

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

Key Information

Company: Half Space Entertainment N.V.

Approving Official: Director Starkeast Management B.V.

Responsible Office: Compliance Department

Effective Date: 30 June 2025

Next Review Date: 29 June 2026

1. Introduction

<https://letsbamble.com/> is operated by Half Space Entertainment N.V., a limited liability company registered in Curacao with company registration number 166129 (0), with a registered address at Kaya W.F.G. (Jombi) Mensing 24 Unit A Curacao (“Company”), licensed in Curacao under Curacao laws and regulations.

Half Space Entertainment N.V. (the “Company” or the “Operator”) is fully committed to preventing the use of its services for money laundering, terrorist financing, and other forms of financial crime.

We implement strict Anti-Money Laundering (AML) and Counter-Terrorist Financing (CTF) measures and require full compliance with the standards set forth in this Policy by all members of management and employees.

This Policy applies to all transactions conducted through our website <https://letsbamble.com/> and constitutes an integral part of our internal control framework.

2. Purpose

The purpose of this Policy is to establish a common framework and minimum standards for identifying, preventing, and reporting any suspicious activities related to money laundering and terrorist financing.

The Policy is designed to ensure the Operator’s compliance with:

- Curaçao legislation, including but not limited to:
 - the National Ordinance on Identification when Providing Services (NOIS);
 - the National Ordinance on the Reporting of Unusual Transactions (NORUT);
 - Landsverordening op de kansspelen (LOK);
 - Sanctions National Ordinance;

- The Kingdom Sanction Act.
- License conditions issued by the Curaçao Gaming Authority (CGA);
- International standards, including recommendations of the Financial Action Task Force (FATF).

3. Audience

This Policy is mandatory for all employees, managers, directors, and business partners of the Company who are directly or indirectly involved in customer transaction processing, verification procedures, or compliance oversight.

All relevant staff are required to familiarize themselves with this Policy and complete mandatory AML/CTF training.

4. Definitions

For the purposes of this Policy, the following terms shall have the meanings ascribed below:

AML (Anti-Money Laundering): a set of measures aimed at preventing the financial system from being used to legitimize proceeds of crime.

AMLCO (Anti-Money Laundering Compliance Officer): the designated compliance officer responsible for overseeing the implementation and enforcement of this Policy.

CDD (Customer Due Diligence): the process of collecting and verifying customer identification data to assess associated risks.

CGA (Curaçao Gaming Authority): the regulatory authority overseeing gaming operations in Curaçao.

CTF (Counter-Terrorist Financing): measures aimed at preventing and disrupting the funding of terrorist activities.

EDD (Enhanced Due Diligence): additional verification measures applied to high-risk customers.

FATF (Financial Action Task Force): an intergovernmental organization that sets international AML/CTF standards.

FIU (Financial Intelligence Unit): the national authority for receiving and analyzing suspicious transaction reports (in Curaçao — FIU Curaçao).

KYC (Know Your Customer): the obligation of financial institutions to identify and verify their customers.

Money Laundering: the process of concealing the illicit origin of funds, including:

- converting or transferring property known to be derived from criminal activity;

- concealing or disguising the true nature, source, location, disposition, or ownership of property;
- acquiring, possessing, or using such property.

PEP (Politically Exposed Person): An individual who holds or has held a prominent public position.

SDD (Simplified Due Diligence): minimal verification measures applied to low-risk customers under certain conditions.

SOW (Source of Wealth): information on how a customer accumulated their overall wealth.

SOF (Source of Funds): information on the origin of the specific funds used in a transaction.

Suspicious Transaction: a transaction that, by its nature or circumstances, raises reasonable grounds to suspect a link to money laundering or terrorist financing.

4. Organization of the AML for <https://letsbamble.com/>

Following the AML legislation, <https://letsbamble.com/> has appointed the “highest level” for the prevention of ML: The entire management of Half Space Entertainment N.V. is in charge.

Furthermore, an AMLCO (Anti Money Laundering Compliance Officer) is in charge of the enforcement of the AML policy and procedures within the System.

The AMLCO is placed under the direct responsibility of the general management.

5. AML policy changes and implementation requirements

Each significant change of <https://letsbamble.com/> AML policy is subject to approval by the general management of Half Space Entertainment N.V. and the Anti-money laundering compliance officer.

6. Policy implementation

The Operator implements a multi-layered control system to identify and mitigate the risks of money laundering and terrorist financing. This system is managed by the AMLCO, who is accountable to the Company's senior management.

6.1. Business risk assessment

The Operator has conducted and regularly reviews (at least annually) an Enterprise-Wide Risk Assessment (EWRA) to identify and analyze the AML/CTF risks to which its business is exposed. The EWRA considers the following key factors:

- **Products and Services:** risks associated with the games and payment options offered.
- **Customer Base:** geographic and behavioral risks associated with our players.
- **Delivery Channels:** risks inherent to the online platform.
- **Geographic Risks:** risks associated with the countries from which our customers and their transactions originate.

The findings of the EWRA form the basis for developing and calibrating all procedures described in this Policy.

6.2. Customer risk assessment

The Operator applies a risk-based approach by assigning each customer a risk level (Low, Medium, High) based on the following criteria:

- **Geographic Risk:** the customer's country of residence and its status on FATF lists or other international watchlists.
- **Behavioral Risk:** the nature of transactions, frequency and volume of wagers, and use of various payment methods.
- **Other Factors:** PEP status, presence on sanctions lists, and changes to personal information.

Based on this risk assessment, the appropriate level of due diligence (SDD, CDD, EDD) is applied to the customer.

Country categorization:

- **Low risk:** countries with robust AML/CTF systems that are not included on any restrictive lists.
- **Medium risk:** countries identified as having certain deficiencies in their AML/CTF regulation. Customers from these countries are subject to lower thresholds for enhanced verification.
- **High risk (prohibited jurisdictions):** the Operator does not accept customers from countries that are:
 - Included on the FATF "black" or "grey" lists.

- Under international sanctions.
- Designated as prohibited by the Company's internal decision (see Section 6.3).

6.3. Customer acceptance policy

The Operator will not enter into business relationships with or conduct transactions for individuals from the following jurisdictions (Restricted Countries):

- USA;
- Curacao;
- Netherlands;
- Aruba;
- Sint Maarten;
- All countries on the FATF "blacklist" (Myanmar, North Korea, Iran);
- UN sanctioned: Central African Republic, Democratic Republic of Congo, Eritrea, Guinea-Bissau, Iran, Iraq, Lebanon, Libya, Mali, North Korea, Somalia, South Sudan, Sudan, Yemen;
- Any other jurisdictions under UN, EU, or OFAC sanctions.

This list of restricted jurisdictions is reviewed and updated regularly.

6.4. Customer Due Diligence (CDD)

The Operator implements a tiered customer verification system based on risk. All verification procedures are designed to be clear, robust, and compliant with regulatory standards.

(a) Simplified Due Diligence (SDD):

Applied upon registration. The customer must provide basic personal information, including full name, date of birth, country of residence, and full address. This information is mandatory for account creation.

(b) Customer Due Diligence (CDD):

Standard verification is mandatory for all customers who reach a cumulative deposit or withdrawal threshold of NAF 4,000 (or its equivalent in another currency), or upon any withdrawal request if deemed necessary. The CDD process requires the submission of documents as detailed in section 6.4.1 below.

(c) Enhanced Due Diligence (EDD):

Applied to customers who reach a cumulative deposit or withdrawal threshold of **EUR 5,000**,

(or its equivalent in another currency) or who are identified as high-risk (e.g., PEPs). EDD includes all CDD requirements, plus a formal inquiry into the customer's **Source of Funds (SOF) and Source of Wealth (SOW)**, as detailed in section 6.4.1.

Account restrictions: Until the required verification procedure (CDD or EDD) is completed, all withdrawal requests and the ability to make further deposits will be suspended.

6.4.1. Document requirements and verification standards

To complete the CDD or EDD process, customers must submit the following documents, which must meet the specified standards.

Proof of Identity (POI):

- **Accepted Documents:** A clear, color copy of a valid government-issued Passport, National ID card, or Driving License.
- **Submission Standards:**
 - All four corners of the document must be clearly visible.
 - The document must be fully legible, with no blur or glare.
 - The document must not be expired and should be valid for at least three (3) months from the date of submission.
 - The customer's full name, date of birth, and photograph must match the details provided during registration.

Proof of Address (POA):

- **Accepted Documents:** A full copy of a recent (issued within the last three months) utility bill (e.g., electricity, water, gas), bank statement, or an official government-issued document confirming the customer's residential address.
- **Submission Standards:**
 - The document must clearly show the customer's full name and current residential address.
 - The name of the issuing institution and the date of issue must be clearly visible.
 - All four corners of the document must be visible.

"Selfie" with Identity Document and Note:

- **Submission Standards:** A high-resolution photograph of the customer:
 - Clearly showing their face, without hats or sunglasses.
 - Holding their Proof of Identity document open next to their face.
 - Holding a handwritten note that displays a unique, randomly generated code provided by the Operator during the submission process.
 - The details on the ID document in the selfie must be legible.

Source of Funds/Wealth (for EDD):

- **Purpose:** To understand the origin of the customer's funds and overall wealth to ensure it is legitimate.
- **Examples of Accepted Documents:**
 - **Employment:** Recent payslips or an employment contract.
 - **Business Ownership:** Company registration documents, recent financial statements.
 - **Sale of Assets:** A notarized sales agreement for property or other assets.
 - **Inheritance/Gift:** A will, testament, or a notarized gift deed.
 - **Investments:** A portfolio statement from a reputable financial institution.

Verification process:

The Operator will verify the submitted documents using both manual checks by trained compliance staff and, where applicable, third-party electronic verification services. The Operator reserves the right to request additional information or notarized documents if the initial submission is deemed insufficient.

6.5. Ongoing monitoring

The Operator conducts ongoing monitoring of customer transactions and activity to detect unusual or suspicious behavior. This monitoring includes:

- **Automated monitoring:** Systems track transactions for threshold breaches, uncharacteristic behavior (e.g., deposits without gaming activity), use of different IP addresses, and various payment methods.
- **Manual reviews:** Compliance department staff regularly review system-generated alerts and conduct account reviews, especially for high-risk customers.
- **Sanctions and PEP screening:** The customer base is regularly screened against updated international sanctions lists and lists of Politically Exposed Persons.

6.6. Reliance on third parties

The Operator partners only with reputable and licensed Payment Service Providers (PSPs) that have their own effective AML/CTF policies. This serves as a first line of defense against suspicious funds entering the platform. However, the ultimate responsibility for fulfilling CDD requirements always remains with the Operator.

6.7. Reporting of unusual transactions

Any employee who detects a transaction that raises suspicion of money laundering or terrorist financing must immediately report it to their supervisor and the AMLCO.

In accordance with the National Ordinance on the Reporting of Unusual Transactions (NORUT) and its associated decrees, the following transactions or intended transactions are deemed unusual or suspicious and must be reported:

- Transactions which, in connection with money laundering or terrorism financing, are reported to the Police or to the Department of Justice.
- Transactions by or on behalf of a natural or legal person, a group, or an entity, who is named on a list adopted by virtue of the Sanctions National Ordinance (N.G. 2014 no. 55).
- Transactions in the amount of NAF 5,000 or more (or its currency equivalent), regardless of whether the transaction is made in cash, by check, or through electronic or other non-physical means. The NAF 5,000 threshold does not only apply to single transactions. It also applies to a series, combination, or pattern of transactions involving a total amount that meets or exceeds this limit and is considered per gaming day. This rule is designed to prevent structuring (smurfing).
- In addition to the automatic criteria above, any transaction (regardless of the amount) must be reported if it appears suspicious. Examples include depositing and withdrawing with little to no gameplay, reluctance to provide CDD documents, use of third-party accounts, etc.

The AMLCO will conduct an internal investigation. If the suspicion is substantiated, the AMLCO, in accordance with the requirements of the NORUT, will decide whether to file a Suspicious Transaction Report (STR) with FIU Curaçao.

The filing of an STR with the FIU is confidential. Employees are strictly prohibited from "tipping-off" the customer that a report has been or will be filed.

6.8. Anti-Money Laundering Compliance Program

6.8.1 Appointment and responsibilities of the AML compliance officer

The Company appointed a senior officer at management level, independent of gaming or operational functions, to serve as the Anti-Money Laundering Compliance Officer (“AML Compliance Officer”).

The AML Compliance Officer vested with adequate authority, autonomy, resources, and unrestricted, timely access to all relevant information, including customer due diligence (CDD) records and transaction data, necessary for the effective discharge of their duties.

The responsibilities of the AML Compliance Officer shall include, but are not limited to, the following:

- Designing, implementing, and maintaining the Company’s AML/CFT compliance program;
- Ensuring the Company’s ongoing compliance with applicable AML/CFT laws, regulations, and internal policies and procedures;
- Monitoring and analyzing customer activity and transactions to detect, investigate, and report suspicious activity to the Financial Intelligence Unit (FIU) in a timely manner;
- Serving as the central point of contact for internal reporting of suspicious activities and ensuring confidentiality of such reports;
- Maintaining comprehensive records of all internal reports and external filings related to suspicious transactions;
- Developing, delivering, and overseeing AML/CFT training programs for all relevant staff;
- Monitoring legal and regulatory developments in AML/CFT and updating the Company’s program and procedures accordingly;
- Preparing and submitting regular AML compliance reports to senior management and the Board of Directors;
- Establishing and maintaining internal procedures for the freezing or blocking of accounts pursuant to legal requirements, while ensuring measures are in place to mitigate the risk of tipping-off.

6.8.2 System of internal policies, procedures, and controls

The Company establishes and maintains a comprehensive system of internal policies, procedures, and controls to ensure effective implementation of its Anti-Money Laundering and Countering the Financing of Terrorism (AML/CFT) obligations.

This AML Policy, together with all supporting operational procedures, forms the foundation of the Company's internal control framework for AML/CFT compliance.

All policies and procedures:

- Documented in writing;
- Reviewed and approved by the Board of Directors or senior management;
- Communicated clearly and effectively to all relevant employees.

The internal controls shall be designed to operationalize AML/CFT policy into effective daily practices and shall cover, at a minimum, the following areas:

- Customer Due Diligence (CDD) and ongoing monitoring;
- Risk assessment and risk-based approach to customer and transaction evaluation;
- Identification, investigation, and reporting of suspicious transactions to the Financial Intelligence Unit (FIU);
- Record-keeping and data retention procedures in accordance with legal and regulatory requirements.

These internal controls shall be subject to periodic review and update to ensure ongoing effectiveness and alignment with evolving legal, regulatory, and business requirements.

6.8.3 Independent Audit Function

The Company ensures that its Anti-Money Laundering and Countering the Financing of Terrorism (AML/CFT) Compliance Program is subject to an independent audit at least annually to assess its adequacy and effectiveness.

The audit may be conducted by either:

- A qualified internal audit department that is independent of the AML compliance function; or
- An external auditor with relevant expertise.

The appointed auditor must possess appropriate qualifications and must not be involved in the day-to-day operations of the Company's AML/CFT compliance activities.

The scope of the audit shall include, at a minimum, the following areas:

- Assessment of the adequacy and completeness of written AML/CFT policies, procedures, and internal controls;
- Evaluation of the Company's compliance with applicable AML/CFT laws, regulations, and industry standards;
- Review of the effectiveness of Customer Due Diligence (CDD) procedures and customer risk assessment processes, including sampling of customer files;
- Review of the AML/CFT training program to ensure adequacy, relevance, and effectiveness;
- Transaction testing to evaluate the system's capacity to detect, monitor, and escalate unusual or suspicious activity;
- Assessment of the accuracy and timeliness of suspicious transaction reporting to the Financial Intelligence Unit (FIU);
- Evaluation of the Company's record-keeping practices in accordance with legal and regulatory requirements.

Upon completion of the audit, a written report detailing the findings, identified deficiencies, and recommendations for corrective action shall be submitted to senior management and the Board of Directors. Management responsible for implementing corrective measures in a timely manner to address any identified weaknesses.

7. Compliance and Consequences of Non-Compliance

Adherence to this Policy is a mandatory condition for all individuals falling under its scope (as defined in Section 3). Any violation of this Policy will be treated as a serious offense and may result in disciplinary action, up to and including termination of employment. Furthermore, non-compliance with AML/CTF requirements can lead to severe legal consequences for the Company, including substantial fines, license revocation, and criminal liability for the individuals involved.

8. Record keeping

The Operator shall ensure the secure and confidential storage of all data and documents obtained during customer due diligence procedures (CDD/EDD), as well as records of all transactions.

All identification data, files, and business correspondence with customers shall be retained for a period of five (5) years after the termination of the business relationship. Transaction records shall be retained for five (5) years from the date the transaction was completed.

Records shall be stored in a manner that allows for their timely retrieval upon request by the CGA, FIU, or other competent authorities.

Strict security measures are applied to protect data from unauthorized access, in accordance with applicable data protection laws.

9. Training

The Operator recognizes that a comprehensive and ongoing training program is a fundamental component of its Anti-Money Laundering and Countering the Financing of Terrorism (AML/CFT) framework. The training program is designed to ensure that all relevant personnel—ranging from front-line employees to senior management—are fully aware of the risks associated with money laundering and terrorist financing (ML/TF), understand their legal and regulatory obligations, and are equipped to effectively fulfill their role-specific responsibilities in preventing and detecting financial crime.

9.1 Training Objectives

The primary objectives of the Operator's AML/CFT training program are to:

- Ensure all employees understand their personal and corporate responsibilities under Curaçao's AML/CFT legislation and regulatory framework;
- Develop employees' ability to identify and appropriately handle transactions that may be indicative of money laundering or terrorist financing ("red flags");
- Ensure familiarity with the Operator's internal AML/CFT policies, procedures, and control measures;
- Establish clear and effective processes for the internal escalation and reporting of suspicious activity to the AML Compliance Officer (AMLCO);
- Protect the Operator from legal, regulatory, and reputational risks arising from AML/CFT non-compliance.

9.2 Target Audience and Role-Specific Content

The AML/CFT training program shall be tailored to the specific roles and responsibilities of employees as follows:

a) All new employees

All new hires undergo mandatory foundational AML/CFT training during onboarding, covering the nature and risks of ML/TF, the Operator's compliance commitment, internal

policies, customer due diligence (CDD) obligations, and procedures for reporting unusual transactions.

b) Front-line Staff (e.g., Customer Support, Payments/Finance, VIP Managers)

These employees shall receive detailed, practical training on:

- ML/TF typologies relevant to the online gambling sector;
- Identification of objective and subjective indicators of suspicious transactions;
- Handling customer inquiries related to CDD;
- Internal reporting procedures, including the obligation to avoid “tipping off” customers.

c) AMLCO and Compliance Staff

Compliance personnel, including the AMLCO, shall receive advanced, ongoing training, including participation in external seminars, webinars, and conferences. Training address evolving ML/TF typologies, legal/regulatory updates, and best practices in AML/CFT compliance.

d) Supervisors and Managers

Managers receive enhanced training covering all aspects of the Operator’s AML/CFT policies to ensure effective team supervision and enforcement of compliance.

e) Senior Management and the Board of Directors

Senior leadership and the Board regularly briefed on ML/TF risks, regulatory developments, and the status and effectiveness of the Operator’s AML/CFT compliance program.

9.3 Training Frequency

Initial training: mandatory prior to an employee’s engagement in customer-facing or transaction-handling activities.

Annual refresher training: required for all relevant staff at least once per calendar year. This reinforces core AML/CFT principles and provides updates on new ML/TF trends, regulatory changes, and internal policy revisions.

Ad-hoc training: provided as necessary in response to significant events, such as major regulatory changes, new product launches, or identification of emerging ML/TF risks.

9.4 Record-Keeping and Effectiveness Measurement

The Operator maintains detailed records of all AML/CTF training activities to demonstrate compliance and effectiveness. Records shall be made available to the Gaming Control Board upon request and shall include:

- Training materials and content delivered;
- Names, roles, and departments of trained employees;
- Dates of training sessions;
- Results of assessments or tests conducted to measure employee comprehension and competency;
- An updated, documented training plan outlining AML/CTF training activities for the forthcoming year.

10. Contact information

For any questions related to this Policy or AML/CTF procedures, please contact:

- **Responsible office:** Compliance Department
- **Contact person:** Anti-Money Laundering Compliance Officer (AMLCO)
- **Email:** help@letsbamble.com

For general customer support inquiries, please use help@letsbamble.com

11. Policy review

This Policy is subject to regular review to ensure its ongoing relevance and effectiveness.

The Policy shall be reviewed at least once per year, or more frequently if there are significant changes in legislation, the Operator's business model, or its risk assessment.

All amendments to this Policy must be approved by the Company's senior management.

12. Contact us

If you have any questions about our AML/CTF Policy, please get in touch with us by email: help@letsbamble.com

If you have any complaints about our AML/CTF Policy or the checks done on your Account and your Person, please get in touch with us by email: help@letsbamble.com.

Director

Starkeast Management B.V. represented by
Menno Jordaen

and
Steven J. Eisdien