

HNA GAMING N.V – ANTI-MONEY LAUNDERING (AML) POLICY

Version: 1.0

Effective Date: 07/10/2025

Next Review Date: 07/10/2026

Approving Official(s): Board of Directors, HNA Gaming N.V

Responsible Office: Compliance Department

Compliance Officer: Marco Ramunno

1. Policy Statement

At HNA Gaming N.V, we hold an unwavering commitment to the highest standards of ethics and integrity. We consider the prevention of money laundering and the combatting of terrorist financing as paramount responsibilities. Our dedication to full compliance with Curaçao's legal framework is steadfast.

This AML policy articulates our comprehensive approach to detecting and deterring money laundering and terrorist financing activities within our sphere of operations. It applies to **all employees, officers, management, and third parties** engaged in or on behalf of HNA Gaming N.V.

2. Purpose

The purpose of this policy is to ensure that HNA Gaming N.V operates in full compliance with Curaçao's anti-money laundering (AML) and counter-terrorism financing (CTF) requirements.

We aim to detect, prevent, and report any suspicious activities consistent with the following legislation and standards:

- *Landsverordening toezicht bank- en kredietwezen 1994*
- *Landsverordening melding ongebruikelijke transacties* (National Ordinance Reporting Unusual Transactions)
- *Landsverordening identificatie bij dienstverlening van financiële instellingen*

Additionally, we align with the **Financial Action Task Force (FATF)** recommendations and other international best practices to ensure integrity and transparency in our business operations.

3. Audience

This policy applies to:

- All employees, officers, and directors of HNA Gaming N.V
- Contractors and consultants engaged by HNA Gaming N.V
- Third-party service providers and vendors with access to company systems or customer information

All parties must understand and comply with this policy's requirements and cooperate fully in AML/CTF matters.

4. Definitions

AML: Anti-Money Laundering

CTF: Counter Terrorist Financing

CDD: Customer Due Diligence

EDD: Enhanced Due Diligence

SDD: Simplified Due Diligence

KYC: Know Your Customer

PEP: Politically Exposed Person

FIU: Financial Intelligence Unit of Curaçao

Suspicious Transaction: Any transaction that appears inconsistent with a customer's known legitimate business or personal activities.

5. Policy Implementation

5.1 Business Risk Assessment

HNA Gaming N.V applies a **risk-based approach** to all operations. The organization periodically conducts comprehensive risk assessments to identify, assess, and mitigate money laundering and terrorist financing risks.

The business risk assessment considers:

- Nature of products and services offered
- Geographic exposure
- Transaction volume and complexity
- Customer types and distribution channels

Internal controls and monitoring systems are designed to mitigate these risks, ensuring compliance with national and international AML standards.

5.2 Customer Risk Assessment

Customer risk assessments (CRA) are conducted during the establishment of every business relationship.

Each customer is categorized as **low, medium, or high risk** based on:

- Source of funds and wealth
- Geographic risk
- Business activities
- Transaction history
- PEP or sanctions exposure

The CRA determines whether **SDD, CDD, or EDD** is applied. Assessments are reviewed periodically or when customer circumstances change.

5.3 Customer Acceptance Policy

HNA Gaming N.V.'s **Customer Acceptance Policy (CAP)** ensures that only clients with verifiable identities and legitimate sources of funds are accepted.

Key principles:

- Full KYC verification prior to account activation
- Refusal to establish business with anonymous or fictitious persons
- Mandatory EDD for PEPs or high-risk customers
- Sanctions screening at onboarding and continuously thereafter

The CAP is implemented with strict adherence to Curaçao AML/CTF laws and international sanctions regulations.

5.4 Customer Due Diligence

Our AML framework integrates comprehensive **KYC and CDD** procedures:

- Verification of customer identities using valid, government-issued documents
- Collection and assessment of relevant personal and financial data
- Risk-based transaction monitoring

- Ongoing verification and documentation retention

For **PEPs and high-risk customers, Enhanced Due Diligence (EDD)** applies, including:

- Verification of source of funds and wealth
- Sanction and watchlist screening
- Continuous monitoring and reassessment

Funds suspected to be linked to criminal activity may be **frozen** pending further investigation and reported immediately to the **Curaçao FIU**.

5.5 Ongoing Monitoring

Continuous monitoring ensures the detection of unusual transactions or deviations from expected customer behavior.

This includes:

- Transaction pattern analysis
- Review of account activity
- Screening updates for PEPs and sanctions
- Alerts and escalation procedures for suspicious transactions

Monitoring frequency is proportionate to customer risk level.

5.6 Reliance on Third Parties for CDD

HNA Gaming N.V may rely on third-party service providers for certain elements of customer due diligence under strict oversight.

Before such reliance, we:

- Assess the third party's AML/CTF capabilities and reputation
- Enter into formal agreements defining data-sharing and compliance responsibilities
- Retain ultimate responsibility for compliance with Curaçao AML regulations

Regular audits and reviews ensure continued adherence by third parties.

5.7 Reporting of Unusual Transactions

All employees are obligated to identify and report unusual or suspicious transactions.

Procedures:

- Employees report suspicions directly to the AML Compliance Officer
- The Compliance Officer investigates and, if warranted, files a **Suspicious Transaction Report (STR)** to the **FIU Curaçao** promptly
- Reports are maintained confidentially and logged for at least **five years**

Internal and external reporting timelines strictly adhere to Curaçao's legal requirements.

5.8 Anti-Money Laundering Compliance Program

Our **AML Compliance Program** establishes a structured, risk-based approach for mitigating ML/TF risks.

Key components include:

- Appointment of an **AML Compliance Officer**
- Regular employee training and awareness programs
- Written AML procedures for CDD, EDD, transaction monitoring, and record keeping
- Procedures for blocking or freezing accounts suspected of money laundering
- Periodic review and testing of internal controls

The Compliance Program is reviewed annually and updated to reflect evolving regulatory requirements.

6. Compliance and Consequences of Non-Compliance

Non-compliance with this policy or Curaçao AML laws can lead to:

- Internal disciplinary action, including termination
- Regulatory penalties or license revocation
- Civil and criminal prosecution

All employees must promptly report any suspected violations. Management enforces a zero-tolerance stance toward willful non-compliance.

7. Related Information

This policy should be read alongside the following documents and frameworks:

- Curaçao AML/KYC legal framework
- FATF Recommendations
- FIU Curaçao reporting guidelines
- Internal HNA Gaming N.V procedures for AML monitoring and reporting
- Code of Ethics and Conduct

8. Contact Information

Compliance Officer:

Marco Ramunno

HNA Gaming N.V – Compliance Department

 Email: compliance@hnagaming.com

 Phone: +35699290679

9. Policy History

- **Version 2.0 – 07/10/2025:** Initial release of the comprehensive AML Policy, aligning with Curaçao AML/CTF legislation and FATF recommendations.
- Future revisions will be documented here with respective dates and summaries.

10. Policy URL (if applicable)

This policy is accessible via the HNA Gaming N.V corporate website under:

[Insert exact URL – e.g., <https://www.hnagaming.com/compliance/aml-policy>]