

Code Harbor N.V.

Know-Your-Client (KYC) Policy

Approving Official(s):	Yevhen Dyba	Signature: 	Date: 30.04.2026
Responsible Office	Compliance Department		
Effective Date	30.04.2026		
Next Review Date:	29.04.2026		

Table of Content

1. Policy Statement..... 3

2. Purpose..... 3

3. Scope and Applicability..... 3

4. Definitions and Framework.....3

5. Documents.....4

6. Verification Process.....5

7. PEP and Sanctions Screening..... 7

8. Ongoing Monitoring.....7

9. Data Protection And Confidentiality..... 8

10. Policy History..... 8

1. Policy Statement

Code Harbor N.V. (hereinafter - the Company) operates the online casino at wildwinz.com (hereinafter - the Website) under a licence issued by the Curaçao Gaming Authority (CGA). The Company reserves the right, at any time, to request any KYC documentation it deems necessary to determine the identity, age, and location of a registered player. We reserve the right to restrict access to services, suspend gameplay, or withhold payment of winnings until identity is sufficiently verified, or for any other reason permitted under applicable law and our Terms and Conditions.

2. Purpose

The purpose of this Policy is to establish a comprehensive framework for customer identification, verification, and ongoing due diligence procedures. The Policy is designed to ensure that Code Harbor N.V. accurately identifies its customers, verifies their identity and age, assesses associated risks, and maintains appropriate customer records in accordance with applicable regulatory requirements, licence conditions, and industry best practices.

The Policy further aims to prevent identity fraud, underage gambling, money laundering, terrorist financing, and other unlawful activities by ensuring that appropriate Know Your Customer (KYC) measures are applied throughout the customer relationship lifecycle.

3. Scope and Applicability

This Policy applies to all employees, officers, contractors, agents, and service providers acting on behalf of Code Harbor N.V. who are involved in customer onboarding, identity verification, account reviews, risk assessments, source of funds verification, ongoing monitoring, or any other customer due diligence activities.

Compliance with this Policy is mandatory for all persons performing activities for or on behalf of Code Harbor N.V. and forms an integral part of the Company's regulatory compliance framework.

4. Definitions and Framework

We take a risk-based approach and perform strict due diligence checks and ongoing monitoring of all players and transactions. In accordance with applicable money laundering regulations and CGA requirements, we apply three levels of due diligence depending on the risk profile, transaction type, and player category:

SDD - Simplified Due Diligence is applied in instances of clearly low-risk players and transactions that do not meet the thresholds triggering standard verification.

CDD - Customer Due Diligence is the standard level of verification applied to the majority of players for identification and ongoing monitoring purposes.

EDD - Enhanced Due Diligence is applied to high-risk players, Politically Exposed Persons (PEPs), players from high-risk jurisdictions, large transactions, or any other cases where heightened scrutiny is required.

5. Documents

Below you can find the types of documents and information that may be requested from you (Documents) depending on the applicable due diligence level:

The minimum identification data set for full Customer Due Diligence (collected at the latest when the NAF. 4,000 / EUR 2,000 threshold is reached, and earlier on a risk basis) includes:

- full name;
- date of birth;
- place of birth;
- permanent residential address;
- nationality;
- identity (document) number.

In clearly documented low-risk scenarios, and until the NAF. 4,000 / EUR 2,000 threshold is reached, identification may be limited to the first three items above (full name, date of birth, and permanent residential address), together with sanctions and PEP screening conducted at registration. The remaining items, and verification of identity against a reliable independent source, are completed as part of full Customer Due Diligence.

Primary identification documents (at least one required):

- valid passport;

- national identity card (front and back);
- document confirming the player's permanent residential address (utility bill, bank statement, or official letter from a public authority), not older than 6 months (where a fixed-line telephone bill is used as proof of address, mobile telephone bills are not accepted).

Additional documents that may be requested:

- driver's licence or other government-issued photo ID;
- selfie of the player holding the identity document (both must be clearly legible);
- bank card photograph showing the first 6 and last 4 digits, the cardholder's name, and the expiry date (the remaining digits must be obscured);
- bank account statement confirming the payment method used;
- source of funds documentation (payslips, tax returns, business ownership evidence) where required under EDD.

Documents may be rejected for the following reasons:

- the name or address on the document does not match the account registration details;
- the document is illegible, damaged, expired, or of insufficient image quality;
- the document does not confirm the required information (age, identity, address);
- the document type is not on the list of accepted documents;
- the document appears to have been altered or tampered with;
- any other reason that the KYC Team or the Company's compliance staff consider appropriate.

6. Verification Process

Once documents are uploaded by the player, a "Verification Pending" status is assigned to the account. The KYC Team will review the submitted documents within 24 hours of receipt and notify the player by email of the outcome: (1) Approved; (2) Rejected; or (3) Additional information required.

Players with "Verification Pending" status may continue to use the platform but are not permitted to make withdrawals until verification is successfully completed.

Upon completion of the document review, the Company issues a final decision. If verification is unsuccessful, the reason is documented internally and communicated to the player together with a support ticket reference number.

If a player fails to pass the KYC process or refuses to provide the required documentation, the Company reserves the right to suspend the account and restrict all deposits and withdrawals. The Company shall maintain a record of all attempts made to obtain the necessary information. If the player subsequently provides the requested documentation, the Company will assess whether the delay affects the ML/TF risk associated with the business relationship before reactivating the account. Where there are no grounds to suspect money laundering or terrorist financing, any remaining funds in the account shall be returned to the player through the same channel used to make the deposit. Where a suspicion of ML/TF/PF exists, the matter shall be reported to the FIU Curaçao via the goAML portal and the funds shall be dealt with in accordance with applicable law and internal procedures.

If a player has successfully completed the KYC process, a detailed algorithmic and manual review of account activity and transaction history is conducted prior to processing any withdrawal to confirm that the withdrawal amount is the result of legitimate gameplay.

The Company is required to complete CDD at the latest when a player's cumulative financial transactions reach NAf. 4,000/ EUR 2,000. Until this threshold is reached, a minimum data set (full name, date of birth, residential address) and sanctions/PEP screening are applied at account registration.

Under no circumstances may a player transfer funds directly to another player's account.

30-Day Rule. If a player reaches the NAf. 4,000 / EUR 2,000 threshold and the required CDD documentation and information is not provided within 30 days from the date the threshold was reached, the Company is obligated to terminate the business relationship with that player. The 30-day period runs from the date on which the threshold was first reached, not from the date of any follow-up request. Where the threshold was reached because of a deposit, the player may not make further deposits or withdraw funds but may continue playing with the funds already credited to the account. Where the threshold was reached because of a withdrawal request, the account must be fully frozen and all gameplay suspended. Upon termination, if no suspicion of money laundering, terrorist financing, or proliferation financing exists, any remaining funds shall be remitted to the same account or wallet from which they originated. If a suspicion of

ML/TF/PF exists, the matter must be reported to the FIU Curaçao via the goAML portal without delay, and internal procedures shall govern whether funds are blocked or returned, taking into account the risk of tipping off the player.

Acting on own behalf. During registration each player must explicitly confirm, by ticking a dedicated checkbox that is not pre-selected, that they are opening and using the account on their own behalf and not for or on behalf of any third party. The Company does not rely on this declaration alone; its ongoing monitoring procedures are designed to detect indications that an account is funded or used by, or for the benefit of, third parties (including syndicates).

Beneficial owners. Where funds wagered through an account are collected from, or winnings shared with, multiple persons (e.g. a syndicate), or where an account is held by a legal person, the Company identifies and takes reasonable measures to verify the identity of each beneficial owner. For legal persons this includes every natural person holding 25% or more of the shares or voting rights, or otherwise exercising ultimate effective control; where no such natural person is identified, the senior managing official is identified and verified.

7. PEP and Sanctions Screening

All players are screened against applicable international sanctions lists (UN, EU, UK, OFAC, Australia, and any local Curaçao list of designated persons and organisations where published) and checked for Politically Exposed Person (PEP) status at the time of registration and on an ongoing basis. A positive match results in immediate account restriction pending further review by the compliance team.

Players identified as PEPs are subject to Enhanced Due Diligence, including senior management approval, source of wealth verification, and heightened transaction monitoring.

The Company does not knowingly accept players who are subject to international sanctions or who are nationals of or resident in a sanctioned or prohibited jurisdiction.

30-Day Rule for Newly Identified PEPs. Where a player who was not identified as a PEP at the time of registration subsequently becomes a PEP, the Company must implement all Enhanced Due Diligence measures within 30 days of identifying the change in status. This includes obtaining senior management approval, verifying the source of wealth and source of funds, and establishing heightened ongoing monitoring. Failure to complete all

EDD measures within the 30-day window requires the Company to terminate the business relationship with that player. The account shall be immediately restricted upon identification of the PEP status, and the CCO shall initiate the EDD process without delay.

8. Ongoing Monitoring

The Company conducts continuous monitoring of player accounts and transactions to detect unusual activity, including sudden changes in deposit or withdrawal behaviour, use of multiple payment methods, or transactions inconsistent with the player's verified profile.

Where unusual activity is detected, the KYC Team may request updated documentation or additional source of funds evidence. Failure to provide such information within the required timeframe may result in account suspension.

Player identity documents and account data are re-verified at regular intervals or upon any material change in account activity, payment instrument, or risk profile.

9. Data Protection And Confidentiality

All documents and personal data submitted for KYC purposes are processed in accordance with applicable data protection legislation, including the General Data Protection Regulation (GDPR) where applicable, and the Company's Privacy Policy (available at wildwinz.com/privacy-policy/). Documents are stored securely and are not shared with third parties except where required by law, by the terms of our regulatory obligations, or as disclosed in the Privacy Policy. The Privacy Policy covers, at minimum: the collection, use, storage, retention, and sharing of personal data. Players are encouraged to review the Privacy Policy for full details of how their data is processed.

KYC records are retained for a minimum of five (5) years following the termination of the business relationship.

10. Policy History

Version: 1.0