

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

Approving Official(s):

Board of Directors and Senior Management

Responsible Office:

Compliance Department

1. Policy Statement

This Anti-Money Laundering (AML) and Counter-Terrorist Financing (CTF) Policy outlines the commitment of **Bet Boom N.V.** to comply with all applicable laws and regulations to prevent money laundering, terrorist financing, and the proliferation of weapons of mass destruction. This policy applies to all employees, contractors, and third-party service providers involved in the operations of our land-based and online casinos in Curacao.

The policy shall state the casino's intention to comply with current anti-money laundering and terrorist financing legislation as well as provisions and guidelines, in particular the laws and guidelines regarding customer due diligence and the reporting of unusual transactions, i.e. the NOIS and the NORUT.

2. Purpose

The purpose of this policy is to:

- 2.1. Ensure compliance with the Curaçao Gaming Control Board (GCB) Regulations, the National Ordinance on Identification when Rendering Services (NOIS), the National Ordinance on the Reporting of Unusual Transactions (NORUT), the Sanctions National Ordinance, and the Kingdom Sanction Act.
- 2.2. Mitigate the risks of money laundering (ML), terrorist financing (TF), and financing of proliferation (FP).
- 2.3. Establish internal controls, procedures, and training programs to detect and report suspicious activities.

3. Audience

This policy applies to:

- 3.1. All employees, including management, dealers, cashiers, and customer service representatives.
- 3.2. Contractors and third-party service providers involved in customer due diligence (CDD) or transaction monitoring.

4. Definitions

The following terms are used in this AML/CTF Policy with the meanings specified below:

- 4.1. **Beneficial Owner (Ultimate Beneficial Owner – UBO).** A natural person(s) who ultimately owns or controls a customer and/or the person on whose behalf a transaction is conducted. This includes individuals who exercise ultimate effective control over a legal entity.
- 4.2. **Business Risk Assessment (BRA).** An evaluation conducted by the casino to identify and assess the risks of money laundering (ML), terrorist financing (TF), and financing of proliferation (FP) associated with its operations, products, services, and customers.
- 4.3. **Casino.** Refers to both land-based and online casinos, including providers of sports betting, e-sports betting, fantasy sports, lottery, bingo, skill-based games, and virtual sports.

- 4.4. **CFATF (Caribbean Financial Action Task Force).** An organization of 24 Caribbean, Central, and South American states committed to implementing measures to combat money laundering and terrorist financing.
- 4.5. **Compliance Officer.** A senior management-level officer responsible for overseeing the casino's AML/CTF program, ensuring compliance with regulations, and reporting unusual transactions.
- 4.6. **Customer Due Diligence (CDD).** The process of identifying and verifying a customer's identity, assessing their risk profile, and monitoring transactions to detect suspicious activity.
- 4.7. **Customer Risk Assessment (CRA).** An evaluation of the ML/TF risks posed by a specific customer based on factors such as their background, transaction behavior, and geographic location.
- 4.8. **Enhanced Due Diligence (EDD).** Additional verification measures applied to high-risk customers, such as politically exposed persons (PEPs) or customers from high-risk jurisdictions.
- 4.9. **FATF (Financial Action Task Force).** An intergovernmental body that sets international standards for combating money laundering, terrorist financing, and proliferation financing.
- 4.10. **FATF Recommendations.** A global framework of policies and measures to combat financial crimes, adopted by FATF member jurisdictions.
- 4.11. **Financial Intelligence Unit (FIU).** The Curaçao FIU is the authority responsible for receiving, analyzing, and disseminating reports of unusual or suspicious transactions.
- 4.12. **Financial Transaction.** In land-based casinos, this includes:
- Purchasing or cashing in chips/tokens
 - Opening accounts
 - Wire transfers
 - Currency exchanges
 - In online casinos, this refers to deposits and withdrawals (excluding bonuses, wagers, and winnings).
- 4.13. **Kingdom Sanction Act.** "The Rijkssanctiewet" (N.G. 2016, no. 54), implementing international sanctions within the Kingdom of the Netherlands.
- 4.14. **Layering (Money Laundering Stage).** The process of moving illicit funds through multiple transactions to obscure their origin.
- 4.15. **Money Laundering (ML).** The process of disguising illegally obtained funds to make them appear legitimate. It involves three stages:
- Placement – Introducing illicit funds into the financial system.
 - Layering – Concealing the source through complex transactions.
 - Integration – Reintroducing "cleaned" funds into the economy.
- 4.16. **National Ordinance on Identification when Rendering Services (NOIS).** "The Landsverordening identificatie bij dienstverlening" (N.G. 2017, no. 92), requiring customer identification in financial transactions.
- 4.17. **National Ordinance on the Reporting of Unusual Transactions (NORUT).** "The Landsverordening Melding Ongebruikelijke Transacties" (N.G. 2017, no. 99), mandating the reporting of suspicious transactions to the FIU.
- 4.18. **Ongoing Monitoring.** The continuous review of customer transactions to ensure consistency with their risk profile and detect unusual activity.
- 4.19. **Politically Exposed Person (PEP).** An individual who is or has been entrusted with a prominent public function, including:
- Foreign PEPs: Heads of state, senior politicians, military officials.
 - Domestic PEPs: High-ranking local government officials.
 - International Organization PEPs: Senior executives of entities like the UN or EU.
- 4.20. **Sanctions National Ordinance.** The "Sanctielandsverordening" (N.G. 2014, no. 55), enforcing international sanctions in Curaçao.

- 4.21. **Simplified Due Diligence (SDD).** Reduced verification measures applied to low-risk customers, such as those with small transaction volumes.
- 4.22. **Source of Funds (SoF).** The origin of funds used in a specific transaction (e.g., salary, inheritance, gambling winnings).
- 4.23. **Source of Wealth (SoW).** The origin of a customer's total accumulated wealth (e.g., business income, investments).
- 4.24. **Targeted Financial Sanctions (TFS).** Measures requiring the freezing of assets belonging to designated persons or entities (e.g., terrorists, sanctioned regimes).
- 4.25. **Terrorist Financing (TF).** Providing funds for terrorist acts, organizations, or individuals, regardless of whether the funds are legally or illegally obtained.

5. Policy Implementation

5.1. Business Risk Assessment (BRA)

The company will conduct a comprehensive Business Risk Assessment on an annual basis to identify, assess, and document potential money laundering (ML), terrorist financing (TF), and proliferation financing (PF) risks associated with its products, services, customers, and geographic locations. This assessment will evaluate risk factors including customer types, transaction methods, delivery channels, and technological developments. The methodology, risk scoring criteria, and mitigation strategies will be clearly documented and approved by senior management. The Business Risk Assessment will be updated whenever new products are launched, new markets are entered, or significant regulatory changes occur. Special consideration will be given to high-risk indicators such as cash transactions, anonymous payment methods, and politically exposed persons. The completed assessment will be made available to the Curaçao Gaming Control Board upon request.

5.2. Customer Risk Assessment (CRA)

Prior to establishing any business relationship or conducting occasional transactions, the company will perform a thorough Customer Risk Assessment to evaluate the specific ML/TF/PF risks posed by each customer. This assessment will consider factors including the customer's background, source of wealth, geographic location, and intended account activity. Customers will be categorized into low, medium, or high-risk profiles based on this evaluation. High-risk customers, including politically exposed persons and those from high-risk jurisdictions, will be subject to enhanced due diligence measures. The Customer Risk Assessment will be reviewed and updated throughout the business relationship as new information becomes available or when customer behavior changes significantly.

5.3. Customer Acceptance Policy (CAP)

The company maintains a formal Customer Acceptance Policy that establishes clear criteria for onboarding customers and defines circumstances under which business relationships may be declined. This policy prohibits anonymous accounts or accounts in obviously fictitious names. All potential customers will be screened against international sanctions lists (including United Nations and European Union lists) and local designated lists before being accepted. The policy specifically identifies types of customers that may pose higher-than-average ML/TF risks and outlines appropriate risk mitigation measures. The Customer Acceptance Policy requires senior management approval for establishing relationships with high-risk customers and provides guidance for situations where customer identification cannot be properly verified.

5.4. Customer Due Diligence (CDD)

The company implements robust Customer Due Diligence procedures that include:

- a. Collecting and verifying the customer's full legal name, permanent residential address, date of birth, place of birth, nationality, and official identification number;

- b. Identifying and verifying beneficial owners of corporate accounts;
- c. Understanding the purpose and intended nature of the business relationship;
- d. Conducting ongoing monitoring of transactions.

Ongoing monitoring will ensure customer information remains current and transactions align with expected behavior patterns.

5.5. Ongoing Monitoring

The company maintains continuous monitoring systems to scrutinize customer transactions and ensure they remain consistent with established customer profiles and expected behavior patterns. This monitoring includes:

- a. Tracking transaction patterns and volumes;
- b. Identifying unusual or suspicious activity such as large deposits followed by minimal play;
- c. Verifying that source of funds information remains current and appropriate;
- d. Updating customer risk ratings based on new information.

Any transactions that appear inconsistent with a customer's profile will be investigated, and where appropriate, reported to the Curaçao Financial Intelligence Unit. The intensity of monitoring corresponds to each customer's risk rating, with high-risk customers subject to more frequent and detailed reviews.

5.6. Reliance on Third Parties

When relying on third parties to perform elements of Customer Due Diligence, the company will:

- a. Ensure the third party is properly regulated and subject to equivalent AML/CFT requirements;
- b. Obtain immediate access to all customer identification and verification data;
- c. Establish written agreements guaranteeing the third party will provide copies of identification documents upon request;
- d. Periodically test the arrangement to confirm its effectiveness.

The company retains ultimate responsibility for compliance with all Customer Due Diligence requirements and will conduct regular reviews of third-party performance. No reliance will be placed on third parties for ongoing monitoring or suspicious transaction reporting obligations.

5.7. Reporting Unusual Transactions.

The company will promptly report to the Curaçao Financial Intelligence Unit. Each report about an unusual transaction will include at least the following information:

- a. The identity of the client;
- b. Nature and number of the identification document of the client;
- c. The nature, date, time and place of transaction;
- d. The amount, destination and origin of the funds, securities, precious metals, or other values
- e. Involved in the transaction;
- f. The circumstances that identified the transaction as unusual.

Reports will be submitted through the special portal and include all relevant details and supporting documentation. Internal procedures ensure that reports are properly documented and that customers are not "tipped off" about suspicious activity reports. All reporting records will be maintained for at least five years.

5.8. AML Compliance Program

The company's comprehensive AML Compliance Program includes:

- a. Appointment of a qualified Compliance Officer with day-to-day oversight responsibilities;
- b. Development and maintenance of written policies and procedures;
- c. Regular employee training programs tailored to different roles and responsibilities;
- d. An independent audit function to test the program's effectiveness annually.

The Compliance Officer has authority to access all necessary records and reports directly to senior management. Training programs cover AML fundamentals, red flag indicators, reporting obligations, and recent trends in financial crime. Audit results are reviewed by the Board of Directors, with deficiencies promptly addressed through corrective action plans.

6. Compliance and Consequences of Non-Compliance

Violations of this policy may result in disciplinary action, legal penalties, or license revocation. Employees must report suspicious activity without tipping off customers, and failure to comply with reporting obligations may be considered a breach of regulatory requirements. The company will take appropriate action against any employee who willfully disregards AML/CFT obligations.

7. Related Information

This policy implements requirements under the NOIS (N.G. 2017 no. 92), NORUT (N.G. 2017 no. 99), Sanctions National Ordinance (N.G. 2014 no. 55), and Kingdom Sanction Act (N.G. 2016 no. 54). Reference materials include FATF Recommendations and CGA AML Regulations (January 2025).

8. Contact Information

For questions regarding this policy, contact: Zurab Kvaratskhelia.

Mobile phone: +995597742273

9. Policy History

This version implemented April 10, 2025.



(SMES)
Solutions for Management
and Employment Support N.V.