

ANTI-MONEY LAUNDERING (AML) AND COUNTER-TERRORISM FINANCING (CTF) POLICY

Approving Official(s): Yevhen Dyba

Responsible Office: Compliance Department

Effective Date: 15.06.2025

Next Review Date: 14.06.2026

1. INTRODUCTION

1.1. **Code Harbor N.V.** (“the Company”) is committed to maintaining the highest standards in combating Money Laundering (ML), Terrorism Financing (TF), and Proliferation Financing (PF). This policy is based on applicable legislation including the National Ordinance on Games of Chance (LOK 2024), the National Ordinance on the Identification when Rendering Services (NOIS), the National Ordinance on the Reporting of Unusual Transactions (NORUT), the Sanctions National Ordinance, and the Kingdom Sanctions Act. It incorporates guidance from the Curaçao Gaming Authority (CGA) and international best practices, including the FATF Recommendations

1.2. The Company prohibits and actively prevents its services from being used for ML, TF, PF, or other financial crime. This policy applies to all Company employees, contractors, and business partners and forms part of the Company’s internal control framework.

1.3. This document defines the operational procedures and responsibilities that support AML/CTF compliance and risk management. It is reviewed and approved annually by the Board of Directors or when material regulatory changes occur.

1.4. The Company acknowledges its obligations under LOK Article 2.2(k) to comply with all relevant AML/CFT laws and the requirement to report unusual transactions via the goAML portal.

2. OBJECTIVES

- To identify, assess, and mitigate ML/TF/PF risks.
- To implement robust CDD/EDD/SDD procedures.
- To maintain effective monitoring and reporting systems.
- To ensure all employees are trained and aware of their obligations.

3. REGULATORY FRAMEWORK

This policy is based on:

- National Ordinance on Games of Chance (LOK 2024)
- National Ordinance on the Reporting of Unusual Transactions (NORUT)
- National Ordinance on the Identification of Clients when Rendering Services (NOIS)
- Sanctions National Ordinance and Kingdom Sanctions Act
- CGA AML/CFT Regulations (2025)
- Ministerial Decree on Indicators of Unusual Transactions (N.G. 2015, no. 73)
- FATF Recommendations

4. GOVERNANCE AND COMPLIANCE STRUCTURE

4.1. The Company has appointed a CCO (Chief Compliance Officer), who is responsible for the implementation of this Policy, monitoring compliance, reporting unusual transactions, and staff training.

4.2. The CCO is accountable to the Board.

4.3. Independent audits are conducted at least annually to test AML program effectiveness.

4.4. New employees are screened for integrity and undergo onboarding AML/CTF training. All employees receive refresher training annually.

5. BUSINESS RISK ASSESSMENT (BRA)

5.1. The Company conducts a comprehensive Business Risk Assessment (BRA) at least annually to identify and evaluate its exposure to Money Laundering, Terrorist Financing, and Proliferation Financing risks. The assessment considers how the Company's products, services, delivery channels, customer segments, and geographic footprint could potentially be misused for illicit financial activity.

5.2. The BRA methodology includes:

- Identification of ML/TF/PF threats related to each product or service (e.g., abuse of bonuses, layering through rapid deposits/withdrawals)
- Risk factor scoring and weighting
- Categorization of risks as low, medium, or high
- Justification for risk ratings based on transaction volume, client behavior, or regulatory concerns
- Evaluation of the adequacy of existing policies, procedures, and internal controls

- Implementation or adjustment of mitigation strategies based on assessment outcomes

5.3. The BRA incorporates findings from Curaçao's National Risk Assessment (NRA) and informs internal policies, procedures, and employee training programs accordingly.

6. CUSTOMER RISK ASSESSMENT (CRA)

6.1. A Customer Risk Assessment is carried out at the time of establishing a business relationship, based on information collected during the onboarding and Customer Due Diligence process.

6.2. The CRA evaluates the specific ML/TF risks that the Company may be exposed to in relation to the individual customer and results in the assignment of a risk rating (low, medium, or high).

6.3. Factors considered include:

- Customer profile (e.g., PEP status, occupation, source of wealth/funds)
- Jurisdictional risk (e.g., FATF grey/blacklist, Transparency International Corruption Index, OFAC sanctions)
- Transaction patterns, behavior, and expected account usage
- Use of intermediaries, VPNs, or other anonymizing technologies

6.4. The customer's risk profile directly determines the level of due diligence, ongoing monitoring, and transaction scrutiny applied. High-risk customers may be subject to Enhanced Due Diligence and more frequent reviews.

7. CUSTOMER ACCEPTANCE POLICY (CAP)

7.1. The Customer Acceptance Policy is directly informed by the outcome of the Customer Risk Assessment (CRA). Based on the customer's assigned risk level, the appropriate level of CDD (standard, enhanced, or simplified) is applied during onboarding.

7.2. The Company maintains strict acceptance criteria, including:

- Refusal to onboard or termination of customers who fail or refuse to complete CDD
- Mandatory PEP screening, in compliance with NOIS and FATF guidance
- Mandatory screening against international sanctions lists (UN, EU, OFAC)

- Full identification and verification of Ultimate Beneficial Owners (UBOs) for corporate entities
- Restriction or exclusion of vulnerable individuals and customers from high-risk jurisdictions

7.3. The CAP reflects the principles of LOK Article 1.4 and ensures that business relationships are only established with customers who meet all AML/CFT obligations and do not present unmanageable risk.

8. CUSTOMER DUE DILIGENCE (CDD)

8.1. The Company performs Customer Due Diligence on all customers before establishing a business relationship. This includes:

- Identity verification using reliable, independent documentation and data sources
- Proof of address validation
- Identification and verification of Ultimate Beneficial Owners (UBOs) in the case of legal persons
- Collection and verification of source of funds and source of wealth information
- Screening against Politically Exposed Persons (PEP) databases and international sanctions lists (e.g., UN, EU, OFAC)

8.2. Enhanced Due Diligence (EDD) is applied in the following cases:

- The customer is identified as a PEP or related party
- The customer resides in or is connected to a high-risk jurisdiction
- There is a complex corporate or trust structure involved
- Activity is inconsistent with the known customer profile or appears suspicious

8.3. Simplified Due Diligence (SDD) may apply only in clearly documented low-risk scenarios and before the financial transactions reach the threshold of NAF 4,000, since the business relationship has been established. In such cases, the Company will collect sufficient basic information to identify the customer and assess risk, while applying a proportionate level of verification. Required information and documentation for SDD includes:

- Full name of the customer
- Date of birth
- Nationality or country of residence

- Contact information (e.g., email address, phone number)
- Payment method details (e.g., card issuer, digital wallet provider)

8.4. CDD must be completed and verified before allowing gameplay, deposits, withdrawals, or any other financial transactions exceeding NAF 4,000.

8.5. If a PEP or sanctioned individual is identified, the account is immediately restricted. The CCO evaluates whether to freeze funds and will report the case to the Financial Intelligence Unit Curacao (FIU) via the goAML portal. All freezing actions follow the procedure outlined in the National Gazette 2016 asset-freezing protocol.

9. ONGOING MONITORING

9.1. Continuous monitoring of client transactions and behavior is conducted through automated systems and manual reviews.

9.2. Red flags include:

- Sudden increase in deposit frequency or value
- Multiple account usage
- Attempted circumvention of KYC procedures

9.3. Monitoring thresholds:

- Cumulative deposits equal or over NAF 4,000
- Multiple failed verification attempts

10. REPORTING OF UNUSUAL TRANSACTIONS

10.1. All employees are trained to recognize indicators of unusual or suspicious activity, including but not limited to:

- Sudden changes in transaction patterns
- Attempts to avoid CDD/KYC measures
- Use of multiple accounts or payment methods
- Transactions inconsistent with the customer profile

10.2. When an employee identifies such a red flag, they must immediately report it internally to the CCO using the Company's internal Suspicious Activity Report (SAR) template.

10.3. The CCO evaluates each internal SAR without delay. If the transaction is deemed unusual or suspicious, the CCO submits an official SAR to the FIU Curaçao via the goAML portal. This obligation applies whether or not the transaction was completed.

10.4. The CCO maintains a secure and confidential register of all SARs, including internal reports and justification for filings or non-filings.

10.5. In accordance with NORUT, tipping-off (informing a customer that they are under investigation or that a report has been filed) is strictly prohibited.

11. RELIANCE ON THIRD PARTIES

11.1. Our company is using Sumsb for CDD measures. Sumsb is a third-party identity verification and compliance platform used to verify player identities and ensure compliance with KYC (Know Your Customer) and AML (Anti-Money Laundering) regulations. On the casino website, Sumsb handles document checks, biometric (selfie) verification, and sanctions screening to help prevent fraud and ensure that only eligible users can participate. <https://sumsub.com/>

12. SANCTIONS COMPLIANCE

12.1. All customers are screened against relevant sanctions lists (UN, EU, OFAC).

12.2. Positive matches trigger immediate account freezes and reporting to the FIU.

12.3. The Company follows Curaçao's asset-freezing procedure as per the 2016 National Gazette directive.

13. RECORDKEEPING

13.1. The Company retains:

- CDD and KYC documentation
- Transaction logs and monitoring records
- Copies of SARs
- Risk assessment reports
- Staff training logs

13.2. Records are stored securely and retained for at least five (5) years after the end of the customer relationship or transaction.

14. TRAINING AND AWARENESS

14.1. All relevant staff receive AML/CFT training upon hiring and annually thereafter.

14.2. Training includes:

- Legal obligations
- Internal procedures
- Red flag indicators
- Use of goAML (if applicable) and internal reporting tools

15. AUDIT AND REVIEW

15.1. Independent audits of the AML program are conducted annually.

15.2. This policy is reviewed at least once a year and updated to reflect changes in laws or business operations. Updates are approved by the Board of Directors.

16. NON-COMPLIANCE CONSEQUENCES

16.1. Failure to comply with this policy may result in serious consequences for both the individual and the Company, therefore consequences for non-compliance may be:

- Internal disciplinary action, up to and including termination of employment for employees
- Regulatory penalties, fines, or suspension or revocation of the Company's license by the CGA for the Company
- Criminal prosecution and legal sanctions under applicable laws (including NOIS, NORUT, and LOK) for Customers

17. CONTACT INFORMATION

Compliance Department – Code Harbor N.V.

Email: compliance@wildwinz.com

18. POLICY HISTORY

Version: 1.3

What's changed:

We have recently updated our policy history to reflect ongoing improvements and changes made across our operations. These updates aim to enhance clarity, ensure compliance with current regulations, and improve overall transparency. Key

changes include refined language for easier understanding, revised sections to align with best practices, and the addition of new provisions addressing recent developments. We encourage all users to review the updated policy to stay informed about how these changes may affect them.

Previous policy date: 03.2025

19. POLICY URL

https://wildwinz.com/aml_policy/

Yevhen Dyba



Signature