



Know Your Customer Policy

Customer due diligence and identity verification procedures in compliance with CGA requirements and AML/CFT legislation.

v1.0

☐ Draft

TABLE OF CONTENTS

1.0 Purpose & Scope

This Know Your Customer (KYC) Policy establishes the procedures for customer identification, verification, and ongoing due diligence. It ensures the operator can verify the identity of all players, assess risk profiles, and meet regulatory obligations under CGA requirements and applicable AML/CFT legislation.

This policy applies to all customers registering for an account, making deposits, requesting withdrawals, or engaging in gaming activity on the platform.

2.0 Regulatory Basis

This policy is aligned with:

- CGA KYC and Customer Due Diligence Requirements
- Curaçao National Ordinance on Identification when Rendering Financial Services (NOIRS)
- FATF Recommendation 10 (Customer Due Diligence)
- EU Anti-Money Laundering Directive provisions (where applicable)

3.0 Customer Identification Program

At registration, all customers must provide:

- **Full Legal Name** — as it appears on government-issued identification
- **Date of Birth** — must confirm player is at least 18 years of age
- **Residential Address** — full postal address

- **Email Address** — verified through confirmation link
- **Phone Number** — verified through SMS OTP (where applicable)
- **Nationality/Country of Residence** — used for risk assessment and jurisdiction checks

The system automatically checks the provided country of residence against the restricted jurisdictions list and blocks registration from prohibited territories.

4.0

Verification Procedures

Identity Verification (Level 1):

- Government-issued photo ID: Passport, national ID card, or driving license
- Document must be valid (not expired), clearly readable, and show full name, photo, date of birth, and document number
- Selfie verification: Live or recent photograph of the player holding their ID document

Address Verification (Level 2):

- Utility bill (electricity, water, gas, internet) dated within 3 months
- Bank statement dated within 3 months
- Government correspondence or tax document dated within 12 months
- Document must show full name and address matching registration details

Payment Verification (Level 3):

- Proof of ownership for payment methods used (e.g., bank card showing name and last 4 digits)
- Bank statement or e-wallet screenshot confirming account ownership

5.0

Verification Thresholds & Triggers

The following thresholds trigger mandatory verification requirements:

Before First Withdrawal Full Level 1 + Level 2 verification required
Cumulative Deposits ≥ €2,000 Identity verification mandatory
Single Transaction ≥ €1,000

Identity confirmation required

Cumulative Deposits $\geq$ €10,000

Source of funds documentation required

6.0 Source of Funds & Wealth

Source of Funds (SOF) verification is required when:

- Cumulative deposits exceed €10,000
- Customer is identified as a PEP or PEP associate
- Transaction patterns indicate potential risk
- As part of Enhanced Due Diligence for high-risk customers

Acceptable SOF Documentation:

- Employment contract or payslips (last 3 months)
- Business ownership documentation and financial statements
- Investment portfolio statements
- Property sale documentation
- Inheritance documentation (grant of probate, solicitor confirmation)
- Savings account statements demonstrating accumulation over time

7.0 Ongoing Monitoring

Customer due diligence is not a one-time exercise. Ongoing monitoring includes:

- Periodic re-verification of customer documents (at least annually for high-risk)
- Monitoring for changes in customer risk profile
- Transaction pattern analysis against established customer profile
- Sanctions and PEP screening at regular intervals
- Updating customer records when new information becomes available

8.0 High-Risk Customer Management

Customers categorized as high-risk based on the risk assessment are subject to:

- Enhanced Due Diligence (EDD) procedures
- Senior management approval for account activation and continued relationship
- Increased monitoring frequency
- Lower trigger thresholds for SOF requirements
- Quarterly relationship reviews

9.0 Third-Party Verification Services

The operator may engage licensed third-party verification providers to assist with:

- Automated document verification (AI-powered ID checks)
- Biometric/liveness verification
- Database checks against government registries
- PEP, sanctions, and adverse media screening

All third-party providers must be vetted, contracted, and compliant with applicable data protection regulations. The operator retains responsibility for all KYC decisions regardless of third-party input.

10.0 Non-Compliance & Account Restrictions

Where a customer fails to provide required verification documents within the prescribed timeframe:

- Account may be restricted (deposits disabled, withdrawals frozen)
- Gaming activity may be suspended
- Account may be permanently closed if verification is not completed within 30 days
- Remaining funds will be handled in accordance with CGA regulations and terms of service

The compliance team will attempt to contact the customer at least three times before account closure.

11.0 Data Handling & Privacy

All KYC data is handled in strict compliance with data protection regulations:

- Data collected solely for KYC/AML purposes and not used for marketing
- Encrypted storage and secure transmission of all identification documents
- Access restricted to authorized compliance and management personnel
- Retention period: minimum 5 years after account closure, as required by CGA

- Secure destruction of data after the retention period expires

12.0 Policy Review

This KYC Policy is reviewed at least annually and updated as necessary to reflect changes in CGA requirements, applicable legislation, and industry best practices. All amendments are approved by the Compliance Officer and Board of Directors.