.
- Hot and Warm Wallet Security and Monitoring: operational and liquidity-management wallets are secured with real-time monitoring, enhanced access controls, and strict transaction limits.

Cryptocurrency balances across hot, warm, and cold wallets are reconciled daily. Transactions from cold wallets require approval from senior management and are logged for audit review.

7. Blockchain Analytics Capability

The Company applies blockchain analytics and transaction-monitoring capability, through Chainalysis and Elliptic, sufficient to:

- Trace the origin and destination of funds.
- Identify exposure to high-risk or prohibited sources (mixers, sanctioned entities, fraud-linked wallets), consistent with the red-flag indicators set out in Section 17 (Red Flags and High-Risk Transactions).
- Assess and risk-score wallets and transactions.
- Investigate and evidence suspicious activity, with findings documented to support Suspicious Activity Reporting and regulatory audit.
- Screen wallet addresses at the point of deposit, risk-scoring exposure to darknet markets, scams, and mixers before funds are credited.
- Monitor transactions on an ongoing basis, in real time and post-transaction, for new risk exposure and suspicious patterns.
- Verify source of funds by tracing blockchain history, documented to support KYC/EDD and audit requirements.
- Screen destination wallets before outbound withdrawal transfers.

All transaction monitoring alerts are reviewed by the Compliance Officer immediately. Where any part of this capability is provided by a third party, the Company retains visibility over, and accountability for, the results.

8. Digital Assets and Transaction Sources

Crypto-assets are treated as high risk and are subject to asset-specific risk assessment. The Company's preference is to transact in fiat-backed, regulated stablecoins. For other assets, the following acceptance rules apply:

- Privacy-enhancing cryptocurrencies that obscure transaction data and prevent effective monitoring, blockchain analysis, and source-of-funds verification (including but not limited to Monero, Zcash shielded transactions, Dash where privacy features are used, and Litecoin MWEB where privacy is optional) are not accepted.
- Pooled or omnibus wallet structures operated by VASPs are not accepted, as the Company's current operating model does not permit attribution of pooled-wallet transactions to individual customers, source-of-funds assessment, and monitoring/reporting to the required standard.
- Meme or highly speculative tokens are not accepted, reflecting their volatility and liquidity profile, immature governance/ecosystem, and elevated financial-crime risk.
- Wrapped tokens and bridged assets are not accepted where the provenance, custody, backing, or transaction history of the underlying asset cannot be independently verified, including wrapped versions of established coins such as wrapped Bitcoin.

9. Expressly Prohibited Assets

LUCKYROO N.V. does not accept crypto-assets that originate from, pass through, or are associated with sanctioned cryptocurrency mixers or tumblers, nor assets linked to wallet addresses appearing on any applicable sanctions list or flagged by Chainalysis and Elliptic.

The Company acknowledges that the CGA may designate further digital assets, token types, or transaction mechanisms as prohibited, and will implement any such designation without delay.

10. FATF Travel Rule Compliance

The Company recognises the FATF Travel Rule (Recommendation 16). Where applicable, when crypto-assets are transferred between regulated entities (exchanges, custodial wallet providers, and VASPs), the required originator and beneficiary information accompanies the transfer and is made available to competent authorities upon request.

11. Use of Third-Party VASPs and Payment Providers

LUCKYROO N.V. does not currently use any third-party VASP or crypto payment provider; all wallets used in connection with the licensed operation are owned and operated directly by the Company.

Should the Company engage a third-party VASP or payment provider in future, the use of that provider will not transfer, reduce, or dilute the Company's obligations regarding AML/CFT, transaction monitoring, player protection, or incident reporting. The Company will ensure that any such provider is regulated, registered, or otherwise subject to reputable oversight in its home jurisdiction, and demonstrates AML/CFT controls, Travel Rule capability, sanctions screening, transaction monitoring, operational resilience, and transparency. The Company will document its due diligence and risk assessment for each such provider before engagement.

12. Unhosted (Self-Hosted / Non-Custodial) Wallets

LUCKYROO N.V. does not accept crypto-assets from unhosted (self-hosted / non-custodial) wallets or DeFi protocols.

13. AML Due Diligence and Reporting Procedures

Client Due Diligence (“due diligence” or “CDD”) processes comply with the procedures detailed herein. These include the identification of the Client, ML/TF risk assessment, assessment of the financial position of the Client, validity of identity, and the source of funds.

The following procedures, which constitute the ML/TF prevention measures, are carried out to perform customer due diligence at the inception of a business relationship with a Client:

- Identification of persons who apply to the Company as potential Clients.
- Verification of whether the potential Client acts as a principal; if represented by another person (agent), identification and verification of the representative applies as well.
- Obtaining information on the Client’s management structure and the nature of its activity, if applicable.
- Obtaining information on the purpose and intended nature of the relationship with the Company.

The above steps are essential prior to the initiation of a business relationship with the potential Client. After the Client is engaged in the business relationship, the following ML/TF prevention measure must be taken:

- Ongoing monitoring of the business relationship with the Client and the monetary operations and transactions of the Client.

Suspicious Activity Reporting (SAR): all flagged transactions are reported to FIU Curaçao, following regulatory standards. When suspicious transactions trigger an alert in the compliance system, the Compliance Officer reviews these alerts, and a SAR is submitted to FIU Curaçao within 24 hours if warranted. Records of suspicious transactions are stored securely for audit purposes. This SAR process operates alongside, and does not replace, the crypto-incident reporting obligations under Article 5.10 set out in Section 19 (Incident Reporting).

14. Transaction Management

The default expectation is that withdrawals are processed to the same wallet and in the same crypto-asset as the original deposit.

A withdrawal to a different wallet address is permitted only where that wallet is whitelisted, pre-screened, and verified as belonging to the same customer, and has passed KYC/AML checks.

A withdrawal in a different crypto-asset or stablecoin is permitted only where the full transaction flow remains transparent and auditable, the conversion is conducted via a regulated VASP, and records are maintained.

Players cannot transfer amounts to each other on the platform.

15. Operator Wallets

All wallets used in connection with the licensed operation are owned or controlled by LUCKYROO N.V. (or an approved group/payment entity). Personal wallets, UBO-linked wallets, employee wallets, and informal wallet arrangements are prohibited.

Wallets are segregated between player-flow, operational, and treasury purposes to prevent comingling of player funds and company funds. Player funds are held in segregated wallets.

Only authorized personnel with multi-factor authentication can access digital asset storage. Any transfer outside standard procedures triggers immediate review.

16. Hot, Warm and Cold Wallet Controls

The Company’s wallet architecture (hot, warm, and cold) is documented, risk-assessed, and subject to appropriate controls:

- Hot Wallets: used for day-to-day player deposits and withdrawals, with balances limited to operationally necessary amounts and secured with real-time monitoring and strict transaction limits.

- Warm Wallets: used for liquidity management, under enhanced access controls and transaction-approval procedures.
- Cold Wallets: used for treasury, reserves, and longer-term safeguarding, held offline, with documented key management, reconciliation, and auditability.

Multi-signature controls, withdrawal whitelisting, multi-factor authentication, hardware security modules (HSMs), or equivalent measures are applied proportionate to the value and risk of each wallet.

The Company maintains records sufficient to evidence ownership/control, transaction history, reconciliations, access rights, approvals, and any movement of funds between wallets. Transfers from cold storage to warm or hot wallets require senior-level approval, and any adjustments are documented daily. Discrepancies in wallet balances are flagged for immediate investigation.

17. Red Flags and High-Risk Transactions

Whilst performing ongoing monitoring of the crypto pay-ins and pay-outs, some transactions will need to be reviewed manually. This review is conducted by the Compliance Team.

In most cases, LUCKYROO N.V. traces the origin of the coins by going back multiple steps to fully understand the coin flow between different entities and addresses and to make sure there are no direct connections with illicit sources.

Crypto assets can be traced on the blockchain from the first moment of creation (usually through mining) until the last time they were spent. It is possible to trace coins back to the original source to minimize the risk of coins that were stored or passed through “tainted” wallets. Tainted wallets or high-risk wallets are the following:

- Wallets that were hacked.
- Wallets that were used to fund or are the proceeds of illegal or terrorist activity.
- Wallets that were used to pay for services or goods on the dark web.
- Wallets that were used to obfuscate the origins of the coins, i.e. mixers and tumblers.
- Wallets that have otherwise suspicious origins.

A significant proportion of the crypto assets held or used in a transaction being associated with privacy-enhancing features or products and services that potentially obfuscate transactions or undermine the Company’s ability to know its customers and implement effective AML/CTF controls is treated as a red flag, including where the assets or transaction are associated with:

- Mixers or tumblers.
- Obfuscated ledger technology.
- Internet Protocol (IP) anonymizers.
- Ring signatures.
- Stealth addresses.
- Ring confidential transactions.
- Atomic swaps.
- Non-interactive zero-knowledge proofs.
- Privacy coins.

Further red flags include: a significant proportion of the crypto assets held or used in a transaction being associated with second-party escrow services; and the crypto asset coming from, or being associated with, the darknet or other illegal/high-risk sources, such as an unregulated exchange, or being associated with market abuse, ransomware, hacking, fraud, Ponzi schemes, sanctioned wallet addresses, or unregulated gambling sites.

18. Regular Audits and Compliance Reviews

Quarterly internal audits and an annual third-party audit verify adherence to compliance protocols, with findings reported to the Board.

19. Incident Reporting

In line with the incident-reporting requirements under the LOK, the Company identifies, assesses, and reports all crypto-related incidents in accordance with Article 5.10. Reportable incidents include:

- Security breaches (compromised private keys, wallet access, or unauthorised transactions).
- System failures impacting crypto processing (exchange outages, blockchain congestion, failed transactions).
- Crypto fraud schemes (coordinated deposit/withdrawal patterns, chip-dumping, or collusion).
- Material discrepancies in wallet balances or transaction records.
- Any event affecting the integrity, security, or traceability of crypto transactions.
- Exposure to sanctioned wallets, mixers, or prohibited sources.
- Smart-contract failures.
- Blockchain forks or chain-level disruptions.

20. Training and Staff Awareness

All staff managing cryptocurrency transactions undergo regular training on:

- AML/CFT regulations specific to cryptocurrency.
- Cybersecurity standards.
- Incident management for handling suspected fraud or breaches.
- Digital-asset risk identification and assessment, including the acceptance rules in Section 8 (Digital Assets and Transaction Sources) and Section 9 (Expressly Prohibited Assets).

21. Transition Period

This Policy sets out LUCKYROO N.V.'s adoption and compliance timeline against the CGA Crypto Policy Guideline (June 2026):

- Immediate effect: prohibitions on sanctioned wallets, mixers, prohibited assets, personal/UBO-linked wallets, and acting as an exchange/PSP/VASP apply with immediate effect.
- By 30 September 2026: this Policy is uploaded to the CGA Portal.
- By 31 December 2026: documented crypto risk assessments, VASP due diligence, wallet-ownership controls, transaction-monitoring procedures, and staff training are completed.
- By 30 June 2027: full wallet segregation, blockchain-analytics capability, reconciliation processes, withdrawal whitelisting, and audit-ready record-keeping are fully implemented.