

NIOLLO B.V.



Cryptocurrencies Policy for Niollo B.V.

Version Control

Prepared by	Date	Version	Description
Compliance Officer	01 October 2025	1.0	Creation
Compliance Officer	18 February 2026	2.0	Compliance Update

Contents

- Version Control 2
- 1. Purpose, Scope, and Policy Statement 4
 - 1.2 Scope 4
 - 1.3 Policy Statement 4
- 2. Risk Management Principles..... 5
 - 2.2 KYC and AML Compliance..... 5
 - 2.2.3 AML Screening 6
 - 2.3 Cryptocurrency Transaction Monitoring..... 6
 - 2.3.2 Threshold Alerts 7
 - 2.3.3 Transaction Management..... 7
 - 2.4 Third-Party Risk Management..... 7
 - 2.4.2 PSP Onboarding..... 8
 - 2.5 Regulatory and Legal Compliance 8
 - 2.6 Volatility and Conversion Risks 9
 - 2.6.2 Liquidity Management 9
- 3. Incident Management 9
 - 3.2 Investigation and Reporting..... 9
 - 3.3 Remediation Measures..... 10
- 4. Enforcement and Consequences 10
- 5. Training and Awareness..... 10
- 6. Review and Updates 10
- 7. Record Keeping and Audit Trail..... 10
- Risk Description 12**
 - Likelihood Impact (High/Med/Low) (High/Med/Low) 12**
 - Mitigation Measures 12**
 - Responsible Party 12**
- Annex 2: Incident Reporting Form 13**
 - Involved Parties 13
 - Preliminary Investigation..... 13
 - Next Steps 13

CRYPTOCURRENCY POLICY

1. Purpose, Scope, and Policy Statement

1.1 Purpose

The purpose of this policy is to establish a comprehensive framework for identifying, managing, and mitigating risks associated with the indirect use of cryptocurrency in player transactions.

While the operator, Breckenridge Curacao N.V., does not directly accept cryptocurrency, the policy outlines responsibilities across Payment Agents and Payment Service Providers (PSPs) to ensure regulatory compliance, financial security, and operational integrity. This is in strict accordance with Curaçao's National Ordinance on Games of Chance (LOK), FATF standards, and other applicable international guidelines.

1.2 Scope

This policy applies to:

- All departments involved in payments, compliance, risk management, and audits.
- The Payment Agent processing transactions on behalf of the company.
- Any PSPs engaged by the Payment Agent that accept cryptocurrency from players.
- All crypto asset workflows, including deposit, wagering, withdrawal, and treasury operations.

1.3 Policy Statement

The operator is committed to a zero-tolerance approach to financial crime, safeguarding players' financial integrity, and adhering to international and local regulations regarding cryptocurrency transactions. To this end, the operator enforces stringent controls, conducts comprehensive due diligence, and collaborates with Payment Agents and PSPs to manage cryptocurrency risks effectively.

2. Risk Management Principles

2.1 Governance and Oversight

- The Compliance Department will collaborate with the Payment Agent to assess and mitigate risks associated with cryptocurrency transactions.
- An internal audit will be conducted annually to evaluate compliance with regulatory and security standards. Findings must be documented, and corrective actions initiated within 30 days.

2.2 KYC and AML Compliance

2.2.1 Enhanced KYC Protocols

- PSPs must implement enhanced KYC measures for all players engaging in cryptocurrency transactions.
- Required KYC documents include:
 - ✓ Government-Issued ID Verification: Valid, unexpired photo identification.
 - ✓ Proof of Address: Recent utility bill or equivalent document issued within the past three months.
 - ✓ Detailed information on the origin of cryptocurrency funds for deposits exceeding € 2,000 or their fiat equivalent. Operator will maintain copies of player documentation for a minimum of five years
 - ✓ Obtain appropriate evidence of wallet control

2.2.2 Permitted and Prohibited Assets and Transaction Flows

To maintain compliance with AML and counter-terrorist financing frameworks, the following rules apply:

Prohibited Assets and Cryptocurrency Types

- **Privacy coins**, including but not limited to:
 - Monero (XMR)
 - Zcash (ZEC)
 - Dash (DASH)
- **Meme coins** considered high-risk due to volatility and lack of fundamental utility, including:
 - DOGE

- SHIB
- PEPE
- **Wrapped tokens of unknown origin**, including non-transparent or unverifiable wrapped versions of Bitcoin, Ethereum, or other assets.

Prohibited Deposit and Withdrawal Flows

- Any deposit routed via **sanctioned mixers or tumblers**, including but not limited to:
 - Tornado Cash
 - Blender.io
 - Sinbad.io
- Wallets listed on **international sanctions lists**, including OFAC, EU, or UN listings.

Permitted Assets

- Major, transparent, traceable cryptocurrencies such as Bitcoin (BTC) and Ethereum (ETH), subject to PSP blockchain analytics screening.

2.2.3 AML Screening

PSPs are required to perform comprehensive AML checks on all cryptocurrency transactions, leveraging blockchain analysis tools to identify:

- High-risk wallet addresses (e.g., flagged for previous involvement in illicit activities).
- Transactions involving sanctioned jurisdictions.
- Transactions involving sanctioned lists
- Anomalous patterns inconsistent with typical gaming behavior.
- The Payment Agent will review the PSPs' AML reports quarterly and provide updates to the operator's Compliance Team.

2.3 Cryptocurrency Transaction Monitoring

2.3.1 Automated Monitoring Systems

PSP's must deploy automated monitoring tools to identify anomalies such as:

- High transaction volumes inconsistent with player behavior.
- Transactions linked to flagged wallet addresses or high-risk jurisdictions.
- Structuring of transactions to avoid reporting thresholds.

2.3.2 Threshold Alerts

Cryptocurrency transactions exceeding the predefined threshold of € 2,000 (or equivalent in cryptocurrency) must trigger an alert to:

- The Payment Agent's Risk Management Unit.
- The operator's Compliance Department, which will conduct an immediate review.

All alerts and investigations must be logged into a Transaction Monitoring Register and in case of further reporting by the MLRO this needs to be evidence in the Transaction Monitoring Register.

2.3.3 Transaction Management

The following rules govern how cryptocurrency transactions must be handled:

1. **Withdrawal Wallet Requirement:**

- The operator must process withdrawal requests **only to the same wallet** from which the original deposit was received.

2. **Currency Consistency:**

- Withdrawals must be processed in **the same cryptocurrency** as the original deposit.

3. **No Internal Transfers:**

- Players are prohibited from transferring balances or cryptocurrency between player accounts within the platform.

These controls are designed to ensure that the gaming platform is not used as a mechanism for peer-to-peer value transfer, obfuscation of asset provenance, or informal remittance activity, and must therefore be enforced without exception unless required by law enforcement or regulatory instruction.

2.4 Third-Party Risk Management

2.4.1 Payment Agent Due Diligence

The Compliance Department will annually evaluate the Payment Agent's risk controls through:

- Comprehensive compliance audits focusing on adherence to contractual obligations.
- Reviews of PSPs' blockchain analytics tools and KYC/AML measures.

Third-Party Risk Management Report will be submitted to senior management annually.

2.4.2 PSP Onboarding

PSP onboarding must include rigorous verification of:

- Licenses or registrations status.
- Compliance with FATF Travel Rule requirements, including the secure transmission of sender and receiver details during cryptocurrency transactions.
- Implementation of anti-fraud tools, such as multi-factor authentication and transaction verification.
- Transaction monitoring capabilities

PSPs must demonstrate operational capability to transmit and receive FATF Travel Rule data where acting as or interfacing with Virtual Asset Service Providers (VASPs). The operator shall periodically obtain assurance (through audit rights, certifications, or testing summaries) that such data exchange mechanisms remain functional and compliant.

2.5 Regulatory and Legal Compliance

- The company will monitor global regulatory changes related to cryptocurrency to ensure continuous compliance.
- Any updates to relevant laws will be reflected in policy amendments.
- An annual Compliance Impact Assessment will be conducted to identify regulatory gaps.

2.5.1 Cryptocurrency Asset Risk Classification

Prior to permitting any cryptocurrency exposure through PSP channels, the operator shall conduct and document an asset-level risk classification considering:

- Transparency and traceability of the blockchain;
- Regulatory status of the asset and whether issued by a regulated entity;
- Susceptibility to anonymity-enhancing features;
- Liquidity and market integrity risks; and
- Exposure to typologies associated with gambling misuse.

Fiat-backed, regulated stablecoins may be utilised subject to due diligence. Algorithmic or unregulated stablecoins require enhanced risk approval by Compliance and Senior Management.

2.6 Volatility and Conversion Risks

2.6.1 Conversion Timelines

- Cryptocurrency transactions must be converted into fiat within a 24-hour window to mitigate market volatility. Exceptions require senior management approval and must be documented.
- Conversion delays caused by market conditions will be reported to the Compliance Department.

2.6.2 Liquidity Management

- The Payment Agent must maintain sufficient liquidity reserves to manage cryptocurrency conversion delays during periods of market instability.

3. Incident Management

3.1 Detection and Escalation

- PSPs or the Payment Agent must flag suspicious cryptocurrency transactions.
- The Compliance Team must be notified within 24 hours of flagged activity.

Crypto-Operational Incidents

The incident framework shall extend to cryptocurrency-specific operational risks including:

- blockchain network forks impacting transaction finality;
- compromised or inaccessible wallets or private keys at PSP level;
- smart-contract or protocol failures affecting asset transferability;
- material disruption of exchanges used for conversion;
- blockchain congestion causing delayed settlement.

PSPs must notify the operator immediately upon detection of such events.

3.2 Investigation and Reporting

- Investigations will involve:
 - ✓ Analysis of PSP transaction monitoring data.
 - ✓ Blockchain analytics.
 - ✓ Additional KYC documentation if needed.
- Suspicious transactions must be reported to financial intelligence units within legally mandated timeframes.

3.3 Remediation Measures

- Recommendations for process improvements and enhanced controls will be submitted to the Senior Director of Regulatory Relations in Compliance

4. Enforcement and Consequences

Non-compliance by Payment Agents or PSPs may result in:

- Contract termination.
- Reporting to regulatory authorities.
- Financial penalties as per contractual agreements.
- Internal staff violations may lead to disciplinary actions, including termination of employment.

5. Training and Awareness

Annual training will be provided on:

- Cryptocurrency risk management.
- Updated regulatory requirements.
- Use of blockchain analytics tools.

6. Review and Updates

- This policy will be reviewed periodically and updated based on regulatory changes.
- All amendments must be approved by senior management.

7. Record Keeping and Audit Trail

7.1 Record-Keeping

The Payment Agent will maintain detailed records for all cryptocurrency-related activities, including:

- Player KYC documentation.
- PSP AML reports.

- Blockchain analytics outputs.
- Transaction Monitoring Register entries.
- Evidence of wallet control.
- Conversion logs for fiat transitions.
- Correspondence related to risk assessments and investigations.

All records must be:

- Stored securely in accordance with GDPR and local regulations.
- Retained for a minimum of five years.

7.2 Audit Trail Requirements

The Compliance Team shall:

- Maintain an immutable audit log of alerts, reviews, escalations, and SAR filings.
- Ensure audit trails document: The reviewer handling each case.
- The rationale for all decisions.
- All communications between PSPs, Payment Agents, and Compliance.
- Provide senior management with quarterly summaries of crypto-related compliance activities.

Records must enable independent reconstruction of cryptocurrency transaction flows by correlating PSP reports, blockchain transaction identifiers (TXIDs), and fiat settlement records, ensuring auditability against publicly verifiable blockchain data.

Annex 1: Crypto Risk Assessment Template

Assessment Area	Risk Description	Likelihood (High/Med/Low)	Impact (High/Med/Low)	Mitigation Measures	Responsible Party
Customer Identity Risk	Insufficient KYC checks on crypto-origina8ng funds	High	High	Require robust KYC/AML standards from PSPs	Payment Agent
Illicit Source of Funds	Funds originating from sanctioned jurisdictions	Medium	High	Use blockchain analytics to flag high-risk wallets	PSPs & Payment Agent
Conversion Delays	Delayed fiat conversion leading to volatility risk	Low	Medium	Mandate immediate conversion policies	Payment Agent
Regulatory Non-Compliance	PSP failure to comply with evolving crypto laws	High	High	Conduct regular PSP compliance audits	Compliance Team
Transaction Fraud	Suspicious transaction patterns or anomalies	Medium	High	Implement automated monitoring tools	Payment Agent

Annex 2: Incident Reporting Form

- **Date of Incident:** [Enter Date]
- **Time of Incident:** [Enter Time]
- **Reported By:** [Name/Role]
- **Incident Description:** [Provide a brief summary of the suspicious activity]

Involved Parties

- **Player ID/Account:** [Enter Details]
- **PSP Name:** [Enter Name]
- **Cryptocurrency Involved:** [Specify, e.g., Bitcoin, Ethereum]
- **Transaction Amount (Fiat/Equivalent Crypto):** [Enter Amount]

Preliminary Investigation

- **Source Wallet Address:** [Enter Address]
- **Blockchain Analytics Results:** [Summarize Findings]
- **Risk Level Assessment:** [High/Medium/Low]
- **Immediate Action Taken:** [Freeze Funds, Notify Authorities, etc.]

Next Steps

- **Further Investigation Required (Yes/No):** [Specify]
- **Date for Follow-Up:** [Enter Date]
- **Responsible Team/Individual:** [Enter Details]