

Anti-Money Laundering and Countering the Financing of Terrorism (AML/CTF) Policy

1. Introduction

Daintree Interactive B.V., a business-to-business (B2B) provider of gambling-related services and goods, registered and operating in Curaçao, is committed to preventing money laundering and terrorism financing. This Anti-Money Laundering and Countering the Financing of Terrorism (AML/CTF) Policy outlines our procedures to ensure compliance with applicable regulations. As a B2B provider, Daintree Interactive B.V. supplies critical services or goods to gaming operators, implementing robust Know Your Customer (KYC) and AML/CTF measures to safeguard our operations and maintain the integrity of our commercial relationships.

This policy applies to all employees, contractors, and third parties engaged with Daintree Interactive B.V.. It ensures our business practices align with international best practices, including standards set by the Financial Action Task Force (FATF), and Curaçao's regulatory framework, fostering a safe, transparent, and responsible gambling environment.

2. Objectives

The objectives of this AML/CTF Policy are to:

- Prevent the use of our services for money laundering, terrorism financing, or other illicit activities.
- Ensure compliance with Curaçao's regulatory requirements for B2B gambling providers.
- Implement effective KYC processes when onboarding third-party clients (e.g., gaming operators or suppliers).
- Identify and report suspicious transactions or activities to the relevant authorities.
- Protect vulnerable persons and maintain the integrity of the gambling industry.
- Promote a culture of compliance through training and awareness.

3. Scope

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

- Provision of critical services or goods to gaming operators.
- Onboarding and ongoing monitoring of third-party clients.
- Financial transactions, including payments received from or made to clients.

- Interactions with the Curaçao Gaming Authority (CGA) and other regulatory bodies.

4. Regulatory Compliance

Daintree Interactive B.V. adheres to the regulatory framework governing B2B gambling providers in Curaçao, including requirements for AML, KYC, and the prevention of terrorism financing. We maintain policies and procedures to ensure compliance with:

- Licensing requirements for suppliers of critical services or goods.
- Obligations to identify and verify Ultimate Beneficial Owners (UBOs) and Key Persons of clients.
- Reporting of unusual or suspicious transactions to the appropriate authorities.
- Safeguards to prevent vulnerable persons from engaging in gambling activities.
- Record-keeping and reporting obligations to support regulatory oversight.

Our compliance program is designed to meet the standards set by the CGA and aligns with international AML standards, ensuring a responsible and transparent gambling ecosystem.

5. Know Your Customer (KYC) Procedures

5.1 Onboarding Third-Party Clients

Before entering into a commercial relationship with any third party, Daintree Interactive B.V. conducts thorough KYC due diligence to verify the identity and legitimacy of the client.

5.1.1 Natural Persons

For clients who are natural persons, Daintree Interactive B.V. collects and verifies:

- Official full name.
- Permanent residential address.
- Identity card or passport number.
- Date and place of birth.
- Occupation or principal business activity.
- Place of business activity.

Verification requires a certified true copy of an original, unexpired government-issued identification bearing a photograph. The certification must include the certifier's name, signature, profession or designation, date of certification, and contact details. Proof of residential address is required via a certified true copy of:

- A utility bill, bank statement, or equivalent document issued by a government authority, not older than 3 months. Phone bills are not accepted.

For high-risk cases, additional verification of source of wealth and source of funds is required, using documents such as bank statements, tax returns, or other evidence of legitimate income.

5.1.2 Corporate Persons

For corporate clients, Daintree Interactive B.V. collects and verifies:

- Official full name.
- Registration number.
- Date of incorporation.
- Registered address and principal place of business (if different).
- Names of all directors and Ultimate Beneficial Owners (UBOs, holding >10% shares, voting rights, or control).
- Principal business activity.
- Source of wealth and source of funds.

Verification requires:

- Constitutional documents (e.g., Memorandum and Articles of Association).
- Certificate of Incorporation or Registration.
- Certificate of Good Standing (where applicable).
- Certified identification documents for UBOs and Key Persons.
- Group structure (if part of a larger group) to identify UBOs.

Documents in a foreign language must be translated by an independent, competent translator, with the translation dated, signed, and certified as faithful to the original.

5.1.3 Risk Assessment

Each client undergoes a risk assessment to assign a risk category (Low, Medium, High) based on:

- Nature, scale, and complexity of the client's activities.
- Products, services, and delivery channels.
- Geographic location of operations and source of funds.

5.2 Ongoing Monitoring

Daintree Interactive B.V. conducts continuous monitoring of client relationships to detect changes in ownership, control, or risk profile, including:

- Annual updates to KYC records, with frequencies based on risk category:
 - **Low Risk:** Review every 3 years.
 - **Medium Risk:** Review every 2 years.
 - **High Risk:** Review annually.
- Monitoring transactions for unusual patterns or activities indicative of money laundering or fraud.
- Reviewing client compliance with their own AML/KYC and responsible gambling obligations.
- Updating client information upon trigger events (e.g., new business relationships or changes in ownership).

5.3 Enhanced Due Diligence (EDD)

For high-risk clients, including Politically Exposed Persons (PEPs), clients in non-reputable jurisdictions, or those not physically present for identification, Daintree Interactive B.V. applies EDD, including:

- Senior management approval to establish or continue the relationship.
- Certified, high-quality documentation (e.g., notarized IDs or corporate documents).
- Verification of source of wealth and funds using supplementary measures.
- Enhanced ongoing monitoring of transactions and business activities.

A **PEP** is defined as a person entrusted with prominent public functions (e.g., head of state, senior politician, judicial official, or high-ranking officer), their immediate family members, or close associates with significant control or financial influence.

6. Transaction Monitoring and Reporting

6.1 Transaction Monitoring

Daintree Interactive B.V. monitors all financial transactions with clients to identify and investigate suspicious activities, including:

- Reviewing payment patterns for inconsistencies (e.g., high-value transactions, rapid transfers, or transactions with no clear business purpose).
- Ensuring transactions align with the client's stated business activities and risk profile.
- Using automated systems (where applicable) to flag unusual transactions based on predefined risk indicators.

6.2 Reporting Suspicious Transactions

If a transaction or activity is suspected of being linked to money laundering, terrorism financing, or other illicit activities, Daintree Interactive B.V. will:

- Report the activity to the Curaçao Financial Intelligence Unit (FIU) via the goAML reporting system, as required for B2B gambling providers.
- Provide all relevant details, including client identity, transaction details, and the nature of the suspicion.
- Refrain from informing the client of the report to avoid tipping off, in line with confidentiality obligations.
- Ensure senior management oversees the reporting process.

6.3 Record-Keeping

All KYC and transaction records are retained for a minimum of five years, including:

- Client identification and verification documents.
- Transaction logs, including payment details and supporting documentation.
- Reports of suspicious activities and correspondence with regulatory authorities. Records are stored securely in compliance with data protection regulations and made available to the CGA upon request.

7. Responsible Gambling and Vulnerable Persons

As a B2B provider, Daintree Interactive B.V. supports its clients in implementing responsible gambling measures to protect vulnerable persons, including:

- Ensuring clients have policies to identify and exclude vulnerable persons (e.g., minors, individuals with gambling addiction, or those banned from gambling).
- Providing technical or operational support for age verification and self-exclusion mechanisms.
- Advising clients on responsible gambling practices, such as setting deposit limits or offering self-exclusion options.

8. Risk Assessment and Mitigation

Daintree Interactive B.V. conducts regular risk assessments to identify and mitigate AML risks specific to its B2B operations, considering:

- **Client Risk:** Risk level based on client type, ownership structure, and business activities.
- **Product Risk:** AML risks associated with services or goods provided.
- **Geographical Risk:** Risks tied to jurisdictions where clients operate, especially non-reputable jurisdictions.

- **Business Practices Risk:** Risks from transaction channels or employee complicity.
- **Technological Risk:** Vulnerabilities in technological developments used in service delivery.

Mitigation measures include:

- Structured KYC due diligence for all clients.
- Enhanced monitoring for high-risk clients and transactions.
- Annual risk assessments reviewed by senior management.
- Staff training to recognize and address AML risks.

9. Training and Awareness

All employees and relevant contractors receive regular AML training to ensure awareness of:

- AML and KYC obligations under Curaçao's regulations.
- Procedures for identifying and reporting suspicious activities.
- Responsible gambling principles and the protection of vulnerable persons. Training is conducted annually and upon onboarding, with additional sessions for high-risk roles (e.g., client-facing staff). Training records are maintained for CGA inspections.

10. Internal Controls and Audits

Daintree Interactive B.V. maintains robust internal controls to ensure AML compliance, including:

- Regular audits of KYC and transaction monitoring processes, overseen by senior management.
- Independent reviews by external auditors, if required by the CGA.
- Documentation of all compliance activities, including risk assessments and incident reports.

11. Cooperation with Authorities

Daintree Interactive B.V. cooperates fully with the CGA, FIU, and other relevant authorities by:

- Providing timely and accurate information upon request.
- Submitting required reports, such as annual financial statements and incident reports, by CGA deadlines.
- Participating in CGA audits or inspections to verify compliance.

12. Policy Review and Updates

This AML/CTF Policy is reviewed annually or upon significant regulatory changes to ensure alignment with Curaçao's gambling and AML regulations. Updates are approved by senior management and communicated to all employees.

13. Contact Information

For inquiries related to this AML/CTF Policy, please contact:

Daintree Interactive B.V.

Dr. M.J. Hugenholtzweg 25, Willemstad, Curacao

accounts@daintreegaming.com

Approval

This AML/CTF Policy was approved by the Board of Directors of Daintree Interactive B.V.
on

[Insert Date].

[Authorized Representative]

[Name and Title]