

Anti-Money Laundering and Counter-Terrorism Financing Policy

Mill Interactive B.V.

Version 1.0 | Effective: June 30, 2025 | Reviewed Annually

Preface

This Anti-Money Laundering and Counter-Terrorism Financing (AML/CTF) Policy outlines the framework and procedures that Mill Interactive B.V. follows to detect, prevent, and report money laundering and terrorist financing across its business activities. The policy reflects our commitment to maintaining integrity, transparency, and accountability in compliance with Curaçao's legal obligations and the CGA's January 2025 AML Policy Template.

It serves as a critical guide for all employees, contractors, and partners in safeguarding our operations against financial crime and reputational risk.

1. Policy Statement

This policy defines Mill Interactive B.V.'s commitment to AML/CTF compliance. It affirms our zero-tolerance stance on financial crime and our adherence to Curaçao AML legislation and CGA directives.

Money laundering is the process by which individuals or entities conceal the origins of illicit funds to make them appear legitimate. It generally follows three stages:

- Placement: Introducing illicit funds into the financial system.
- Layering: Conducting complex transactions to obscure the origin.
- Integration: Reintroducing the now-laundered funds as apparently legitimate assets.

Terrorist financing may involve both lawful and unlawful funds used to support terrorist activity. Although the source may be legal, the intended use makes it illicit under AML/CTF laws.

Mill Interactive B.V. is committed to combating both ML and TF risks through prevention, detection, and reporting protocols aligned with international standards.

2. Purpose

The purpose of this policy is to implement a structured framework that enables Mill Interactive B.V. to identify, assess, manage, and mitigate ML/TF risks in its online

operations. It ensures compliance with regulatory obligations and supports a transparent financial ecosystem.

3. Audience

This policy applies to all:

- Employees
- Board members and management
- Compliance staff
- Contractors, consultants, and affiliates

All must understand and comply with this policy to protect the Company from ML/TF-related risks and liabilities.

4. Definitions

This section provides clarity on key AML/CTF concepts:

- Money Laundering (ML): Concealing the origins of criminal proceeds.
- Terrorist Financing (TF): Providing funds with intent to support terrorist acts.
- Customer Due Diligence (CDD): Measures to identify and verify customers.
- Enhanced Due Diligence (EDD): Additional scrutiny for high-risk clients.
- Politically Exposed Person (PEP): Individuals with prominent public functions and their close associates.
- Ultimate Beneficial Owner (UBO): A natural person who owns or controls $\geq 25\%$ of an entity.
- Suspicious Transaction Report (STR): A report submitted to authorities when suspicious activity is identified.

5. Policy Implementation

Implementation of this policy lies with the MLRO and is supervised by the Board. Operational practices are designed to integrate these procedures at all customer touchpoints.

Review Cycle: Annually

Responsible Office: Compliance Department

Approved by: Board of Directors

Effective Date: June 30, 2025

5.1 Business Risk Assessment

Business Risk Assessments (BRA) help identify ML/TF exposure across business lines. BRA evaluates:

- Customer base and jurisdictional reach

- Products, services, and delivery channels
- Volume and nature of transactions

BRA outcomes are documented, reviewed annually, and used to design proportionate internal controls.

5.2 Customer Risk Assessment

Every customer is subject to a Customer Risk Assessment (CRA) that categorizes them as low, medium, or high risk. Risk categories consider:

- Geographic risk (e.g., FATF-listed countries)
- Customer type (PEPs, corporate structures)
- Product engagement and transactional behavior

CRA outcomes dictate the depth of CDD applied and monitoring frequency.

5.3 Customer Acceptance Policy

Mill Interactive B.V. applies strict onboarding standards:

- No anonymous or unverifiable customers are accepted.
- Customers must provide valid identification and address information.
- High-risk individuals (PEPs, non-cooperative jurisdictions) are subject to EDD and may be denied.

The Company maintains an internal watchlist to flag and restrict high-risk or sanctioned individuals.

5.4 Customer Due Diligence

CDD is conducted:

- Before establishing a business relationship
- When transactions reach or exceed NAF 4,000
- When suspicion of ML/TF arises

Minimum information includes:

- Full name, date of birth, nationality
- Government-issued ID
- Verified residential address

For corporate clients, Mill Interactive identifies UBOs and collects incorporation documents. All PEPs are flagged for EDD and Board-level approval.

5.5 Ongoing Monitoring

Ongoing monitoring ensures consistency between customer profile and activity. It includes:

- Real-time and batch transaction reviews
- Alerts for abnormal patterns or jurisdictions
- Periodic KYC refresh based on risk level

Trigger events include:

- Changes in ownership
- Unusual transaction velocity
- Use of high-risk payment instruments

5.6 Reliance on Third Parties

Mill Interactive may rely on third parties for CDD only when:

- A contract guarantees access to verification records
- The third party is supervised under AML regulations
- The Company performs periodic assurance on quality of checks

Ultimate compliance responsibility remains with Mill Interactive B.V.

5.7 Reporting of Unusual Transactions

Any employee encountering suspicious behavior must report it to the MLRO immediately.

The MLRO:

- Logs all reports
- Assesses the need for STR submission
- Files STRs with FIU Curaçao where applicable
- Documents all decisions including rationale when an STR is not filed

All reports are retained for five years and are audit-accessible.

5.8 Anti-Money Laundering Compliance Program

The AML Compliance Program includes:

- Appointment of an independent MLRO
- Integration of BRA and CRA findings into decision-making
- Automated transaction monitoring tools
- Escalation protocols for suspicious behavior
- Annual review of controls, training, and reporting efficacy

The program is revised annually or upon material risk or regulatory change.

6. Compliance and Consequences of Non-Compliance

Violations of this policy may result in:

- Employment termination
- Regulatory penalties
- Legal prosecution
- Reputational damage to the Company

Employees and contractors are expected to uphold the highest standards of integrity in compliance matters.

7. Related Information

- AML/CFT Decree of Curaçao
- FATF Recommendations
- CGA AML Policy (Jan 2025)
- FIU Curaçao Reporting Platform: <https://www.fiucuracao.cw>

8. Contact Information

For AML-related inquiries or to report concerns:

MLRO Contact:

 compliance@millinteractive.com

Mill Interactive B.V.

9. Policy History

Version 1.0 – Approved by Board on June 30, 2025

Next Review Due: June 30, 2026

10. Policy URL

To be published internally via Company Compliance Portal.