

Crypto Risk Policy

Daintree Interactive B.V. (hereinafter “Company”) Crypto Risk Policy

1. Introduction

Daintree Interactive B.V., a business-to-business (B2B) provider of gambling-related services and goods, registered and operating in Curaçao under a license from the Curaçao Gaming Authority (CGA), is committed to managing risks associated with cryptocurrency transactions. This Crypto Risk Policy supplements our Anti-Money Laundering and Countering the Financing of Terrorism (AML/CTF) Policy, focusing on crypto-specific risks in our B2B operations. As a B2B provider, the Company supplies critical services or goods to B2C gaming operators. This Policy ensures compliance with Curaçao’s regulatory framework under the Landsverordening op de kansspelen (LOK), including enhanced AML measures for crypto, and aligns with international standards such as those from the Financial Action Task Force (FATF).

2. Objectives

The objectives of this Crypto Risk Policy are to:

- Prevent the use of cryptocurrency in our services for money laundering, terrorism financing, or other illicit activities.
- Ensure compliance with CGA requirements under LOK for B2B providers, including robust KYC, CDD, and transaction monitoring for crypto-related dealings.
- Implement effective risk-based measures when onboarding and monitoring B2C operator clients that may involve crypto transactions.
- Identify and report suspicious crypto-related activities to relevant authorities.
- Maintain the integrity of our B2B operations in the gambling industry.

3. Scope

This policy applies to all business activities conducted by Daintree Interactive B.V., including:

- Provision of critical services or goods to B2C gaming operators that may involve cryptocurrency payments or integrations.
- Onboarding and ongoing monitoring of B2C operator clients for crypto-related risks.
- Financial transactions with clients, including any crypto payments received from or made to clients.
- Interactions with the CGA and other regulatory bodies regarding crypto compliance.

4. Regulatory Compliance

Daintree Interactive B.V. adheres to the LOK framework governing B2B gambling providers in Curaçao, including crypto-specific AML, KYC, and CTF requirements. We maintain policies to ensure compliance with:

- CGA guidelines on crypto payments, mandating thorough CDD, EDD, sanctions/PEP screening, and transaction monitoring.
- Obligations to identify and verify Ultimate Beneficial Owners (UBOs) and Key Persons of B2C clients involved in crypto.
- Reporting of unusual or suspicious crypto transactions to the competent authority.
- International standards, including FATF guidelines and EU directives.

Our compliance program meets CGA standards and aligns with global best practices for crypto risk management in gambling.

5. Know Your Customer (KYC) Procedures for Crypto

5.1 Onboarding B2C Clients Involved in Crypto

Before entering a relationship with any B2C operator client that may involve crypto, Daintree Interactive B.V. conducts thorough KYC due diligence.

5.1.1 Natural Persons (if applicable to client structure)

Collect and verify: Official full name, permanent address, ID/passport number, date/place of birth, occupation, and source of funds/wealth (especially for crypto holdings).

Verification uses certified government-issued documents and proof of address (not older than 3 months).

5.1.2 Corporate Persons

Collect and verify: Official name, registration number, date of incorporation, registered address, names of directors/UBOs (>10% control), principal activity, and source of funds/wealth (including crypto sources).

Verification requires constitutional documents, Certificate of Incorporation, and certified IDs for UBOs/Key Persons.

5.1.3 Crypto-Specific KYC Measures

- Verify crypto wallet addresses used by clients for payments.
- Use blockchain analytics tools to screen wallets for links to illicit activities or sanctioned entities.

- Require declaration of crypto fund origins; reject privacy coins or high-risk assets.

5.2 Ongoing Monitoring

Conduct continuous monitoring of client relationships, with reviews based on risk:

- Low (every 3 years), Medium (every 2 years), High (annually).

Monitor for changes in crypto usage, ownership, or risk profile.

5.3 Enhanced Due Diligence (EDD)

Apply EDD for high-risk clients (e.g., PEPs, non-reputable jurisdictions, or heavy crypto involvement): Senior approval, notarized documents, enhanced source of funds verification, and increased transaction scrutiny.

6. Transaction Monitoring and Reporting for Crypto

6.1 Transaction Monitoring

Monitor all client transactions involving crypto for inconsistencies:

- Review patterns for unusual volumes, rapid transfers, or crypto-to-fiat conversions without clear purpose.
- Use automated tools to flag high-value crypto transactions or those from high-risk wallets.
- Ensure alignment with client's stated activities and risk profile.

6.2 Reporting Suspicious

Transactions Suspect crypto activities are reported to the competent authority, with details on client, transaction, and suspicion.

Avoid tipping off clients.

Senior management oversees reporting.

6.3 Record-Keeping

Retain all crypto-related KYC, transaction, and reporting records for at least five years, stored securely per data protection rules, and available to CGA upon request.

7. Risk Assessment and Mitigation for Crypto

Conduct regular assessments of crypto risks in B2B operations:

- Client Risk: Based on type, structure, and crypto involvement.
- Product Risk: AML vulnerabilities in crypto-enabled services.
- Geographical Risk: Exposure to high-risk jurisdictions for crypto.
- Technological Risk: Blockchain vulnerabilities.

Mitigation includes structured KYC/EDD, enhanced monitoring for crypto, annual reviews, and staff training on crypto risks.

8. Training and Awareness

All employees receive annual AML/CTF training, with crypto-specific modules on identifying suspicious crypto patterns, wallet screening, and blockchain risks.

Training is documented and includes onboarding sessions.

Additional training for client-facing staff.

9. Internal Controls and Audits

Maintain internal controls for crypto compliance:

- Regular audits of KYC and monitoring processes, overseen by senior management.
- Independent external audits if required by CGA.

10. Cooperation with Authorities

Cooperate fully with CGA, FIU, and others by providing crypto-related information, submitting reports, and participating in audits.

11. Policy Review and Updates

This Policy is reviewed annually or upon regulatory changes, approved by senior management, and communicated to employees.

Contact Information

For inquiries: accounts@daintreegaming.com

Approval

Approved by:

Date: