



AML/CTF POLICY

B2B



MAY 30, 2025

DAINTREE INTERACTIVE B.V.
Dr. M. J. Hugenholtzweg 25, Willemstad, Curaçao

Table of Contents

1. Policy Statement.....	2
2. Purpose	2
3. Audience	2
4. Definitions.....	2
5. Policy Implementation.....	2
5.1 Business Risk Assessment	3
5.2 Customer Risk Assessment.....	3
5.3 Customer Acceptance Policy	3
5.4 Customer Due Diligence	3
5.5 Ongoing Monitoring	3
5.6 Reliance on Third Parties.....	3
5.7 Reporting of Unusual Transactions.....	3
5.8 AML Compliance Program	3
6. Compliance and Consequences of Non-Compliance	4
7. Related Information.....	4
8. Contact Information.....	4
9. Policy History	4
10. Policy URL	4

1. Policy Statement

Daintree Interactive B.V. is committed to conducting business in an ethical and compliant manner. A stringent zero-tolerance policy is enforced regarding acts of money laundering and terrorist financing. Daintree's AML/CTF Program is aligned with the Curaçao Gaming Control Board's AML Policy Template and complies with the National Ordinance on the Identification of Clients (NOIS), the Reporting of Unusual Transactions (NORUT), the Sanctions National Ordinance, and international frameworks including the FATF 40 Recommendations. As a B2B operator, Daintree does not deal with end-users or players but is responsible for ensuring AML/CFT controls are applied to all business counterparties.

2. Purpose

The purpose of this policy is to define the responsibilities of Daintree Interactive B.V., its directors, officers, and staff concerning anti-money laundering and counter-terrorism financing obligations. It guides staff in identifying suspicious activities and taking the appropriate steps to mitigate financial crime risk. The policy is designed to protect the organization, its stakeholders, and its reputation.

3. Audience

This policy applies to all entities and personnel of Daintree Interactive B.V., including directors, officers, employees, contractors, agency workers, seconded staff, consultants, and business partners regardless of location.

4. Definitions

ML: Money Laundering

TF: Terrorist Financing

PEP: Politically Exposed Person

CDD: Customer Due Diligence

EDD: Enhanced Due Diligence

MLRO: Money Laundering Reporting Officer

CRA: Customer Risk Assessment

BRA: Business Risk Assessment

UTR: Unusual Transaction Report

FIU: Financial Intelligence Unit of Curaçao

5. Policy Implementation

5.1 Business Risk Assessment

Daintree proactively identifies and assesses the ML/TF risks arising from its operations, jurisdictional presence, and business partners. These risks are reviewed through a Business Risk Assessment (BRA) process, which is reviewed annually or upon significant business changes. The BRA includes jurisdictional risk, client type, and services offered.

5.2 Customer Risk Assessment

A Customer Risk Assessment (CRA) is performed for each B2B client before establishing a relationship. The assessment covers ownership structure, industry sector, country of operation, and the strength of the client's internal AML controls.

5.3 Customer Acceptance Policy

Daintree applies a rigorous acceptance policy requiring documentation such as incorporation certificates, shareholder registers, beneficial ownership details, and sanctions screening. Clients operating in high-risk jurisdictions or failing due diligence checks are rejected.

5.4 Customer Due Diligence

CDD procedures include verifying corporate identity, beneficial ownership, business purpose, and evaluating AML controls. EDD is conducted on high-risk clients or PEP-linked entities. Sanctions lists and adverse media are also checked.

5.5 Ongoing Monitoring

Relationships are monitored to identify changes in client behavior, ownership, or risk profile. Reviews are conducted periodically and upon triggers such as regulatory alerts, control weaknesses, or adverse media.

5.6 Reliance on Third Parties

Daintree may rely on third parties to assist in conducting certain CDD elements, provided that those third parties are supervised and regulated entities. Ultimate responsibility remains with Daintree Interactive B.V.

5.7 Reporting of Unusual Transactions

The MLRO is responsible for reporting suspicious activities and Unusual Transaction Reports (UTRs) to FIU Curaçao via the secure portal (https://portal.fiucuracao.cw/goAMLWeb_PRD/Home) All personnel must report concerns promptly, and tipping-off is strictly prohibited.

5.8 AML Compliance Program

The AML program includes the appointment of a dedicated MLRO and deputies, internal controls, recordkeeping, training, audits, and policy reviews. The Risk and Compliance Committee oversees program integrity and reviews effectiveness regularly.

6. Compliance and Consequences of Non-Compliance

Non-compliance with this policy may result in disciplinary actions including dismissal, termination of business relationships, and criminal prosecution. Daintree reserves the right to amend this policy at its discretion.

7. Related Information

- Curaçao NOIS and NORUT
- Sanctions Ordinance
- FATF 40 Recommendations
- CGA AML/CFT Policy Template (2025)
- EU AML Directives

8. Contact Information

MLRO – Daintree Interactive B.V.

Email: compliance@daintreebv.com

9. Policy History

This policy replaces earlier internal AML notes and informal procedures. Adopted in June 2025.

10. Policy URL

Internal only – not publicly published.