

Apollo Sync B.V.

KYC Policy

1. Registration Requirement

Players who do not register an account with the Company will not be permitted to access the Services, place bets, make deposits or receive winnings. Registration is a mandatory prerequisite for participation in any gambling activity on the website.

During registration, the Company collects identifying information as described in this Policy. By registering, the player authorises the Company to undertake the verification checks described herein.

By agreeing to the Terms, you authorise us to undertake verification checks as we require or may be required by third parties (including regulatory bodies) to confirm your identity and contact details and to prevent money laundering and terrorist financing and in order to verify if you are subject to a politically exposed person or a sanctions regime (the “Checks”).

The Company reserves the right to request documents to verify your Account (Age and Identity Verification). These include, but are not limited to: valid ID containing the place of birth and nationality (national ID, passport, driving licence), proof of address not older than 6 months (e.g. utility bill such as electricity, water bill or bank statement attesting your residential address), bank cards, proof of online deposit, bank statements, source of funds, source of wealth, etc. This procedure is mandatory in order to confirm and verify the age and identity, as well as the residential address of the account holder.

2. CDD Initiation

2.1. Timing of CDD

Customer Due Diligence is initiated no later than when a customer's cumulative deposits reach ANG 4,000. Any EUR equivalent stated by the Company is indicative only and does not replace the operative ANG threshold. The Company may initiate CDD at an earlier point at its discretion, including upon registration, where the customer presents a higher risk profile.

2.2. Calculation of the Deposit Threshold

The deposit threshold is calculated as the aggregate of all deposits made by the

customer from the date of registration. Linked transactions — namely those which appear to form part of an overall transaction pattern intended to circumvent the threshold — shall be aggregated for the purpose of this calculation. The Company's systems track cumulative deposits in real time.

2.3. Actions Upon Reaching the Threshold

Upon a customer's cumulative deposits reaching ANG 4,000:

- The customer is notified that identity verification is required
- Upon reaching the CDD threshold, the account shall be placed under verification restriction. No further deposits, withdrawals, or gameplay shall be permitted until the required verification has been completed to the Company's satisfaction, unless a narrower restriction is expressly permitted under applicable law and internal controls.
- The customer has 30 calendar days to submit all required documents

If the player fails to provide requested documents within 3 calendar days of the verification request, any pending withdrawal request may be cancelled and returned to the player's account balance pending completion of verification. If the player fails to complete the requested verification within 30 calendar days, the account may be blocked and the business relationship terminated, subject to AML/CFT requirements.

3. Failure to Complete CDD/KYC

If a customer fails to provide all required CDD/KYC documentation within 30 (thirty) calendar days from the date on which the deposit threshold was reached, the following procedure shall apply:

Step 1: On Day 30, the customer's account is immediately blocked. No further deposits, withdrawals or gameplay are permitted.

Step 2: AML/CFT Compliance Officer is notified and assesses whether the circumstances warrant submission of a SAR to the FIU Curaçao.

Step 3: If no SAR is required, any available balance in the customer's account (net of applicable deductions) shall be returned to the originating payment source within a reasonable period.

Step 4: The business relationship is formally terminated. The account is permanently closed and the customer is informed that their account has been closed due to failure to complete identity verification (without disclosing any AML concerns if a SAR is in process).

Step 5: All records relating to the customer are retained for a minimum of 5 years in accordance with the Company's record-keeping policy.

In the event that, for any reason, an Account Holder denies or is unable to satisfy the Website's requirements for further verification of the Account Holder's identity within thirty (30) days from the date on which the request was made, the Website may take action required to ensure compliance with legal and regulatory obligations. Consequently, we reserve the right to limit and/or restrict access to your account including, without being limited to, restricting access to the amounts deposited into the account.

In the event that a SAR has been filed and the Company is awaiting consent from the FIU, funds shall not be returned until such consent is obtained or the Company is otherwise authorised to release them.

4. PEP and Sanctions Screening

4.1. Initial Screening

All customers are screened against PEP and sanctions databases at the point of registration.

4.2. Threshold-Triggered Screening

Regardless of whether PEP screening has already been conducted at registration, the Company shall conduct a further PEP and sanctions screening at the point of CDD initiation, i.e., when the customer's cumulative deposits reach ANG 4,000, and in any event no later than the date on which CDD documentation is reviewed and processed. This re-screening is mandatory and shall be documented in the customer's file.

4.3. Ongoing Screening

The entire customer database is screened against updated PEP and sanctions lists every 6 (six) months. Additional ad-hoc screening is performed upon receipt of updated lists or specific guidance from the CGA or FIU.

4.4. Match Procedure

Any positive match (whether at registration, threshold or periodic screening) shall be handled in accordance with the AML Policy Section 4.7. Any customer identified as a PEP, family member, or close associate of a PEP shall be subject to Enhanced Due Diligence, source-of-funds/source-of-wealth review, senior management approval, and ongoing enhanced monitoring. The Company may reject or terminate the relationship where the resulting risk is unacceptable or cannot be adequately mitigated.

Any potential sanctions match shall be escalated immediately for review. Where a sanctions match is confirmed, the account shall be rejected, restricted, frozen, or closed as required by applicable sanctions law, AML/CFT obligations, and internal escalation procedures.

5. Medium and High Risk Customers

5.1. Minimum Information Requirements

As a minimum, the following information shall be obtained from all customers classified as MEDIUM or HIGH risk:

(1) Nature of business / occupation / employment: The customer's current occupation, employer and the nature of their business activities.

(2) Additional sources of wealth: Any other activities from which the customer derives their wealth beyond their primary occupation (e.g., investments, inheritance, sale of property, sale of business, dividends).

(3) Expected source and origin of funds: The specific source of the funds that the customer intends to use throughout the business relationship (e.g., salary, savings, business income, investments).

(4) Anticipated nature and level of transactions: The customer's expected transaction pattern, including the anticipated frequency and value of deposits and withdrawals throughout the business relationship.

5.2. Supporting Evidence for HIGH Risk Customers

For HIGH risk customers, supporting documentary evidence must be obtained for each of the items in Section 5.1 above. Acceptable evidence includes:

For (1): Employer letter, employment contract, business registration certificate.

For (2): Inheritance documents, investment account statements, property sale contracts.

For (3): Bank statements (minimum 3 months), payslips (minimum 3 months).

For (4): Customer's written declaration of expected transaction levels.

AML/CFT Compliance Officer must approve all HIGH risk customer relationships before the business relationship is established or continued.

6. Ongoing Monitoring

The Company adopts the following procedure to ensure that player-related

documents, data and information are reviewed and kept up-to-date:

(a) Expiry monitoring: The verification system tracks document expiry dates. When an identity document is within 60 days of expiry, the system automatically requests a renewal document from the customer.

(b) Periodic review: All customer CDD documentation is reviewed on a risk-sensitive basis — at minimum every 6 months for HIGH risk customers, every 12 months for MEDIUM risk customers, and every 24 months for LOW risk customers.

(c) Event-triggered review: CDD documentation is reviewed and updated whenever the Company becomes aware of information that may affect the customer's risk profile, including: changes in customer behaviour, new adverse media, change of jurisdiction, or significant increase in transaction volumes.

(d) Documentation of updates: All updates to customer records are logged in the Company's KYC system with a timestamp and the identity of the staff member who performed the update.

7. Data Storage

In accordance with Article 5.9(1)(j) of the National Ordinance on Games of Chance (LOK), all digital records containing critical information about players, their gaming transactions, and their financial transactions must be maintained at all times on a server located within a Tier-IV certified data centre that is registered in Curaçao.

Specifically, the following categories of data are subject to this requirement:

(a) Player identity and KYC documentation (including copies of identity documents, proof of address, source of funds documentation);

(b) All deposit and withdrawal transaction records;

(c) Gaming transaction logs (bet placements, game results, account credits and debits);

(d) CDD and EDD records;

(e) PEP and sanctions screening results;

(f) Suspicious Activity Reports (internal and external);

(g) Responsible gaming interactions and self-exclusion records.

The Company shall ensure that its data hosting provider holds a valid Tier-IV certification (or equivalent) and is registered in accordance with Curaçao law.

Evidence of this certification shall be maintained by AML/CFT Compliance Officer and provided to the CGA upon request.

7.1. Data Storage Infrastructure

All digital records referenced in this Policy shall be stored on a server of a Tier-IV certified data centre registered in Curaçao, in accordance with Article 5.9(1)(j) of the LOK. AML/CFT Compliance Officer is responsible for verifying and maintaining evidence of the data centre's Tier-IV certification on an annual basis.

8. Transaction Monitoring

8.1. Risk-Based Transaction Scrutiny

The Company applies transaction monitoring proportionate to the customer's risk classification, as follows:

LOW RISK customers: Automated monitoring only via the Transaction Monitoring System. Manual review triggered only upon generation of an automated alert. Transactions reviewed quarterly in aggregate.

MEDIUM RISK customers: Automated monitoring plus manual review of all withdrawals above ANG 2,000. Monthly review of transaction patterns by the AML Team. All withdrawals require AML Team approval before processing.

HIGH RISK customers: Automated monitoring plus manual review of ALL transactions (deposits and withdrawals). Weekly review of transaction patterns by the AML Team. All transactions require AML/CFT Compliance Officer approval above ANG 4,000. Source of funds documentation required for each deposit above ANG 1,000.

8.2. Timing of Transaction Scrutiny

Transaction scrutiny is conducted as follows:

- Automated alerts: reviewed within 24 hours of generation
- Withdrawal approvals (Medium risk): within 2 business days
- Withdrawal approvals (High risk): within 3 business days
- Periodic manual reviews: within the timeframes specified in Section 6

8.3. Structuring Detection

Particular attention is paid to transactions that may indicate structuring (i.e., deliberately breaking up transactions to fall below reporting or CDD thresholds). Structuring indicators are included in the automated Transaction Monitoring System triggers as described in Section 3.8 of the AML Policy.

2/2