

AML/CTF POLICY

KING ENTERPRISES N.V.

Approving Official: Director, King Enterprises N.V.

Responsible Office: Compliance Department

Effective Date: May 15, 2025

Next Review Date: May 01, 2026

1. Policy Statement

King Enterprises N.V. is fully committed to preventing money laundering, terrorist financing, and proliferation financing. This policy outlines the procedures and responsibilities in compliance with the applicable legislation of Curaçao and the guidance issued by the Curaçao Gaming Authority (CGA).

2. Purpose

This AML/CTF Policy serves to detect, deter, and prevent the use of King Enterprises N.V.'s services for financial crime. It ensures compliance with national laws (including the Penal Code, NOPML, NORUT, NOIS) and international standards (FATF).

3. Audience

This policy applies to:

- All employees of King Enterprises N.V.
- Contractors and third-party service providers with access to customer or transaction data.

4. Definitions

- ML/TF: Money Laundering / Terrorist Financing.
- CDD: Customer Due Diligence.
- EDD: Enhanced Due Diligence.
- STR: Suspicious Transaction Report.

- PEP: Politically Exposed Person.

5. Policy Implementation

5.1 Business Risk Assessment

A comprehensive ML/TF risk assessment is conducted at least annually, evaluating:

- Products and services (online poker platform).
- Delivery channels.
- Customer profiles and jurisdictions.
- Internal systems and controls.

5.2 Customer Risk Assessment

Each customer is assessed at onboarding. Risk profiles are based on:

- Geographic location.
- Occupation.
- Payment behavior.
- Account activity.

5.3 Customer Acceptance Policy

Customers are accepted based on their risk level:

- Low-risk: Simplified CDD.
- Medium-risk: Standard CDD.
- High-risk or PEPs: Enhanced CDD and senior management approval.

5.4 Customer Due Diligence

CDD includes:

- Identity verification (passport, ID, utility bill).
- Age verification (18+ only).
- PEP and sanctions screening.

- Source of funds for large or unusual transactions.

5.5 Ongoing Monitoring

Ongoing monitoring includes:

- Monitoring transactions for anomalies.
- Periodic refresh of KYC data.
- Flagging unusual activity based on customer profile.

5.6 Reliance on Third Parties

If KYC is performed by third parties (e.g., payment processors), written agreements are in place to ensure:

- Access to identification data.
- Compliance with Curaçao standards.

5.7 Reporting of Unusual Transactions

All employees are trained to identify and internally report suspicious activity. The Compliance Officer reviews and files STRs with the FIU as required.

5.8 AML Compliance Program

The program includes:

- Appointment of a dedicated Compliance Officer.
- Annual risk assessments.
- AML training for staff.
- Review and update of internal controls.

6. Compliance and Consequences of Non-Compliance

Non-compliance may result in:

- Disciplinary action (including termination)..
- Regulatory penalties.
- Reputational damage.

7. Related Information

- Penal Code of Curaçao
- NOPML, NORUT, NOIS
- FATF Recommendations
- CGA AML Guidelines (2024)

8. Contact Information

Compliance Department

Email: info@kingenterprisesnv.com

9. Policy History

- Version 1.0: October 2024 (internal policy draft)
- Version 2.0: May 2025 (restructured to align with CGA Template)

10. Policy URL

The policy is not currently available on a website.