

KYC POLICY (KNOW YOUR CUSTOMER)

Magic365.com

1. Introduction

This Know Your Customer (KYC) Policy sets out the mandatory procedures for the identification, verification, and monitoring of customers applied by Magic Stones N.V. — the operator of the Magic365.com platform — in accordance with the legislation of Curaçao, including the National Ordinance on the Reporting of Unusual Transactions (NORUT), the National Ordinance on Identification when Rendering Services (NOIS), the National Ordinance on Games of Chance (LOK), and the Guidelines of the Curaçao Gaming Authority (CGA). This Policy aligns with international standards, including the FATF Recommendations.

2. Objectives of the Policy

The aim of this Policy is to prevent the use of the Magic365.com platform for money laundering, terrorist financing, or unlawful activity, and to ensure age compliance, lawful origin of funds, and protection of customer interests.

3. Applicability

This Policy applies to all customers registering, depositing, placing bets, or withdrawing funds on the platform, as well as all employees involved in customer support, compliance monitoring, and technical assistance.

4. Responsible Persons and Governance Structure

The MLRO is responsible for implementing the KYC Policy. The Data Protection Officer (DPO) ensures compliance with personal data obligations. The Head of Customer Service manages communications, and the technical team supports blocking systems, alerts, and monitoring.

5. Age and Identity Verification

All players must confirm, at the moment of registration, that they are at least 18 years of age or have reached the legal gambling age in their country of residence, whichever is higher. The Company applies a strict zero-tolerance policy regarding underage gambling. If it is discovered that a player participated while being underage, their account will be immediately closed, all wagers and winnings invalidated, and deposits confiscated. The incident is documented and reported to the CGA.

Identity verification is a mandatory procedure for all players and is conducted in two stages:

- Initial verification prior to the first deposit (light KYC);
- Full verification prior to the first withdrawal or upon reaching cumulative deposit thresholds (enhanced KYC).

The following documents may be requested:

- government-issued photo ID (passport, national ID, or driver's license);
- proof of residential address not older than 90 days (e.g., utility bill, bank statement);
- proof of ownership of the payment method used (e.g., partial credit card scan, bank statement);
- selfie or live video verification, with or without document in hand.

All documents must be clear, authentic, and verifiable. Players are solely responsible for ensuring the validity of submitted documents. Submitting falsified, altered, misleading, or fraudulent documents will result in immediate account suspension, rejection of all transactions, and potential permanent exclusion from the platform. Magic365.com may request additional documents at any time and reserves the right to restrict account access until full verification is complete.

Verification is conducted manually by trained compliance officers and/or via automated verification systems integrated with public and private data sources. The Company also reserves the right to engage third-party vendors to validate customer identity, age, address, and payment details using secure KYC platforms.

During the verification process, access to withdrawals may be temporarily restricted. In case of non-cooperation, non-response to document requests, or provision of unverifiable data, the Company may reject transactions, freeze funds, and report the case to the FIU or other competent authorities.

6. Unique Account and Duplicate Accounts

Each player may only open one personal account linked to a unique IP address, device, and individual. Duplicate accounts are considered a violation and may be closed at any time. In case of account recovery, the player must notify the Company and obtain permission. Otherwise:

- all transactions from duplicate accounts are void;
- all bonuses, winnings, and refunds are forfeited and may be recovered;
- no refunds are issued from duplicate accounts;
- any abuse (e.g., bonus exploitation) results in forfeiture of original deposits;
- withdrawn funds may be reclaimed, and authorities informed.

7. Source of Funds and Source of Wealth

The Company may request a source of funds declaration, bank statements, and income proof (payslips, contracts). Failure to provide or provision of false data leads to account freezing and FIU Curaçao notification. Proof of wealth must support long-term asset accumulation (inheritance, business income, etc.).

8. Ban on Anonymous and Nominee Accounts

The registration and operation of anonymous, pseudonymous, or nominee accounts are strictly prohibited. All players must undergo full identification and verification; accounts that cannot be reliably linked to an identified individual are blocked.

Accounts associated with anonymizing technologies or privacy-preserving tools — including but not limited to cryptocurrency mixers, tumblers, privacy coins (e.g., Monero, Zcash), or unverified self-custodial wallets — are treated as a serious AML breach.

Use of false identities, forged documents, or proxy ownership is classified as an attempt to circumvent regulatory obligations and will result in immediate account termination and asset freezing.

In such cases, the Company will:

- suspend or permanently disable the account;
- confiscate all balances and winnings;
- log the incident and report it to the FIU Curaçao under the Unusual Transaction Reporting framework (NORUT);
- flag the user in internal blacklists and escalate the matter to law enforcement if criminal intent is suspected.

Additionally, any attempts to deposit or withdraw funds using unidentified wallets or wallets not subject to proper customer due diligence by a licensed VASP will be rejected. Access to the platform will be suspended until the account holder provides satisfactory documentation regarding the wallet's ownership, origin, and compliance history.

The use of shared or nominee accounts — including accounts accessed by third parties, or opened in the name of another individual — is likewise prohibited and constitutes a violation of the Terms and this Policy.

All flagged incidents are subject to enhanced review and MLRO escalation. Repeat attempts or coordination between multiple users for the purpose of obscuring identity will be considered aggravated misconduct

9. Underage Players

If a player is found to be underage at registration, the account is blocked, all transactions are voided, deposits confiscated, and winnings reversed. The violation is reported to CGA.

10. Sanctions Lists and PEP Screening

Customers are screened at registration and periodically against international sanctions lists (UN, EU, OFAC). A match results in immediate account blocking. If a player is identified as a PEP, EDD applies, including income verification and MLRO approval.

Magic365.com strictly adheres to enhanced procedures for identifying and managing relationships involving Politically Exposed Persons (PEPs), in line with the Curaçao regulatory framework and FATF Recommendation 12. A PEP is defined as an individual who is or has been entrusted with a prominent public function within the past 12 months, including but not limited to heads of state, senior politicians, high-ranking government officials, judicial or military officers, executives of state-owned enterprises, or important political party officials. The definition extends to their immediate family members and close associates.

All customer data is screened using automated name screening systems against global PEP databases at the onboarding stage and regularly thereafter. A positive match automatically elevates the risk rating and triggers Enhanced Due Diligence (EDD).

The following measures apply to PEPs:

- Mandatory collection of source of wealth and source of funds documentation;
- Verification of the ownership and control of payment instruments;
- Approval by the MLRO prior to account activation or reactivation;

- Continuous monitoring of the customer's account activity for abnormal transactions or misuse of political influence.

If a PEP attempts to use nominee structures, unverified wallets, or methods inconsistent with declared income, the account is flagged and subject to immediate review. The MLRO must reassess all active PEP profiles at least every 6 months, ensuring ongoing justification for maintaining the relationship.

Magic365.com reserves the right to reject or terminate business relationships with PEPs where the MLRO deems the reputational, legal, or financial risk to be excessive. All decisions regarding the handling of PEP-related accounts are documented and retained for audit purposes.

11. Risk Profiling and Behavioral Monitoring

Each customer is assigned a risk level based on geography, behavior, and source of funds. Behavioral monitoring detects anomalies (multiple IPs, deposit changes, betting patterns, addiction signs). Suspicious activity triggers further review. Declined users are listed in a rejection registry for 5 years.

12. Enhanced Due Diligence (EDD)

EDD is triggered in cases including:

- identification as PEP;
- origin from FATF high-risk jurisdictions;
- deposits exceeding €15,000;
- use of anonymous or crypto funds;
- complex financial structures. EDD requires:
- source of income and wealth confirmation;
- documents proving payment instrument control;
- biometric checks (if needed). MLRO must reassess all EDD cases semiannually.

13. Transaction Processing and AML Measures

Deposits must come from accounts owned by the player. Third-party funding is not permitted. Any attempt to deposit criminally-derived funds is prohibited. Transactions are monitored and reported to FIU and law enforcement. Refusal to provide information leads to account suspension. Suspected ML/TF activity results in freezing and disclosure to authorities. Withdrawals require renewed KYC and source confirmation.

14. Data Storage

All records are retained for at least 5 years, including rejected applications. Data is stored in encrypted form using ISO/IEC 27001 standards. Access is audited and limited to authorized staff. Personal data is not disclosed outside the team. All communications, decisions, and logs are archived.

15. Automation and Alerts

The Company uses automated tools including:

- Name Screening Systems (sanctions, PEP);
- GeoIP and Device Fingerprinting;
- RBA Scoring Engine;
- behavioral anomaly detection (transaction patterns, multiple logins, betting deviations). Alerts are generated and reviewed by the compliance team.

16. Staff Training

Employees receive onboarding and annual AML/KYC training. Topics include PEP detection, UTR filing, abuse indicators, verification techniques, anonymous asset analysis, structuring red flags, geo-risks, and multi-accounting.

17. Violations and Sanctions

Violation of KYC/AML policy may lead to account suspension and fund freezing. Incidents are logged and reported to relevant authorities. Staff violations result in disciplinary actions.

18. Notification, Review, and Publication

The Policy is reviewed annually or upon legal changes. It forms part of the Terms and Conditions, is publicly available, and must be acknowledged during registration.

Contact Information

MLRO: Maksym Uhnivenko

Email: j.compliance@magic365.com

General contact: ks.vatan@magic365.com

Effective Date: 15.06.2025

Approved by the Board of Directors of Magic Stones N.V.



By: Vivian Ersilia o.b.o (SMES) Solutions for Management and Employment Support N.V.

Managing Director

Date: 09.07.2025