

Code Harbor N.V.

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

Approving Official(s):	Yevhen Dyba	Signature: 	Date: 04.05.2026
Responsible Office	Compliance Department		
Effective Date	04.05.2026		
Next Review Date:	03.05.2027		

Table of Content

1. Policy Statement.....	3
2. Purpose.....	3
3. Scope and Applicability.....	4
4. Definitions and Framework.....	4
5. Governance and Compliance Structure.....	6
6. Policy Implementation.....	7
6.1 Business Risk Assessment.....	7
6.2 Customer Risk Assessment.....	8
6.3 Customer Acceptance Policy.....	9
6.4 Customer Due Diligence.....	9
6.5 Ongoing Monitoring.....	12
6.6 Reporting of Unusual Transactions.....	12
6.7 Reliance on Third Parties.....	13
6.8 Anti-Money Laundering Compliance Program.....	14
6.9 Sanctions Compliance.....	15
6.10 Recordkeeping.....	17
6.11 Training and Awareness.....	17
6.12 Audit and Review.....	17
7. Compliance and Consequences of Non-Compliance.....	18
8. Related Information.....	19
9. Contact Information.....	19
10. Policy History.....	19
11. Policy URL.....	20

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, and is aligned with the Regulations for the Combating of Money Laundering, the Financing of Terrorism and Proliferation of Weapons of Mass Destruction (January 2025). The Curaçao Gaming Control Board (GCB) is the designated supervisory authority for AML/CFT compliance in the gaming sector and issued those Regulations; references in this policy to the CGA as the gaming regulator should be read together with the CGA's role as the AML/CFT supervisory authority.

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.

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.

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. 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. Scope and Applicability

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. Governance and Compliance Structure

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.

The Chief Compliance Officer is a senior officer at management level, independent of the gaming operations, and meets the CGA fit-and-proper and competence requirements: at least two years of AML/CFT compliance experience in a reporting role together with a bachelor's degree or a CGA-recognised AML certification (e.g. CAMS or AMLFC), or at least four years of AML/CFT compliance experience. The CCO undertakes a minimum of 10 hours of AML-related training annually and has knowledge of NOIS, NORUT and CGA AML regulations, including EU and OFAC sanctions screening.

The CCO role is not combined with the functions of UBO, CEO, CFO, COO, Casino Manager or Slot Manager, with any other operational function, or with the internal audit function. The CCO has timely access to customer identification and CDD data, transaction records and all other relevant information, and is able to act independently

The CCO is accountable to the Board.

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

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

Prior to appointment, the Company shall conduct appropriate screening of employees, contractors, and Key Persons whose roles may expose the Company to ML/TF risks. Screening measures shall be proportionate to the function and may include identity verification, verification of employment history, assessment of professional qualifications, and integrity checks, including criminal background screening where legally permissible.

Employees shall be required to disclose any conflicts of interest or circumstances that may impair their integrity or independence. The Company reserves the right to reassess employee suitability on an ongoing basis, particularly when an employee is promoted, transferred to a sensitive role, or where new risk indicators arise.

The Company shall cooperate fully and transparently with the Curaçao Gaming Authority and other competent supervisory and investigative authorities. This includes the timely provision of information, documents, records, and reports requested in the context of licensing supervision, AML/CTF oversight, inspections, or investigations.

The Company shall notify the CGA without undue delay of any material AML/CTF breaches, significant compliance incidents, or systemic deficiencies that may affect the safe, responsible, transparent, and reliable offering of games of chance, in accordance with LOK requirements.

6. Policy Implementation

6.1 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.

The Business Risk Assessment - including the methodology applied, the rationale for each low/medium/high risk rating, the outcome, and the information sources used - is documented and approved by the Board of Directors, and is made available to the CGA on request.

6.2 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.

6.3 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.

6.4 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. For legal persons, identification and verification covers every natural person holding 25% or more of the shares or voting rights, or otherwise exercising ultimate effective control; where no such natural person can be identified, the senior managing official is identified and verified.
- 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

Prior to reaching the XCG 4,000 (EUR 2,000) threshold, the Company applies a minimum level of CDD measures simultaneously with account registration, regardless of the risk profile. At a minimum, the following information must be collected from every player at the point of account opening, before any financial transactions take place:

- Full name
- Date of birth
- Permanent residential address
- PEP status and sanctions screening (conducted simultaneously with registration)

Once the XCG 4,000 (EUR 2,000) threshold is reached, full CDD must be completed before the player may make further deposits or withdrawals. Simplified Due Diligence (SDD) may only be applied in clearly documented low-risk scenarios and must never be applied where there is any suspicion of ML/TF/PF. The XCG 4,000 (EUR 2,000) threshold is calculated on a daily basis, taking into account all deposits and withdrawals made by the player since the establishment of the business relationship, including any peer-to-peer transfers; transactions that are individually below the threshold but cumulatively meet or exceed it are treated as linked transactions. Full CDD comprises, at a minimum, the full identification data set (full name, date of birth, place of birth, permanent residential address, nationality, and identity document number), verification of identity against a reliable independent source, identification and verification of any beneficial owner, and PEP and sanctions screening. In clearly documented low-risk scenarios, identification may be limited to full name, date of birth and permanent residential address.

30-Day Rule for CDD Non-Compliance. If a player reaches the XCG 4,000 (EUR 2,000) threshold and the required CDD documentation and information is not received within 30 days from that point, the Company is obligated to terminate the business relationship with that player. Where the XCG 4,000 (EUR 2,000) threshold was reached due to a deposit, the player may not make further deposits or withdraw funds; however, they may continue playing with funds already in their account. Where the threshold was reached due to 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 does exist, the matter must be reported to the FIU Curaçao via the goAML portal, and internal procedures shall determine whether funds are to be blocked or returned, taking into account the risk of tipping off the player.

Politically Exposed Persons (PEP) - Enhanced Procedures. Where a player is identified as a PEP, or as a family member or close associate of a PEP, the following four mandatory steps must be applied:

(a) Detection system. The Company maintains appropriate risk-management systems and automated screening tools to identify whether a customer or beneficial owner qualifies as a PEP at the point of onboarding and on an ongoing basis throughout the business relationship. PEP screening is conducted simultaneously with sanctions screening at account registration, and re-screening is performed regularly thereafter.

(b) Senior management approval. Prior to establishing or continuing a business relationship with a PEP, written approval must be obtained from senior management or the Chief Compliance Officer. This requirement applies both to new PEP customers at onboarding and to existing customers who are subsequently identified as PEPs. No PEP account may be activated or maintained without this documented authorisation.

(c) Source of wealth and source of funds. The Company must take reasonable measures to establish both the source of wealth (the origin of the PEP's accumulated assets over their lifetime) and the source of funds used in specific transactions. The player must provide a declaration regarding their source of funds, which the Company verifies against independent and reliable sources, including public records where available. Where public sources are insufficient, additional documentation may be requested from the customer.

(d) Enhanced ongoing monitoring. PEP accounts are subject to a heightened level of transaction scrutiny and more frequent review of the business relationship. Any deviation from the established customer profile or expected activity pattern must be

investigated promptly and, where warranted, reported to the FIU Curaçao via the goAML portal.

30-Day Rule for Newly Identified PEPs. If a player who was not identified as a PEP at onboarding subsequently acquires PEP status, the Company must implement all four measures described above within 30 days of identifying the change in status. Failure to complete this process within the 30-day window requires the Company to terminate the business relationship with that customer. If a PEP or sanctioned individual is identified at any stage, the relevant account is immediately restricted. The CCO evaluates whether to freeze funds and will report the matter to the FIU Curaçao via the goAML portal. All asset-freezing actions are carried out in accordance with the procedure published in the National Gazette on 16 September 2016.

6.5 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 or withdrawals reaching XCG 5,000 (EUR 2,500) (threshold for reporting of unusual transactions per NORUT)
- Multiple failed verification attempts

6.6 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

In addition to internal red flags, the Company applies the official objective and subjective indicators of unusual transactions as established under the Ministerial Decree on Indicators of Unusual Transactions (N.G. 2015, no. 73), as amended from time to time.

Objective indicators include transactions that meet legally defined thresholds or patterns requiring mandatory reporting, irrespective of suspicion. Subjective indicators include transactions or behavior that give rise to reasonable grounds to suspect money laundering, terrorist financing, or proliferation financing, based on the employee's knowledge, experience, and the customer's risk profile.

All employees must apply these indicators in conjunction with internal monitoring rules and promptly escalate any identified unusual transaction to the CCO for assessment and potential reporting to the FIU Curaçao.

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.

6.7 Reliance on Third Parties

The Company engages Sumsub as its third-party identity verification and AML compliance provider. Sumsub performs document verification, biometric (selfie) checks, sanctions screening, and PEP status screening on behalf of the Company as part of the CDD process at player registration and on an ongoing basis. Further information about Sumsub is available at: <https://sumsub.com/>

Notwithstanding the reliance on Sumsub, the ultimate responsibility for CDD compliance remains with the Company at all times. The engagement of a third-party provider does not transfer legal or regulatory accountability. The Company retains full responsibility for the customer risk assessment, the determination of PEP status, the decision whether to establish or continue a business relationship, and the conduct of ongoing monitoring.

The Company has a data processing and service agreement with Sumsb that requires: (i) the immediate provision to the Company of all identification data and CDD documentation collected in the course of verification; (ii) the availability of such records upon request by the Company, the CGA, the FIU Curaçao, or other competent authorities; and (iii) periodic testing of this arrangement to confirm it functions as documented. The Company verifies on an ongoing basis that Sumsb is duly licensed, regulated, and supervised in its jurisdiction of operation, and that Sumsb's internal AML/CTF policies, procedures, and controls meet the standards required under Curaçao law and the CGA Regulations. Any material change in Sumsb's regulatory status or compliance posture must be assessed by the CCO and, if necessary, result in a review of the third-party arrangement.

6.8 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/PF 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.

6.9 Sanctions Compliance

As part of its AML/CTF compliance obligations, the Company conducts systematic sanctions screening of all players (and, where an account is held by or funded on behalf of a legal person, of its Ultimate Beneficial Owners, directors and senior management), both prior to establishing a business relationship and on an ongoing basis thereafter. Sanctions are legally enforceable measures adopted by the international community to address financial crime, terrorism, and the financing of proliferation. Their purpose is to alter the conduct of targeted states, regimes, or individuals when other diplomatic channels have proved insufficient. Such measures may encompass restrictions on trade, financial services, economic resources, or international movement.

The Company adheres to all applicable sanctions frameworks, including those administered by the United Nations, the European Union, the United Kingdom, the United States (OFAC), and Australia. No business relationship, transaction, or service may be established or maintained with any individual, legal entity, or jurisdiction appearing on any of these lists. Where a confirmed match is identified, the relevant account is immediately restricted, assets are frozen in accordance with applicable law, and the matter is escalated to the Financial Intelligence Unit Curaçao (FIU) via the goAML portal. National-level designations are also monitored and applied where relevant.

UN Sanctions

The UN Security Council maintains a consolidated register of individuals and entities subject to targeted financial measures, primarily in connection with ISIL (Da'esh), Al-Qaeda, the Taliban, and broader terrorist activity under Resolution 1373. Member states carry a binding obligation under international law to freeze the assets of listed parties and to notify competent authorities of any potential matches. The Company treats UN designations as mandatory prohibitions regardless of the counterparty's jurisdiction of incorporation.

The UN consolidated sanctions list is publicly accessible at: <https://www.un.org/securitycouncil/content/un-sc-consolidated-list>

EU Sanctions

The European Union introduces restrictive measures under its Common Foreign and Security Policy (CFSP) framework as established by the Treaty on European Union. EU measures may mirror existing UN Security Council designations or reflect autonomous EU determinations where a distinct foreign policy rationale is present. Autonomous EU

measures cannot be directed at individuals or entities in the absence of such a foreign policy dimension. The EU consolidated sanctions map is accessible at: <https://www.sanctionsmap.eu/#/main>

UK Sanctions

Following its departure from the European Union, the United Kingdom operates an independent sanctions programme administered by the Office of Financial Sanctions Implementation (OFSI). The Company does not establish or maintain any commercial or financial relationship with individuals, organisations, or jurisdictions listed under the UK sanctions regime. The current designations are published by OFSI at: <https://www.gov.uk/government/organisations/office-of-financial-sanctions-implementation>

OFAC Sanctions

OFAC, operating under the US Department of the Treasury, implements and enforces targeted economic and trade measures in support of US national security and foreign policy objectives. Its designations cover foreign governments, terrorist organisations, narcotics networks, and entities linked to weapons proliferation. Although OFAC jurisdiction formally extends to US persons and entities, non-US companies conducting transactions denominated in US dollars may also fall within its reach, given that USD clearing operations route through US correspondent banks in New York, thereby engaging US jurisdiction over the transaction.

OFAC maintains the Specially Designated Nationals (SDN) List, identifying individuals and entities whose assets are subject to blocking measures and with whom dealings are generally prohibited. The SDN List search tool is available at: <https://sanctionssearch.ofac.treas.gov/>

Australia Sanctions

Australia administers its own autonomous sanctions programme through the Department of Foreign Affairs and Trade (DFAT). The Company does not enter into any contractual, financial, or operational arrangement with individuals, entities, or jurisdictions appearing on the Australian consolidated sanctions list. The list is maintained and publicly accessible at: <https://www.dfat.gov.au/international-relations/security/sanctions/consolidated-list>

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

6.10 Recordkeeping

The Company shall maintain complete, accurate, and up-to-date records relating to customer identification, verification, risk assessments, transactions, monitoring activities, internal and external suspicious activity reports, sanctions screening results, employee training, and audit findings.

Records shall be retained for a minimum period of five (5) years after the termination of the business relationship or completion of the transaction, or longer where required by applicable law or instructed by the CGA or FIU Curaçao.

All records shall be stored securely, protected against unauthorized access or alteration, and shall be made available without delay to competent authorities upon lawful request.

6.11 Training and Awareness

All relevant staff receive AML/CFT training upon hiring and annually thereafter. These training sessions are conducted periodically and are tailored to the specific needs of staff, based on the latest regulatory developments and best practices in the industry. Training includes, but not limited:

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

Training is tailored to the function of each group of staff and covers, at a minimum: new employees (general nature of ML/TF/PF and internal reporting obligations); front-line, customer-facing staff (how the platform may be misused and how to recognise and escalate suspicious activity); audit staff; AML compliance staff; supervisors and managers; and senior management and the Board.

The Company maintains training records that include the content of each training programme, the names of staff trained, the dates of training, the results of any testing of staff understanding, and an ongoing training plan. These records are made available to the CGA on request.

6.12 Audit and Review

Independent audits of the AML program are conducted annually. The audit shall be conducted by a qualified internal audit function that is operationally independent from

the Compliance Department or by an external independent auditor with demonstrable AML/CTF expertise.

The scope of the audit shall include, at a minimum, the effectiveness of customer due diligence measures, transaction monitoring systems, reporting of unusual transactions, sanctions compliance, record-keeping practices, employee training, and overall adherence to applicable laws and CGA regulations.

Audit findings, conclusions, and remediation recommendations shall be documented in writing and submitted to the Board of Directors and the Chief Compliance Officer. Identified deficiencies shall be addressed without undue delay, and corrective actions shall be tracked until full remediation is achieved.

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.

The internal or external auditor performing the AML/CFT audit must be independent of the Compliance Department and must hold relevant qualifications comprising at least two years of AML/CFT compliance experience together with a relevant degree and an AML certification recognised by the CGA (such as CAMS or CAMS-Audit from ACAMS, or the AMLFC certification from the AML Foundation & Compliance Institute).

7. 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 applicable sanctions lists as described in section 6.9 of this Policy.

Where serious or repeated non-compliance with this Policy is identified, the Company may take immediate remedial action, including suspension of duties, restriction of

system access, or termination of employment or contractual relationships, in accordance with applicable labor and contractual laws.

In the case of customers, the Company may suspend or terminate the business relationship, block accounts, refuse transactions, and report the matter to the FIU Curaçao or other competent authorities, where required or deemed appropriate.

All termination decisions related to AML/CTF non-compliance shall be documented, justified, and approved by senior management or the Board, as applicable.

8. 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)
- Ministerial Decree on Indicators of Unusual Transactions (N.G. 2015, no. 73)
- FATF Recommendations

9. Contact Information

Compliance Department - Code Harbor N.V.

Email: compliance@wildwinz.com

10. Policy History

Version: 1.6

Previous policy date: 15.12.2025

Version 1.6 - Policy adapted to CGA AML/CTF Regulations (January 2025); sections updated to reflect CGA template requirements, extended sanctions compliance section

(UN, EU, UK, OFAC, Australia), enhanced CDD and PEP procedures including 30-day rules, expanded third-party reliance section (Sumsb), and alignment with FATF Recommendations.

11. Policy URL

https://wildwinz.com/aml_policy/