

KYC Policy

Version as of December 24, 2025

PREAMBLE

This Know Your Customer ("KYC") Policy (the "**Policy**") is an internal regulatory document adopted by the Company (as defined below) for the purposes of establishing, implementing, and maintaining effective procedures for user identification, verification, and ongoing due diligence in connection with the provision of online gaming services.

This Policy is intended exclusively for internal use and regulatory review and is not published on the Company's website <https://lwin.pro/> ("**Website**"). The Policy is designed to meet the applicable requirements of the Curaçao gaming regulatory framework, including requirements and supervisory guidance issued by the Curaçao Gaming Authority, and relevant supervisory expectations.

This Policy does not replace or duplicate the Company's Anti-Money Laundering and Counter-Terrorist Financing ("**AML/CTF**") Policy, which governs AML-specific controls, reporting obligations, and suspicious activity handling. References to AML-related matters in this Policy are limited to the extent necessary to describe KYC-related processes.

1. INTRODUCTION AND PURPOSE

1.1. The purpose of this Policy is to define the Company's internal standards, principles, and procedures for identifying and verifying users, confirming the accuracy of user information, and ensuring that only eligible and verified users are permitted to access and use the Company's services. This Policy forms part of the Company's internal compliance framework supporting its licensing and ongoing regulatory obligations.

1.2. This Policy aims to:

- ensure compliance with applicable Curaçao gaming regulatory requirements;
- prevent access to the Services by underage persons;
- reduce the risk of fraud, identity misuse, and misuse of the Website;
- support the integrity, security, and lawful operation of the Company's gaming services.

2. SCOPE

2.1. This Policy applies to all employees, contractors, consultants, temporary staff, interns, volunteers, third-party service providers, and any other individuals or entities involved in the operation, administration, or oversight of KYC-related processes on behalf of the Company.

2.2. This Policy applies to all users who register an Account and use the Company's Services, regardless of jurisdiction, device, or access method.

2.3. This Policy covers all stages of the user lifecycle, including but not limited to:

- account registration;
- identity and age verification;
- payment-related verification;
- withdrawals;
- ongoing monitoring and re-verification;
- account restriction or closure related to KYC matters.

3. DEFINITIONS

For the purposes of this Policy:

3.1. **Account** means a registered user account created on the Website.

3.2. **Company** means 1WIN N.V. a company incorporated under the laws of Curaçao with Company Number 147039 and licensed by the Curacao Gaming Authority to offer games of chance under license number OGL/2024/587/0621 in accordance with the National Ordinance on Games of Chance, and registered at Dr. H. Fergusonweg 1, Curacao, and having all rights to operate the gaming software.

3.3. **Player / User** means any natural person who registers an Account and uses the Services.

3.4. **KYC** means the set of procedures used to identify and verify Users.

3.5. **Verification** means the process of confirming the accuracy and authenticity of User information and documents.

3.6. **Third-Party Verification Provider** means an external service provider engaged by the Company to support identity or data verification.

4. GOVERNANCE AND RESPONSIBILITIES

4.1. The Company's management is responsible for approving this Policy and ensuring that adequate resources are allocated for its implementation.

4.2. The Compliance / KYC function is responsible for:

- implementing and maintaining KYC procedures;
- overseeing verification processes;
- ensuring consistency with regulatory requirements;

- acting as a point of contact for regulatory inquiries related to KYC.

4.3. User Support personnel may assist with the collection and review of User information and documentation in accordance with internal procedures.

4.4. The Company may engage Third-Party Verification Providers; however, ultimate responsibility for KYC compliance remains with the Company.

5. BASIC KYC PRINCIPLES

5.1. The Company applies a risk-based and proportionate approach to User identification and verification, taking into account the type of Services provided, transaction patterns, user behavior, geographic indicators, geographic indicators, delivery channels, and other relevant risk factors identified through the Company's internal risk assessment.

5.2. All Users must be identified using their true, accurate, and lawful personal information. The use of fictitious, misleading, or third-party identities is strictly prohibited.

5.3. The Company does not permit anonymous Accounts or the use of Services without prior identification and verification where required by internal thresholds or regulatory expectations.

5.4. The Company does not permit Users to register, maintain, or use Accounts on behalf of third parties. Each Account must be registered and operated solely by the individual who has been identified by the Company. The use of nominees, agents, intermediaries, shared Accounts, or any other arrangements whereby a User acts on behalf of another person is strictly prohibited.

5.5. Verification measures are designed to be effective, reasonable, and limited to the minimum data necessary to achieve KYC objectives, while ensuring regulatory compliance.

5.6. The Company ensures segregation of duties between operational, verification, and decision-making functions, where practicable.

5.7. The Company restricts or prohibits access to its Services by Users located in, resident in, or otherwise connected to certain jurisdictions, where such access is restricted due to legal, regulatory, licensing, or internal risk considerations.

Geographic eligibility is assessed as part of the customer onboarding, verification, and ongoing monitoring processes, using information provided by the User and, where applicable, third-party verification tools.

6. USER IDENTIFICATION AND VERIFICATION PROCESS

6.1. Registration Information

6.1.1. Users are required to provide personal details during Account registration, including name, date of birth, and address.

6.1.2. The name, date of birth, and address provided in the Account must correspond exactly to the information contained in the User's official identity documents.

6.1.3. The name registered on the Account must match the name used on payment instruments associated with deposits and withdrawals, unless otherwise justified and approved in accordance with internal procedures.

6.2. Ownership of Funds

6.2.1. Users confirm that they are the lawful owners of all funds deposited into and withdrawn from their Account.

7. VERIFICATION DOCUMENTS AND METHODS

7.1. For the purposes of identity, address, and payment verification, the Company may request one or more of the following:

- a valid government-issued identity document (e.g., passport or national identity card);
- proof of residential address, such as a recent utility bill or official correspondence not older than three (3) months;
- a recent bank, credit, or debit card statement related to the payment method used, not older than three (3) months;
- verification through trusted third-party databases or electronic verification tools.

7.2. Documents must be provided in English or another language accepted by the Company and must be clear, legible, and complete.

8. VERIFICATION TIMING AND ONGOING KYC

8.1. The Company may perform identity, age, and security checks at any time during the User relationship, including but not limited to the following events:

- prior to or during withdrawal processing;
- upon reaching internal transaction or activity thresholds;
- where inconsistencies in User data are identified;
- upon changes to personal, payment, or Account information;
- where indicators of increased risk are detected.
- where required to comply with applicable sanctions, PEP, or regulatory screening obligations, as governed by the Company's AML/CTF Policy.

8.2. Users may be required to undergo ongoing or repeated verification to ensure that previously collected information remains accurate, current, and reliable.

8.3. The scope and frequency of ongoing KYC measures are determined based on the Company's internal risk assessment and regulatory expectations.

9. AGE VERIFICATION

9.1. The Company strictly prohibits access to the Services by individuals below the legal minimum age applicable under the Company's license and relevant jurisdictional requirements (currently 18 years, unless otherwise required).

9.2. Age verification is performed using registration data, identity documents, and, where applicable, third-party verification tools.

9.3. Accounts found to belong to underage individuals shall be closed in accordance with internal procedures.

10. THIRD-PARTY VERIFICATION PROVIDERS

10.1. The Company may engage Third-Party Verification Providers to support customer identification, document verification, database screening, and electronic verification processes.

10.2. Prior to engagement, the Company conducts due diligence on such providers to assess their reliability, security standards, and regulatory suitability.

10.3. Third-Party Verification Providers operate under contractual arrangements that address data protection, confidentiality, and service scope.

10.4. The use of third-party providers does not transfer or limit the Company's regulatory responsibility for KYC compliance.

11. RECORD KEEPING AND DATA RETENTION

11.1. The Company records and retains User identification data, verification documents, methods used, and verification outcomes.

11.2. Records are retained in accordance with applicable Curaçao regulatory requirements and the Company's internal data retention policies.

11.3. Access to KYC records is restricted to authorized personnel only.

12. HANDLING VERIFICATION FAILURES AND RESTRICTIONS

12.1. Where a User fails to provide requested documentation within seven (7) calendar days or such other period as may be reasonably determined by the Company in justified circumstances, or where verification cannot be completed within a reasonable timeframe determined by the Company, the Company may apply one or more of the following measures:

- restriction of withdrawals or specific Account functionalities;
- temporary withholding of Account balances pending verification;
- cancellation or reversal of transactions where permissible;
- suspension or permanent closure of the Account.

12.2. The Company reserves the right to refuse or discontinue the provision of Services where there are reasonable grounds to believe that continued operation of the Account would expose the Company to regulatory, legal, or operational risk.

12.3. Decisions related to Account restrictions or closures are documented internally in accordance with record-keeping requirements.

13. DATA PROTECTION AND CONFIDENTIALITY

13.1. User information collected for KYC purposes is treated as confidential and processed solely for legitimate compliance and operational purposes.

13.2. The Company implements appropriate technical and organizational measures to protect KYC data against unauthorized access, disclosure, or misuse.

14. TRAINING AND AWARENESS

14.1. Employees involved in KYC-related activities receive appropriate training and guidance tailored to their roles and responsibilities.

14.2. Such training covers, at a minimum, customer identification and verification procedures, internal KYC controls, and escalation requirements.

14.3. Training content is reviewed and updated periodically to reflect regulatory, legal, or operational changes, and where relevant, following internal reviews or supervisory feedback.

15. COMPLIANCE, MONITORING AND POLICY REVIEW

15.1. Compliance with this Policy is subject to ongoing internal monitoring and oversight.

15.2. The Company may conduct internal reviews or audits of KYC processes to assess effectiveness and regulatory alignment.

15.3. This Policy is reviewed at least annually, and additionally where required due to:

- changes in applicable Curaçao gaming or supervisory requirements;
- updates to the Company's business model or risk profile;
- findings from audits, inspections, regulatory feedback, or supervisory communications.

15.4. Any material breach of this Policy may result in corrective measures, including disciplinary action or process remediation.



(SMES) Solutions for Management and Employment Support N.V.

Managing Director

15.01.2026