

Crypto Policy

Aquarius Entertainment N.V.

Curaçao

May 2026

Version Control Table

Approval date	Changes description	Senior manager's signature	Compliance Officer's signature
19.05.2026	First issue		

Table of Contents

Version Control Table.....	2
Table of Contents	2
Introduction	3
Governance	3
Approval of Crypto Assets.....	4
Approval of VASPs	4
Transactions' Management.....	5
Deposits and withdrawals	5
Wallets' management	5
AML and RG controls	6
Incidents Management	6
Incident reports.....	6
Incident response.....	7
Record Keeping	8

Introduction

This **Crypto Policy** (Policy) is applicable for the Senior Management, Compliance Officer, employees working with payments (Payments Team) as well as other employees of the Company. The Policy establishes the procedures and risk controls applicable to the use of crypto assets in connection with the Company's online casino operations.

This Policy shall be signed off by the Compliance Officer and approved by the resolution of the Senior Management. This Policy is subject to review by the Compliance Officer and Senior Management **at least annually**. The proposal for a review and the review of this Policy may be scheduled more often by the decision of the Compliance Officer or Senior Management. The Company must also review and, where necessary, update this Policy in the case of any regulatory change or material incidents.

Governance

The **Senior Management** retains the ultimate accountability for the application of this Policy and is responsible for:

- approval of supported crypto assets;
- approval of VASPs the Company partners with;
- risk appetite determination;
- approval of thresholds and transaction limits;
- review of material incidents;
- implement the appropriate and effective organizational and operational structure necessary to comply with the Policy, paying particular attention to the sufficient authority and the appropriateness of the human and technical resources.

The **Compliance Officer** is responsible for the day-to-day application of this Policy and shall:

- support the Senior Management in the assessment of crypto asset risks;
- receive and assess incident reports;
- escalate incidents to the relevant department;
- ensure the fulfilment of record-keeping obligations;
- perform other functions which are assigned under the applicable law, guidelines, internal policies and job description.

The **Payments Team** is primarily responsible for:

- compliance monitoring of crypto asset transactions and the facilitation of such transactions;
- perform other functions which are assigned under the applicable law, guidelines, internal policies and job description.

Approval of Crypto Assets

Prior to the approval of a new crypto asset, the Company shall assess the risks relating to the specific crypto asset and shall consider at least the following for each crypto asset:

- liquidity;
- anonymity-enhancing features;
- exposure to illicit activities (incl. fraud, ML/TF, sanctions exposure);
- whether the crypto asset is regulated;
- volatility (incl. use of algorithmic measures to maintain its value).

The Company should also consider the necessity to apply any asset-specific deposit/withdrawal limits, cooling-off or hold periods (e.g. based on the volatility and liquidity of the crypto asset).

The following crypto assets and transactions are not permitted in the course of the provision of online casino services:

- privacy coins (e.g. Monero (XMR), Zcash (ZEC) and Dash);
- meme coins (e.g. DOGE, SHIP and PEPE);
- wrapped tokens of unknown origin (e.g. such as wrapped BTC);
- deposits routed via sanctioned mixers/tumblers (e.g., Tornado Cash, Blender.io, Sinbad.io) or wallets on sanctions lists.

In order to assess the above, the Company shall collect or refer to the relevant documents and other sources, which may include the following:

- white papers;
- blockchain analytics reports;
- audit reports;
- exchange listings;
- liquidity and volatility reviews;
- internet searches.

The risk assessment carried out under this section shall be documented and signed-off by the Senior Management.

Approval of VASPs

Prior to partnering with any new VASP, the Company shall assess the risks relating to the specific VASP and shall consider at least the following for each VASP:

- solvency;
- authorization(s)/registration(s) held;
- links to illicit activities (incl. fraud, ML/TF, sanctions exposure);
- incident history;
- whether the VASP demonstrates:
 - robust AML/CFT controls;

- FATF Travel Rule compliance;
 - transaction monitoring capabilities.
- whether the VASP has sufficient security controls, including:
 - multi-factor authentication and/or hardware security models;
 - withdrawal whitelists to restrict outbound transfers;
 - multi-sig protocols for treasury wallet operations.

In order to assess the above, the Company shall collect or refer to the relevant documents and other sources, which may include the following:

- registry extracts;
- direct checks from the registers (incl. corporate, licenses);
- good standing reports;
- internet searches;
- audit reports;
- internal policies (incl. AML/CTF and Sanctions Policies);
- contracts and SLAs;
- questionnaires.

The risk assessment carried out under this section shall be documented and signed-off by the Senior Management.

Transactions' Management

Deposits and withdrawals

When allowing the customers to transact with crypto assets, the Company shall disclose the following information prior to executing the transaction:

- network and other applicable fees;
- conversion or gas-fee handling rules.

The Company accepts deposits from and makes withdrawals only to crypto asset wallets which are opened in the name of the customer. The crypto asset wallet where the withdrawal is made must be the same wallet from which the customer made the deposit. Withdrawals must be processed in the same currency that the deposit was made. The Company shall not facilitate any transfers between customers on the platform.

Wallets' management

The Company shall hold its crypto assets only in a crypto asset wallet which has been opened in the name of the Company or its payment subsidiary (no personal/UBO-linked wallet allowed).

The crypto assets shall be segregated in the following manner:

- operational wallets (for day-to-day transactional flows);

- treasury wallets¹ (for strategic reserves and capital management);
- player-flow wallets (for customer-facing deposits and withdrawals).

AML and RG controls

The Company shall take into account the risks related to transactions using crypto assets when conducting its ML/TF risk assessment and determining the applicable AML/CTF and RG measures (incl. CDD/EDD/ODD, Travel Rule, self-exclusions, behavioral signals).

Incidents Management

Given the heightened risk profile of crypto asset transactions, crypto-asset-related incidents shall be treated as high-priority events requiring immediate review. Crypto-asset-related incidents may include, among other things:

- compromised keys;
- suspicious deposit rings;
- smart-contract failures;
- chain forks;
- exchange outages.

The Company classifies incidents into 4 categories, based on the severity of the incident:

1. Low – minor issues with limited impact, no material financial exposure, and no indication of fraud, AML concern, or customer harm.
2. Medium – incidents with elevated operational risk, limited customer impact, or potential compliance concerns.
3. High – incidents involving significant financial exposure, strong suspicion of fraud or money laundering, cybersecurity or safeguarding concerns.
4. Major – critical events involving severe financial loss, actual compromise of customer assets, major regulatory exposure, systemic control failure, or significant business continuity risk.

Incident reports

The employee shall report are incidents to the Compliance Officer via email or other secure channel. Incident report shall describe the essential details of the incident to provide a comprehensive understanding, including, the following details:

- date and time of the identification of the incident;
- specific systems, solutions or services impacted by the incident
- clear and concise description of the incident, including what occurred, how it was detected, and any preliminary observations;
- an initial evaluation of the incident's potential impact on operations, including any immediate effects on service delivery, security, or compliance (where possible);

¹ multi-sig

- the name, role, and contact information of the individual reporting the incident.

The Compliance Officer should acknowledge the receipt of the incident report and provide an initial assessment of the situation. Depending on the severity and potential impact, the Compliance Officer may escalate the incident to the Senior Management, board of directors or specialized department (e.g. IT). Major incidents require immediate escalation to the senior management.

The employee shall also assess the necessity to send an unusual transaction report in accordance with the Company's AML Policy.

Incident response

After receiving the incident report, the incident response process consists of the following steps:

1. initial assessment;
2. Incident containment
3. Escalation
4. Resolution and recovery
5. Post-incident actions

The Compliance Officer shall conduct, and where necessary coordinate, the **initial assessment** of the incident and determine the appropriate allocation of resources. The assessment should address the following key areas:

- evaluation of the impact on the Company's operations, systems, and data and determining the severity of the incident;
- identifying the systems, networks, or applications affected and assessing whether the incident is localized or widespread.
- estimating the potential risk and damage that could be caused if the incident is not addressed promptly.

Depending on the nature and severity of the incident determined as result of the initial assessment of the incident, the Company shall proportionate **containment measures** to prevent further disruption, exposure or loss. Containment measures may include:

- suspension of withdrawals or deposits;
- freezing affected customer accounts;
- isolation of compromised wallets;
- revocation of privileged access;
- transfer of assets to secure custody;
- suspension of affected crypto assets or VASP services;
- application of temporary transaction limits or manual approval controls.

Depending on the nature and severity of the incident determined as result of the initial assessment of the incident, it may be necessary to **escalate** the incident to the relevant stakeholders, including internal departments and external partners. The Compliance Officer shall coordinate the escalation process.

Following the incident containment and escalation, the Company shall take the proportionate measures for incident **resolution and recovery** to restore the affected operations and systems as well as to identify the root cause of the incident. Resolution and recovery actions may include:

- completion of fraud or AML investigations;
- recovery or reconciliation of affected funds;
- closure of suspicious accounts;
- termination or suspension of VASP relationships;
- wallet replacement or security remediation;
- customer remediation, where appropriate.

The Compliance Officer shall ensure that all incidents are properly documented for future reference. The Company shall regularly track and assess the incident response metrics to evaluate its effectiveness. After each major incident a comprehensive review of the incident management processes shall be conducted, including follow-up review(s) to assess the effectiveness of the incident response measures applied.

Record Keeping

The Company shall follow the record-keeping requirements for Travel Rule payloads, on-chain risk reports, KYC, and transaction logs established in the Company's AML Policy.

The Company shall ensure the reconciliation between blockchain explorers, exchange statements, and internal ledgers – enabling independent audit reproduction.