

Know Your Customer (KYC) Policy

Last Updated: 12 August 2025

1. Introduction

1.1. <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.

This Policy forms a legally binding agreement between the Operator and any individual who registers for or uses the Website’s services (“Customer”). Compliance with this Policy is a prerequisite for opening and maintaining an account.

1.2. Regulatory Foundation and Purpose

The Operator is licensed and regulated in Curaçao and is committed to preventing its services from being used for unlawful purposes. This Policy ensures full compliance with:

- 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).

The objectives of this Policy are:

- a) To establish the lawful identity of the Customer;
- b) To prevent access to services by minors and other Vulnerable Persons, as defined in 1.1(h) of the LOK. This includes individuals who have insufficient control over their gambling behavior, are self-excluded, or have been declared bankrupt;
- c) To mitigate risks of identity fraud and financial crime;
- d) To implement the Customer Due Diligence requirements of the Operator's overarching AML/CTF Policy.

1.3. Customer’s Obligation

By creating an account, the Customer warrants that all information and documents provided to the Operator are true, accurate, current, and complete. The Customer must promptly notify the Operator of any changes to personal or contact details.

2. Customer Due Diligence (CDD) Framework

The Operator applies a risk-based, multi-level approach to CDD. The scope of verification depends on the Customer's risk profile and transaction activity.

2.1. Simplified Due Diligence (SDD)

Trigger: Required upon account registration.

Requirement: Full legal name, date of birth, country of residence, and complete residential address.

Process: Automated screening for age, jurisdiction eligibility, and basic risk assessment. SDD completion is required to activate the account.

2.2. Standard CDD

Trigger: Required when:

- Deposits or withdrawals reach NAF 4,000 (or currency equivalent);
- The Compliance Department requests it following a risk assessment.

Requirement: Submission of documents listed in Article 3.

2.3. Enhanced Due Diligence (EDD)

Trigger: Required when:

- Deposits or withdrawals reach EUR 5,000 (or currency equivalent);
- The Customer is identified as a Politically Exposed Person (PEP) or high-risk;
- Complex or unusual transactions are detected without a clear lawful purpose.

Requirement: CDD documents plus proof of Source of Funds (SOF) and/or Source of Wealth (SOW) in line with the AML/CTF Policy.

2.4. Verification in Relation to Vulnerable Persons

The Operator acknowledges its duty of care towards all Customers. The KYC process serves as a primary tool in fulfilling this duty.

2.4.1. Age Verification: automated and documentary checks are rigorously applied to ensure no individual under the legal age of 18 can access the services.

2.4.2. Self-Exclusion Screening: as part of our due diligence, we may screen Customer details against internal and, where applicable, national or shared self-exclusion registers to prevent access for individuals who have voluntarily opted to cease gambling.

2.4.3. Behavioral Flags: information verified during the KYC process (e.g., age, country of residence) is used as a baseline parameter within our transaction and behavioral monitoring systems. Significant deviations from expected patterns may trigger a Customer profile review, which can include reassessment under our Responsible Gaming framework. For more details, refer to the Operator's Responsible Gaming Policy.

3. Documentary Verification Standards

All documents must be clear, unaltered, high-resolution color copies.

3.1. Proof of Identity (POI)

Accepted:

- Passport (full bio-data page)
- National ID card (front and back)
- Driver's license (front and back)

Standard: All details must be visible; document must be valid; personal data must match registration details.

3.2. Proof of Address (POA)

Accepted (issued within the last 3 months):

- Utility bill (excluding mobile bills)
- Bank or credit card statement
- Mortgage statement or tenancy agreement
- Government-issued document (e.g., tax notice)

Standard: Must show issuer's name/logo, issue date, and Customer's full name/address.

3.3. Selfie Verification

The Operator may require a selfie of the Customer holding their POI and a handwritten note with a unique code and date. The face must be clearly visible; ID details must be legible.

3.4. Document Submission and Review Process

All documents must be submitted exclusively through the secure verification portal located within the Customer's account profile. Documents sent via email or other unsecure channels will not be accepted. The Operator's trained Compliance team will review the submitted documents. The Operator may utilize third-party electronic verification services to assist in validating the authenticity of the provided information.

4. Verification of Financial Instruments

4.1. Ownership Principle

The Customer may only use payment methods registered in their own name.

4.2. Verification Right

The Operator may request proof of ownership of any payment method. Failure to provide proof will result in account suspension and possible cancellation of transactions.

5. Procedural Governance and Consequences

5.1. Restrictions During Verification

When verification is initiated, withdrawals are suspended and deposits or gameplay may also be blocked until completion.

5.2. Compliance Timeline

The Customer must submit the required documents within 30 calendar days from the date the formal request is issued and made visible within their account. The Operator is not responsible for any losses, perceived or actual, incurred by the Customer as a result of account restrictions lawfully imposed during this verification period. The Operator will make reasonable efforts to notify the Customer of the request via email and on-site notifications, but it remains the Customer's responsibility to monitor their account status.

5.3. Non-Compliance or Misrepresentation

Failure to provide documents within 30 days may result in account closure. Providing fraudulent documents will lead to permanent account closure, balance forfeiture, and reporting to authorities.

6. Ongoing Diligence and Data Management

6.1. Ongoing Diligence and Re-Verification

The Customer is under an ongoing obligation to ensure that all personal and contact data held by the Operator is accurate and up to date. The Operator's relationship with the Customer is

subject to continuous monitoring. The Operator reserves the right to request re-verification of the Customer at any time, for reasons including, but not limited to:

- The expiration of a previously submitted identity document.
- A significant change in the Customer's transactional patterns or risk profile.
- A change of registered personal details (e.g., name, address).
- As part of a scheduled periodic review of the customer base, which will occur at least once every two years for active customers.

Failure to comply with a re-verification request will result in the application of account restrictions as outlined in 5.1.

6.2. Data Protection

The Operator complies with GDPR standards. Data is encrypted, stored securely, and accessed only by authorized staff. See Section 8 of the AML/CTF Policy and the Privacy Policy for details.

7. Inquiries and Policy Review

7.1. Contact Information

Questions regarding this Policy may be sent to **help@letsbamble.com**.

7.2. Policy Updates

This Policy is reviewed annually and may be amended in response to regulatory changes or updated risk assessments. The latest version will always be available on the Website.