



Anti-Money Laundering (AML) & Counter-Terrorist Financing (CTF) Policy

1. Policy Statement

This Anti-Money Laundering (AML) and Counter-Terrorist Financing (CTF) Policy establishes the commitment of Genco Pura B.V. (the “Company”) to comply with all applicable AML/CTF regulations and guidelines as required by the Curaçao Gaming Control Board (GCB). The Company is dedicated to preventing its platform from being used for money laundering, terrorist financing, or the financing of proliferation of weapons of mass destruction. This policy applies to all employees, management, contractors, suppliers, and third-party partners.

2. Purpose

The purpose of this policy is to establish a risk-based framework to detect, prevent, and report activities related to money laundering (ML), terrorist financing (TF), and proliferation financing (PF), in compliance with Curaçao AML/CTF regulations effective January 2025. It ensures alignment with the National Ordinance on the Identification of Services (NOIS), the National Ordinance on the Reporting of Unusual Transactions (NORUT), and related sanctions legislation.

3. Scope and Audience

This policy applies to all directors, officers, employees, contractors, agents, payment processors, and third-party vendors engaged in activities involving the Company’s gaming operations.

4. Definitions

- Money Laundering (ML): The process of concealing the origin of funds derived from criminal activities.
- Terrorist Financing (TF): The provision of funds to support terrorist activities.
- Customer Due Diligence (CDD): Identification, verification, and risk assessment of players and business partners.
- Politically Exposed Persons (PEP): Individuals entrusted with prominent public functions, including family and close associates.
- Financial Intelligence Unit (FIU): Curaçao’s national authority responsible for receiving and analyzing suspicious transaction reports.
- Business Risk Assessment (BRA): Internal risk evaluation of the Company’s products, services, and exposure to ML/TF.
- Customer Risk Assessment (CRA): Player-specific risk profiling used to determine CDD levels.



5. Policy Implementation

The Company adopts a risk-based approach to identify, assess, and mitigate ML/TF risks. Policies and controls are designed to comply with Curaçao regulatory requirements and industry standards.

5.1 Business Risk Assessment (BRA)

The Company conducts annual Business Risk Assessments to identify ML/TF threats and vulnerabilities related to its products, services, payment channels, jurisdictions, and customer base. The BRA is reviewed and approved by senior management and made available to the GCB upon request.

5.2 Customer Risk Assessment (CRA)

Customer-specific risk profiles are established at onboarding, assigning risk levels (low, medium, or high) based on nationality, PEP status, transaction volume, payment methods, and other relevant factors.

5.3 Customer Acceptance Policy (CAP)

Players are only accepted upon successful completion of CDD procedures. High-risk customers, including PEPs and players from high-risk jurisdictions, are subject to enhanced due diligence (EDD) measures.

5.4 Customer Due Diligence (CDD)

CDD is mandatory for:

- Transactions ≥ NAf. 4,000 (single or aggregated);
- Linked transactions cumulatively exceeding NAf. 4,000;
- Suspected ML/TF activity;
- High-risk profiles requiring enhanced screening.

CDD includes:

- Verification of player identity and beneficial ownership
- Screening against UN, EU, OFAC, and Curaçao sanctions lists
- Assessment of source of funds and source of wealth
- Ongoing monitoring for unusual transaction patterns.

5.5 Ongoing Monitoring

The Company continuously monitors player transactions, payment methods, and gaming activity to detect suspicious patterns. High-risk customers are subject to increased monitoring and periodic re-verification of identity.



5.6 Reliance on Third Parties

Where third-party KYC or payment providers are used, the Company ensures that these entities comply with equivalent Curaçao AML/CTF obligations and maintain auditable records.

5.7 Reporting of Unusual Transactions

The Company follows mandatory reporting obligations under NORUT. Transactions $\geq$ NAf. 5,000 or those flagged as suspicious must be reported to FIU Curaçao via the goAML portal without delay. Employees are prohibited from disclosing any reporting activity to customers (tipping-off' prohibition).

5.8 AML/CTF Compliance Program

The AML program includes:

- Appointment of a designated Compliance Officer
- Implementation of robust internal controls
- Employee training programs
- Independent AML audits
- Systematic policy updates to reflect regulatory changes.

6. Compliance and Consequences of Non-Compliance

Non-compliance with this policy may result in internal disciplinary action, financial penalties, license suspension, and potential criminal liability in accordance with Curaçao regulations.

7. Employee Training & Awareness

All employees must complete AML/CTF training at onboarding and annually thereafter. Training covers KYC obligations, detection of unusual transactions, and reporting procedures.

8. Record Keeping

In accordance with Curaçao law, the Company retains CDD records, transaction history, and reports for a minimum period of five (5) years from the end of the business relationship or from the date of the occasional transaction.

9. Related Policies & References

- National Ordinance on Identification when Rendering Services (NOIS)
- National Ordinance on Reporting Unusual Transactions (NORUT)
- Sanctions National Ordinance & Kingdom Sanctions Act
- Curaçao Gaming Control Board AML/CTF Guidelines (2025)



10. Contact Information

For inquiries regarding this policy, please contact:

Compliance Officer: Gonzalo Etchepare

Email: gonzalo@bz.com

Phone: +54 91158469708