

Code Harbor N.V.

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

Approving Official(s):	Yevhen Dyba	Signature: 	Date: 30.09.2025
Responsible Office	Compliance Department		
Effective Date	01.10.2025		
Next Review Date:	30.09.2026		

Table of Content

1. Policy Statement.....	3
2. Purpose.....	3
3. Audience.....	3
4. Definitions and Framework.....	3
5. Policy Implementation.....	6
5.1. Business Risk Assessment.....	6
5.2. Customer Risk Assessment.....	7
5.3. Customer Acceptance Policy.....	7
5.4. Customer Due Diligence.....	8
5.5. Ongoing Monitoring.....	9
5.6. Reporting of Unusual Transactions.....	9
5.7. Reliance on Third Parties.....	10
5.8. Anti-Money Laundering Compliance Program.....	10
6. Compliance and Consequences of Non-Compliance.....	11
7. Related Information.....	12
8. Contact Information.....	12
9. Policy History.....	12
10. Policy URL.....	12

1. Policy Statement

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. The Company prohibits and actively prevents its services from being used for ML, TF, PF, or other financial crime.

2. Purpose

The purpose of this policy is to identify, assess, and mitigate risks associated with money laundering, terrorist financing, and proliferation financing. It establishes the framework for implementing Customer Due Diligence (CDD), Enhanced Due Diligence (EDD), Simplified Due Diligence (SDD), monitoring, reporting, and training procedures to ensure full compliance with local and international AML/CFT requirements.

3. Audience

This policy applies to all Company employees, contractors, agents, and business partners involved in the provision of services, and is binding upon all persons who may act on behalf of Code Harbor N.V.

4. Definitions and Framework

For the purpose of this policy, the following definitions apply:

ML – Money Laundering

Money Laundering is the process by which individuals or entities conceal the illicit origin of funds derived from criminal activities, such as fraud, corruption, drug trafficking, or tax evasion. It involves introducing illicit proceeds into the legitimate financial system and disguising their true source through complex layers of financial transactions, ultimately making the funds appear legally obtained. The objective of money laundering is to integrate “dirty money” into the economy in such a way that it cannot be easily traced back to its criminal origin.

TF – Terrorism Financing

Terrorism Financing refers to the act of providing, collecting, or using funds, directly or indirectly, with the intention or knowledge that such funds will be used to support terrorist acts, organizations, or individual terrorists. Unlike money laundering, the origin of funds used in terrorism financing may be either legitimate or illegitimate. The key element is the intended use of the funds — to facilitate or sustain terrorist activities, recruitment, propaganda, or the maintenance of terrorist networks.

PF – Proliferation Financing

Proliferation Financing involves the provision or collection of funds, financial services, or economic resources that are used, or intended to be used, to support the development, production, acquisition, transfer, or deployment of nuclear, chemical, or biological weapons and their delivery systems, in contravention of international laws or sanctions. This type of financing is often linked to evasion of targeted financial sanctions and may involve front companies, intermediaries, and complex trade-based schemes designed to conceal the end-user or final destination of goods or technology.

PEP – Politically Exposed Person

A Politically Exposed Person (PEP) is an individual who holds or has held a prominent public function, whether domestically or in a foreign country, as well as their immediate family members and close associates. Examples include heads of state, senior government officials, members of parliament, judges, military leaders, and executives of state-owned enterprises. Due to their position and influence, PEPs present a higher risk for potential involvement in bribery, corruption, or other financial crimes, which necessitates the application of enhanced due diligence measures when establishing or maintaining business relationships.

KYC – Know Your Client

Know Your Client (KYC) is the process through which a business, particularly in the financial or gaming sector, verifies the identity of its clients and assesses their risk profile. The KYC process typically includes obtaining identifying information (such as name, date of birth, address, and official identification documents), verifying that information, and understanding the nature and purpose of the client's activities.

CDD – Customer Due Diligence

Customer Due Diligence (CDD) refers to the standard process of identifying and verifying the identity of a client and assessing the risks associated with the business relationship. It includes obtaining sufficient information about the customer's identity, financial activities, and intended purpose of the account or relationship. CDD enables the institution to detect unusual or suspicious activities and maintain ongoing monitoring of client transactions. It is a mandatory element of effective AML/CFT compliance frameworks.

EDD – Enhanced Due Diligence

Enhanced Due Diligence (EDD) involves applying additional and more stringent measures to verify the identity and assess the risk profile of customers who present a higher risk of money laundering, terrorism financing, or other financial crimes. This may include obtaining further documentation, verifying the source of funds and wealth, conducting more frequent transaction monitoring, and requiring management approval before establishing or maintaining the relationship. EDD is particularly applied to PEPs, high-risk jurisdictions, and complex ownership structures.

SDD – Simplified Due Diligence

Simplified Due Diligence (SDD) is a risk-based approach applied to customers or transactions that are considered to pose a low risk of money laundering or terrorism financing. Under SDD, institutions may collect a reduced amount of information or perform verification at a later stage, provided that the risk remains minimal. However, SDD must never be applied where there is any suspicion of money laundering, terrorism financing, or other financial crime, regardless of the perceived low-risk profile.

CGA – Curaçao Gaming Authority

The Curaçao Gaming Authority (CGA) is the regulatory body responsible for overseeing, licensing, and supervising the gaming and gambling industry in Curaçao.

FIU – Financial Intelligence Unit Curaçao

The Financial Intelligence Unit Curaçao (FIU Curaçao) is the central national agency responsible for receiving, analyzing, and disseminating financial information related to suspected money laundering, terrorism financing, and proliferation financing. The FIU operates under the legal framework of Curaçao's AML/CFT laws and serves as a bridge between financial institutions, designated non-financial businesses, and law enforcement authorities. Its role is to detect and prevent financial crimes by collecting and analyzing suspicious transaction reports (STRs) and other relevant data, and by cooperating with international FIUs and organizations.

5. Policy Implementation

5.1. Business Risk Assessment

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.

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

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

5.2. Customer Risk Assessment

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.

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).

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

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.

5.3. Customer Acceptance Policy

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.

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

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.

5.4. Customer Due Diligence

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)

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

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)

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

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.

5.5. Ongoing Monitoring

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

Red flags include:

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

Monitoring thresholds:

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

5.6. Reporting of Unusual Transactions

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

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.

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.

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

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

5.7. Reliance on Third Parties

Our company engages Sumsb for CDD measures. Sumsb is a third-party identity verification and compliance platform used to verify player identities and ensure compliance with KYC) and AML 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/>

5.8. Anti-Money Laundering Compliance Program

The AML Compliance Program is risk-based and structured to effectively identify, assess, and mitigate the risks of ML/TF that the organization may encounter. The program establishes minimum compliance standards in accordance with the laws and regulations of Curaçao, ensuring that all business activities are conducted with integrity, transparency, and accountability.

The AML Program encompasses governance measures, employee training, customer due diligence procedures, transaction monitoring, and independent internal audits to ensure continuous compliance and the early detection of suspicious activities. It also includes a defined Account Blocking Procedure, which outlines the steps to be taken when there is suspicion or reasonable grounds to believe that an account is being used for ML or TF activities.

Under this procedure, when suspicious activity is detected through automated monitoring systems or reported by employees, the Compliance Department

conducts an immediate review to verify the grounds for suspicion. If the suspicion is substantiated, the account is promptly restricted or blocked to prevent further transactions. The organization then files a Suspicious Transaction Report (STR) with the FIU Curaçao and maintains full documentation of the investigation and actions taken. Account reactivation, if applicable, may only occur following a compliance review and formal authorization by the Chief Compliance Officer (CCO).

The CCO is responsible for the implementation, oversight, and continuous enhancement of the AML Program, ensuring that compliance testing, reporting, and escalation processes are properly executed. The CCO must also provide periodic reports to the Board of Directors detailing program performance, identified risks, remedial measures taken, and account-blocking actions executed under the AML framework.

6. Compliance and Consequences of Non-Compliance

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

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

Positive matches trigger immediate account freezes and reporting to the FIU. The Company follows Curaçao's asset-freezing procedure as per the 2016 National Gazette directive.

7. Related Information

This policy is based on the following legislation and regulatory instruments:

- 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)
- FATF Recommendations

8. Contact Information

Compliance Department – Code Harbor N.V.

Email: compliance@wildwinz.com

9. Policy History

Version: 1.4

Previous policy date: 06.2025

Key updates include refined language, alignment with CGA guidance, and expanded clarity on monitoring and reporting processes.

10. Policy URL

https://wildwinz.com/aml_policy/