

Crypto Usage Risk Policy for JarvisDelivery B.V.

Effective Date: July 16th, 2025

Next Review Date: July 16th, 2026

1. Introduction

This Crypto Usage Risk Policy (the “Policy”) establishes controls and guidelines for managing risks associated with the acceptance, transfer, and usage of cryptocurrencies by JarvisDelivery B.V. (hereinafter - “JarvisDelivery”, “Company”). It supplements the Company’s existing AML/CFT Policy, designed to mitigate the risks of money laundering, terrorist financing, and fraud through virtual asset transactions.

2. Scope and Applicability

This Policy applies to all customers, partners, contractors, and employees of JarvisDelivery who are involved in crypto transactions within the operational framework of the Company. It also applies to all crypto-related service providers, exchanges, and wallet operators interacting with JarvisDelivery’s platforms.

3. Risk-Based Approach to Crypto

In line with Section 1.3 of the AML/CFT Policy, JarvisDelivery adopts a risk-based approach to crypto asset usage. This includes:

- Assessing the inherent risk of each crypto transaction, including source, volume, and purpose;
- Implementing enhanced controls for higher-risk virtual assets or jurisdictions;
- Continuous monitoring of trends and typologies in crypto-based laundering.

4. Acceptable Use of Crypto Assets

4.1. JarvisDelivery only accepts and transacts with cryptocurrencies that have sufficient liquidity, transparency, and are not associated with high-risk jurisdictions or sanctioned activities.

4.2. The Company will only support wallets and exchanges that are registered or licensed in reputable jurisdictions and are AML/CFT compliant.

4.3. Direct crypto-to-crypto conversions through unregulated third parties are prohibited.

5. Customer Due Diligence for Crypto Users

5.1. Customers intending to use cryptocurrency as a means of payment or investment must undergo full Standard Customer Due Diligence (CDD), as defined in Section 4 of the AML/CFT Policy.

5.2. Where crypto is used, Enhanced Due Diligence (EDD) shall be conducted in the following cases:

- High-value crypto transactions exceeding NAF 5,000 equivalent per one gaming day;
- Use of privacy coins or obfuscation tools (e.g., mixers, tumblers, privacy wallets);
- Source of funds linked to unregulated or peer-to-peer exchanges;
- Transactions from/to wallets without clear beneficial ownership.

5.3. The Company must obtain:

- Source of crypto funds (e.g., wallet history, mining records, exchange records);
- Declaration and documentary evidence of source of wealth if cumulative transactions exceed NAF 4,000.

6. Transaction Monitoring

6.1. Blockchain analytics tools may be used to monitor incoming and outgoing crypto flows only based on their preliminary risk assessment conducted by the relevant team via alerting to the appropriate communication software for:

- Suspicious volume patterns (structuring/smurfing);
- Links to darknet, ransomware, or high-risk services;
- Ties to sanctioned addresses or wallets;
- Mixing/tumbling patterns or enhanced privacy protocols.

6.2. Any anomaly identified will result in:

- Immediate escalation to the Compliance Officer;
- Temporary suspension of account activities;
- Possible filing of a Suspicious Activity Report (SAR) to the FIU.

7. Prohibited Practices

JarvisDelivery strictly prohibits:

- Use of anonymous, non-custodial wallets for corporate payments;
- Use of decentralized exchanges (DEXs) without an identifiable counterparty.

8. Record Keeping

All crypto-related records shall be retained for a minimum of five years in line with Section 7.2 of the AML/CFT Policy. This includes:

- Crypto transaction logs (with timestamp, wallet addresses, hash IDs);
- Wallet ownership verification documents;
- Blockchain analytics reports, if any;
- Related correspondence and internal memos.

9. Training and Awareness

Staff involved in crypto transaction handling will receive specialized training in:

- Blockchain forensics and virtual asset risk assessment;
- Crypto-specific red flags (see Section 6.3 of AML Policy);
- FATF guidance on virtual assets and VASPs.

Training will be updated annually or upon significant regulatory or technological developments.

10. Reporting Obligations

10.1. All crypto transactions suspected of involving criminal property or used to finance terrorism shall be reported internally to the Compliance Officer and externally to the FIU within statutory timeframes.

10.2. Tipping-off rules as outlined in Section 6.7 of the AML/CFT Policy apply fully to crypto transactions.

11. Third-Party Service Providers

Any third-party virtual asset service provider (VASP) engaged by JarvisDelivery must:

- Hold a valid license from a recognized regulatory authority;
- Comply with AML/CFT obligations equivalent to Curacao's regulatory standards;
- Be subject to periodic vendor due diligence and monitoring.

12. Policy Governance

The AML/CFT Compliance Officer is responsible for the implementation and enforcement of this Policy. The Policy will be reviewed annually or more frequently in response to changes in legal or regulatory obligations or evolving threats.

The Policy is signed on this day July 16, 2025



Oleksandr Zaitsev, CO of Sharkscore B.V.