

Know Your Customer Policy

RITCHIE RABBIT GAMES B.V.

1. Purpose of the KYC Policy

The **Know Your Customer (KYC) Policy** establishes mandatory procedures and standards to ensure that Internet Gaming Operators licensed in Curacao

- Verify the identity of their players.
- Prevent fraudulent activities.
- Comply with Anti-Money Laundering (AML) and Counter-Terrorist Financing (CTF) regulations.
- Maintain a safe, transparent, and secure gaming environment.

2. Objectives of KYC

1. **Compliance with Regulations:** Ensure adherence to local and international AML/CTF laws and FATF recommendations.
2. **Player Integrity:** Verify the identity of players to prevent underage gambling, fraud, and financial crime.
3. **Risk Mitigation:** Minimize risks associated with high-risk jurisdictions, Politically Exposed Persons (PEPs), and suspicious transactions.
4. **Transparency:** Promote responsible gaming and safeguard player funds.

3. Scope

This policy applies to:

- All players registering for gaming services.
- Business relationships established with third-party service providers.
- Transactions exceeding designated thresholds or identified as high-risk.

4. Key KYC Principles

1. **Customer Identification:** Verify the identity of players when the total value of aggregate lifetime deposits reaches \$10,000 USD or a withdrawal request of any amount.
2. **Risk-Based Approach:** Apply varying levels of due diligence based on the player's risk profile.
3. **Record Retention:** Maintain all KYC-related documents and transaction records for at least five (5) years.
4. **Continuous Monitoring:** Monitor player behavior and transactions to identify suspicious activity.

5. Customer Identification and Verification Process

5.1 Information Collection

The following information must be collected from all players during registration:

- Full legal name.
- Date of birth (to confirm minimum legal age).
- Nationality.
- Residential address.
- Contact information (email and phone number).
- Payment information (e.g., bank account or e-wallet details).

5.2 Document Verification

Operators must obtain and verify the following documents:

- 1. Proof of Identity**
 - Valid government-issued ID, such as:
 - Passport.
 - National ID card.
 - Driver's license.
 - The ID must contain the player's photo, name, and date of birth.
- 2. Proof of Address**
 - Recent utility bill, bank statement, or government correspondence (not older than three months).
- 3. Payment Verification**
 - Bank statements or screenshots showing ownership of payment methods used.

5.3 Enhanced Due Diligence (EDD)

EDD is required for:

- Players with high-risk profiles (e.g., PEPs or players from high-risk jurisdictions).
- Transactions exceeding \$10,000 USD or groups of linked transactions exceeding \$10,000 USD
- Unusual or complex transaction patterns. EDD measures include:
- Verifying the source of funds and source of wealth.
- Conducting additional identity checks.
- Monitoring transactions more frequently.

6. Risk-Based Approach

Operators must classify players into risk categories based on:

- Geographic location: High-risk countries as per FATF guidelines.
- Player activity: Frequent or high-value transactions.
- Player type: PEPs or individuals with adverse media mentions. Based on the risk classification:
- Low-risk players: Standard Due Diligence (SDD).
- High-risk players: Enhanced Due Diligence (EDD).

7. Ongoing Monitoring

- 1. Transaction Monitoring**
 - Implement automated tools to monitor transactions for unusual activity, such as:
 - Large deposits or withdrawals.

- Rapid movements between accounts.
 - Multiple small transactions designed to evade reporting thresholds.
 - 2. **Behavioral Monitoring**
 - Identify patterns indicative of problem gambling, fraud, or potential ML/TF activities.
 - 3. **Trigger Events**
 - Conduct periodic reviews of player accounts, triggered by:
 - Account inactivity followed by large transactions.
 - Player profile updates (e.g., changes in address or payment method).
 - Notifications from third-party monitoring services.
-

8. Politically Exposed Persons (PEPs)

8.1 Identification

PEPs include individuals who hold or have held prominent public functions, as well as their family members or close associates.

8.2 Enhanced Measures

- Conduct comprehensive checks using third-party databases.
 - Obtain approval from senior management before establishing a business relationship.
 - Regularly review the account and transactions for unusual activity.
-

9. Record Keeping and Confidentiality

1. Retention Period

- Retain all KYC documents, transaction records, and communication logs for a minimum of five (5) years after the business relationship ends.

2. Data Protection

- Securely store player data in compliance with the **Data Protection Act** and international privacy laws such as GDPR.
- Ensure player data is used solely for verification and compliance purposes.

3. Accessibility

- Ensure that KYC records are accessible to regulatory authorities upon request.
-

10. Reporting Obligations

1. Suspicious Activity Reporting (SARs)

- Report suspicious activities within 7 days of detection.
- Include detailed information on the player, transaction, and reasons for suspicion.

2. Threshold Reporting

- Report all transactions exceeding \$10,000 USD, even if no suspicion arises.
-

11. Compliance Oversight

1. Appointment of a Compliance Officer

- Every operator must appoint a **Compliance Officer** responsible for:

- Overseeing KYC implementation.
- Liaising with regulatory authorities.
- Ensuring the submission of SARs and transaction reports.

2. Internal Audits

- Conduct periodic internal audits to evaluate the effectiveness of KYC measures.

3. Training Programs

- Train employees on KYC procedures, including:
 - Identifying fraudulent documentation.
 - Recognizing red flags for ML/TF activities.
 - Reporting obligations under Curacao's regulatory framework.

12. Penalties for Non-Compliance

Failure to comply with KYC requirements may result in:

- Administrative penalties, including fines.
- Suspension or revocation of the operator's gaming license.
- Referral for criminal investigation, if applicable.

13. Continuous Improvement

Operators are encouraged to:

- Regularly review and update KYC policies to align with changes in AML/CTF regulations.
- Adopt advanced technologies, such as AI and blockchain, to enhance verification processes and reduce fraud.

14. Contact Information

For assistance or inquiries regarding KYC compliance, contact:

RITCHIE RABBIT GAMES B.V.

Email: n.rockman.x@gmail.com

Website: ritchierabbit.com

Disclaimer: This KYC policy is a framework designed to meet the regulatory requirements of Curacao. Operators must adapt this policy to their specific operational needs while ensuring full compliance with local laws and regulations.

