

Alisium B.V.

Crypto Usage Policy

Version	Status	Date	Comments	Signature of the Approver
1.0	Approved	10-Nov-2024	Policy created and approved	

Approver	Morganite Corporate Services B.V. / Director
Date Approved	10-Nov-2024
Date last reviewed	10-Nov-2024
Review Frequency	Annual
Next review date	Nov-2025
Security classification	Private and Confidential

1. INTRODUCTION

Alisium B.V. is committed to ensuring safe, secure, and compliant operations concerning cryptocurrency payments and transactions within its online gambling services. This Crypto Usage Policy defines the approach Alisium B.V. employs in handling cryptocurrency-related risks, particularly in the areas of verification, transaction monitoring, AML compliance, data security, and fraud prevention.

2. SCOPE AND PURPOSE

This policy applies to all cryptocurrency transactions processed by Alisium B.V. and extends to all personnel involved in the handling, monitoring, and processing of these transactions.

3. RISK MANAGEMENT MEASURES

3.1 Verification Process

Alisium B.V. considers usage of cryptocurrency as a payment method to pose higher risk than, using traditional fiat payment methods and implements a stringent customer verification process to ensure that all users engaging in cryptocurrency transactions are accurately identified. Verification measures include collecting relevant information from users, such as proof of identity and residence at a lower threshold than in standard situations, i.e. 500 NAF of total deposits/withdrawals.

Enhanced verification is performed for users identified as high-risk, which may include politically exposed persons (PEPs) or users with unusual transaction patterns. This process is periodically reviewed to maintain alignment with regulatory standards and industry best practices.

Responsible persons shall ensure that verification measures are consistently applied and adjusted as necessary to account for the evolving nature of cryptocurrency risk.

The verification process shall be conducted in accordance with the company's AML/CFT Policies.

3.2 Transaction Monitoring

Alisium B.V. uses monitoring systems to review cryptocurrency transactions, ensuring the detection of anomalies or patterns associated with potential money laundering or fraudulent activity.

Each transaction undergoes screening based on transaction limits, frequency, and known cryptocurrency red flags, including rapid, high-value deposits and withdrawals, and usage of privacy-centric cryptocurrencies.

Automated alerts are generated for suspicious activity, which is escalated to the Money Laundering Reporting Officer (MLRO) for further review and potential reporting to the Financial Intelligence Unit Curaçao (FIU).

The transaction monitoring and escalation the suspicious activity shall be conducted in accordance with the company's AML/CFT Policies.

3.3 Anti-Money Laundering (AML) Compliance

Alisium B.V. aligns its AML program with local regulations. Specific AML controls include mandatory identity verification, source of funds verification, and enhanced due diligence for transactions exceeding pre-defined limits. The company also ensures that all employees are trained on AML protocols related to cryptocurrency handling.

Suspicious Activity Reports (SARs) are filed promptly for any transactions suspected of involving money laundering. The AML process is audited periodically to verify the efficacy of controls and identify any necessary improvements.

3.5 Anti-Fraud Measures

The company implements fraud detection systems to identify and prevent fraudulent activity associated with cryptocurrency transactions. This includes IP tracking, device monitoring, and behavior analytics.

Manual reviews are conducted on flagged transactions, and suspicious accounts are promptly frozen pending investigation. Alisium B.V. reserves the right to terminate accounts in cases where fraud is confirmed, with all actions documented in compliance with regulatory reporting requirements.

Responsible persons shall oversee the continuous improvement of fraud prevention measures, considering the dynamic risks associated with cryptocurrency and adapting controls as necessary.

4. GOVERNANCE

4.1 Internal Audit

An internal audit of Alisium B.V.'s cryptocurrency policies and AML framework is conducted annually to evaluate effectiveness, compliance, and risk management practices related to cryptocurrency usage.

The audit covers all relevant aspects, including verification, transaction monitoring, AML compliance, data security, and fraud prevention. Findings from the audit are used to enhance and refine policies and procedures to address any identified gaps or risks.

4.2 Review and Updating of the Policy

This policy is reviewed annually by the MLRO and is updated to reflect changes in regulatory requirements, technological advancements, or company-specific needs.

Updates are communicated to all employees, who are required to acknowledge any new guidelines or procedures introduced as part of this policy.

5. STAFF TRAINING AND AWARENESS

All relevant staff receive mandatory training on the specific risks, controls, and procedures associated with cryptocurrency transactions. Training sessions cover the identification of red flags, proper transaction monitoring protocols, data security requirements, and AML procedures tailored to cryptocurrency usage.

Alisium B.V. ensures that employees understand their responsibilities under this policy and all other AML policies and procedures, including when and how to escalate suspicious activity to the MLRO. Refresher training sessions are conducted annually or as needed, based on updates to the policy or changes in regulatory requirements.

6. REPORTING AND ESCALATION

All staff are required to report any suspicions regarding cryptocurrency transactions immediately to the MLRO. Reporting mechanisms include direct reporting channels and escalation procedures in line with Alisium B.V.'s AML Policies.

The MLRO is responsible for investigating and, where necessary, filing SARs with the FIU. All reports are documented, stored securely, and handled in a manner that protects confidentiality and prevents tipping off.

Internal reporting guidelines are periodically reviewed to ensure alignment with regulatory expectations and industry best practices. The MLRO oversees compliance with reporting standards, reviewing and enhancing protocols as required.

7. REGULATORY COMPLIANCE AND SANCTIONS SCREENING

Alisium B.V. performs ongoing sanctions screening on all its clients against latest international sanctions lists to prevent engagement with prohibited individuals.

Sanctions checks are conducted in real-time through automated systems, and all flagged transactions are halted pending review by the MLRO.

In cases of confirmed matches to sanctions lists, the company undertakes appropriate action, including freezing transactions and notifying relevant authorities in compliance with the applicable laws of Curaçao.

8. RECORD KEEPING

Alisium B.V. maintains accurate and complete records of all cryptocurrency transactions, verification documents, monitoring activity, and SARs for a minimum of five years, in compliance with Curaçao's AML regulations.

Transaction data, verification records, and other relevant documents are stored securely to ensure data integrity, confidentiality, and ease of access for regulatory audits.

Records are periodically reviewed for completeness and accuracy, with the MLRO overseeing compliance with all record-keeping requirements. Data retention schedules are strictly enforced to align with legal and regulatory obligations.

9. POLICY BREACHES AND DISCIPLINARY ACTIONS

Non-compliance with this Crypto Usage Policy, including failure to adhere to verification, monitoring, AML, data security, or fraud prevention protocols, may result in disciplinary action, up to and including termination of employment.

Any violations identified during internal audits, transaction monitoring, or regulatory reviews are escalated to the Compliance Department, which assesses and enforces appropriate remedial actions.

The MLRO is responsible for ensuring all breaches are documented and corrective measures are implemented.

Repeated offenses or significant breaches may lead to further legal action or sanctions, depending on the severity of the violation.

10. EXAMPLES OF ML/TF INDICATORS ASSOCIATED WITH THE USE OF VIRTUAL ASSETS (VA), CRYPTOCURRENCIES

- Client conducts activities with VA, whose public key is related to black market purchases (Darkweb) or other illegal activity
- Client VA public key is disclosed on websites that are associated with illegal activities
- An analysis of the blockchain clearly shows that the virtual wallet has a suspicious source of funds, such as that related to black market purchases
- The Client's email address or phone number is associated with a recognizable VA peer to peer exchange platform for its advertising purposes
- Client's VA transactions are made from questionable IP addresses, from IP addresses registered in sanctioned countries, or from IP addresses identified as suspicious
- A Client, who is significantly older than most users of a VA platforms, opens a VA account and conducts a large amount of different transactions, raising suspicions, that a money mule is involved in the transactions, or an older person has become a victim and is being used to commit criminal activity
- The Client has poor knowledge of VA transactions despite being involved in VA transactions

(this could indicate that the person is a victim of fraud and may be used for ML/TF operations)

- In VA transactions mixing and tumbling services are applied, indicating the intent to hide illicit money flow between the virtual wallet and black market
- Client redirects a large number of VA transactions to VA platforms registered in low-tax or tax-free countries and territories
- Structuring VA transactions (e.g., exchange or transfer) in small amounts, or in amounts under record-keeping or reporting thresholds, similar to structuring cash transactions.
- Making multiple high-value transactions in short succession, such as within a 24-hour period; in a staggered and regular pattern, with no further transactions recorded during a long period afterwards; or to a newly created or to a previously inactive account
- Transferring VAs immediately to multiple VASPs, especially to VASPs registered or operated in another jurisdiction where –
 - there is no relation to where the customer lives or conducts business; or
 - there is non-existent or weak AML/CFT regulation
- Depositing funds from VA addresses that have been identified as holding stolen funds, or VA addresses linked to the holders of stolen funds.
- Incoming transactions from many unrelated wallets in relatively small amounts (accumulation of funds) with subsequent transfer to another wallet or full exchange for fiat currency.

Information Sources:

- 1) FATF Report on Vulnerabilities of Casinos and Gaming Sector
- 2) FATF Report on Virtual Assets Red Flag Indicators of Money Laundering and Terrorist Financing