

ZENO CLUB B.V.

AML/KYC POLICY

I. AML Policy

(Anti Money Laundering)

INTRODUCTION

This anti-money laundering (AML) and know your customer (KYC) policy that is applicable to all staff to help prevent and detect potential money laundering or terrorist financing activity. The Company takes a zero-tolerance approach to money laundering, terrorist activity and other such financial crimes.

Zeno Club B.V., Curaçao registration number: 154987 (hereinafter referred as “Company”) will actively participate in preventing the services of the Company on all Company platforms from being exploited by criminals and terrorists for money laundering or terrorist financing purposes.

This Policy applies to all Company employees, as well as agents, contractors, and third-party service providers involved in the provision of services under the Company’s license.

The Policy has been developed in accordance with applicable Curaçao legislation, including the National Ordinance on the Identification of Clients when Rendering Services (NOIS), the National Ordinance on the Reporting of Unusual Transactions (NORUT), the Sanctions National Ordinance, the Kingdom Sanctions Act, and guidance issued by the Curaçao Gaming Control Board (GCB). It also aligns with the FATF Recommendations and international AML/CTF standards.

The Company applies a risk-based approach, identifying and mitigating money laundering and terrorist financing risks based on the level of risk presented by customers, products, services, delivery channels, and geographic exposure.

The objectives of this policy are:

- ensuring the Company’s compliance with all applicable laws, statutory instruments of regulation, and requirements of the Company’s supervisory body;
- protecting the Company and its staff as individuals from the risks associated with breaches of the law, regulations and supervisory requirements;
- preserving the good name of the Company against the risk of reputational damage presented by implication in money laundering and terrorist financing activities;
- making a positive contribution to the fight against crime and terrorism.



DEFINITIONS (GLOSSARY)

Term	Definition
AML	Anti-Money Laundering
CTF	Counter-Terrorism Financing
CFP	Counter-Financing of Proliferation
CDD	Customer Due Diligence
EDD	Enhanced Due Diligence
CRA	Customer Risk Assessment
BRA	Business Risk Assessment
SAR	Suspicious Activity Report
FIU	Financial Intelligence Unit Curaçao
GCB	Gaming Control Board Curaçao
PEP	Politically Exposed Person
MLRO	Money Laundering Reporting Officer
NRA	National Risk Assessment
goAML	Electronic reporting portal maintained by FIU Curaçao
CAP	Customer Acceptance Policy – criteria for onboarding or rejecting a customer
High-Risk Jurisdiction	Country identified by FATF, OFAC, EU or Curaçao law as high risk

1.1 ANTI-MONEY LAUNDERING

Money Laundering is the process of creating the appearance of funds obtained from criminal activity, being originated from a legitimate source. Criminals attempt to launder money by disguising the source and/or changing the form of the funds, or moving them to a place where they are less likely to attract attention.

Anti-money laundering (AML) is a term used to describe the legal controls that require financial institutions and other regulated entities to prevent, detect, and report Money Laundering activities.

An effective AML program requires a jurisdiction:

- to have criminalized Money Laundering;
- to have given the relevant regulators and police the powers and tools to investigate it;
- to have its institutions identify their customers, establish risk-based controls, keep records and report suspicious activities;
- to be able to share information with other jurisdictions as appropriate.

In the jurisdiction of Curaçao, AML requirements applicable to the gaming sector are primarily derived from:

- the National Ordinance on the Identification of Clients when Rendering Services (NOIS),
- the National Ordinance on the Reporting of Unusual Transactions (NORUT),
- the Sanctions National Ordinance and the Kingdom Sanctions Act,
- the Guidelines and Regulations issued by the Curaçao Gaming Control Board (GCB),
- and international AML/CTF standards established by the Financial Action Task Force (FATF).

In line with these requirements, the Company implements a **risk-based approach** to AML compliance. This includes conducting a Business Risk Assessment and individual Customer Risk Assessments to identify, assess and mitigate the risks of money laundering, terrorist financing, and financing of proliferation. The Company is committed to reviewing and updating these assessments on an ongoing basis.

2. REGULATION

Employees working in the remote gaming industry are required to make a report in respect of information that comes to them in the course of their business:

- when they know;
- when they suspect;
- when they have reasonable grounds for knowing or suspecting that a person is engaged in money laundering or terrorist financing, including criminal spend.

These obligations are collectively referred to as grounds for knowledge or suspicion. What the authorities are looking for is that we are able to demonstrate, with supporting evidence, that a risk assessment is and has been undertaken prior to entering into business relationships with customers



and that adequate customer due diligence is conducted in order to ensure that customers' transactions are consistent with the level of risk presented.

In accordance with guidance from the Curaçao Gaming Control Board, any single transaction or a combination of related transactions reaching or exceeding NAf. 5,000 (approx. EUR 2,490) must be reported as an unusual transaction to the FIU Curaçao, regardless of other risk indicators. This includes deposits, withdrawals, or transfers executed on a single day or in one gaming session.

In this document, we have identified measures that are being applied in order to carry out risk monitoring and the need of where we would require a Declaration of the source of funds from customers in situations which present a high risk and potentially money laundering.

In compliance with the **National Ordinance on the Identification of Clients (NOIS)** and the **National Ordinance on the Reporting of Unusual Transactions (NORUT)**, the Company must ensure that all customers are subject to appropriate **Customer Due Diligence (CDD)** measures. This includes but is not limited to:

- identification and verification of the customer's identity;
- identification and verification of the beneficial owner (if applicable);
- understanding the purpose and intended nature of the business relationship;
- and conducting **ongoing monitoring** of the business relationship and transactions.

These CDD measures must be applied:

- when establishing a business relationship;
- when carrying out occasional transactions equal to or exceeding **NAf. 4,000**;
- when there is suspicion of money laundering or terrorist financing, regardless of the amount;
- or when there are doubts about the veracity or adequacy of previously obtained customer identification data.

Where the required information cannot be obtained or verified, the Company is obliged to **terminate the business relationship**, refrain from executing the transaction, and consider filing a report with the Financial Intelligence Unit (FIU) Curaçao.

If the NAf. 4,000 threshold is reached but the customer has not completed full verification, the Company shall immediately restrict any further deposits or account top-ups. The customer may only use existing balance for gaming purposes. In the event the customer initiates a withdrawal request under these circumstances, the Company shall fully freeze the account until all verification steps are completed.

3. AML POLICY PRINCIPLES

AML policy is based on principles and practices:

- we develop systems and controls that are appropriate for our businesses and comply with legal and regulatory requirements;
 - we assess the AML risks inherent in our current business at least annually; we then adopt a risk-based approach that is flexible, effective, proportionate and cost effective;
 - we have full commitment for this from, and responsibility resting with, senior management;
 - we regularly assess the adequacy of our systems and controls;
 - we maintain, where necessary, records of transactions that meet the needs of law enforcement investigations tackling money laundering and terrorist financing;
- 

- we provide initial and ongoing training for all relevant employees.

The Company's AML policy and the procedures supporting it are reviewed and approved by the **Board of Directors** and the **designated Compliance Officer**, and are subject to revision in case of material business changes or updates to Curaçao legislation and regulatory guidance.

All AML-related systems and internal controls are **documented**, regularly tested, and improved where necessary. This includes transaction monitoring systems, customer risk assessment methodology, due diligence procedures, and escalation protocols.

The Company ensures that its AML program is implemented consistently across all departments and that employees understand their roles and responsibilities within the AML framework.

4. RISK MANAGEMENT

We have a policy and procedures in relation to risk assessment and management, as required under the Money Laundering Regulations (the Regulations). This risk-based approach involves a number of discrete steps in assessing the most proportionate way to manage and mitigate the money laundering and terrorist financing risks we face:

- identify the money laundering and terrorist financing risks that are relevant to us;
- design and implement policies and procedures to manage and mitigate these assessed risks;
- monitor and improve the effective operation of these controls;
- record what has been done, and why.

In line with the Curaçao AML/CFT framework and the guidelines issued by the Gaming Control Board, the Company maintains two types of documented assessments:

- Business Risk Assessment (BRA):

This is conducted **at least annually**, or whenever there are material changes in operations (such as the introduction of new products, payment methods, or jurisdictions). The BRA identifies and evaluates the risks related to products and services, delivery channels, customer types, and geographic exposure.

The BRA is **approved by the Board of Directors** and must be made available to the GCB upon request.

- Customer Risk Assessment (CRA):

A CRA is conducted **prior to establishing a business relationship** or carrying out an occasional transaction. It determines the individual customer's risk level (low, medium, high) and defines the applicable level of due diligence, including potential enhanced due diligence measures.

Both BRA and CRA take into account:

- the Company's internal data and customer behavior;
- applicable outcomes of the National Risk Assessment (NRA);
- guidance from the FATF and Curaçao Gaming Control Board;
- emerging risks from new technologies or delivery mechanisms.

During onboarding, the Company also collects and verifies the following minimum information: full name, permanent residential address, date of birth, place of birth, nationality, and a unique identification number (e.g., passport or national ID). This applies to both individuals and legal entities. Where applicable, beneficial owners holding 25% or more of shares, or controlling persons, must be identified and verified.

The Company monitors its product offerings and payment methods for potential ML/TF risks. The following are considered high-risk indicators:

- Use of anonymous payment methods, such as prepaid cards or certain virtual assets
- Use of third-party bank accounts or cards
- Rapid deposit and withdrawal without gameplay
- Use of multiple casino wallets or game accounts
- Peer-to-peer transfers between customer accounts
- Changes in funding channels or creation of new bank accounts
- Use of stolen identities or payment credentials
- High reliance on e-wallets without clear source of income

Customers exhibiting these patterns are subject to enhanced scrutiny and may be flagged for EDD or escalation to the Compliance Officer.

In addition, the Company evaluates **technological developments** for potential ML/TF vulnerabilities before launching any new product, platform feature, or delivery channel.

The Company applies a documented Customer Acceptance Policy to determine whether to onboard, maintain, or terminate business relationships based on AML/CTF risk.

The following customer categories are **refused or subject to mandatory Enhanced Due Diligence**:

- Customers from **high-risk jurisdictions** as defined by FATF, OFAC, or Curaçao law
- Customers refusing to provide satisfactory KYC documentation
- **PEPs** without clear source of funds or wealth
- Customers associated with known criminal activity or sanctioned individuals
- Customers using **anonymous or third-party payment methods**
- Customers who create multiple accounts to bypass controls

The Company reserves the right to refuse onboarding or to terminate an existing customer relationship at its sole discretion if AML/CTF risks cannot be adequately mitigated.

The Company conducts an internal audit or independent assessment of its AML/CFT compliance framework **at least once per year**, or following any material change in operations, regulatory environment, or risk profile.

The audit shall include, but is not limited to:

- Evaluation of the implementation of AML/CFT policies and procedures
- Effectiveness of transaction monitoring and reporting systems



- Review of training records, staff awareness and responsibilities
- Sampling of customer files and SAR handling procedures
- Testing of access control to AML-sensitive systems
- Review of third-party compliance in delegated KYC/CDD functions
- Verification of record-keeping adequacy and retention periods

Findings are reported directly to senior management and used to improve the AML/CFT framework. Corrective actions are documented and tracked until resolution.

5. SUSPICIOUS ACTIVITY

Suspicious Activity in this case is being referred to as suspicious transactions, extreme player profiles, when deposits are not matching up amongst other elements. Other concrete examples of how we identify players who require our team to undertake a risk monitoring approach of our customers and when to specifically carry out enhanced due diligence checks on the Player Profiles can be further required:

- Passport or ID card.
- Utility bill.
- Bank statement.
- Any other proof of identity.

The Enhanced Due Diligence Checks are subject to players' profile and the amount of Risk they pose to us. Only when we determine some of the above points or a combination of a few will we flag the customer/customers in question and conduct risk monitoring. This will include checks of where the customer works, value of his/her real estate or other property, where the customer lives and checks to see whether the value of the house is logical compared to the customers spending.

5.1 Suspicious Activity Reports SARs

Within that framework, Suspicious Activity Reports (SARs) are an imposed requirement. The Company ensures that any employee reports to the Risk Team where they have grounds for knowledge or suspicion that a person or customer is engaged in money laundering or terrorist financing.

Escalations of SARs should be done in a confidential, discreet manner, in a handwritten form and not via email so as to ensure maximum anonymity.

All employees are **prohibited from disclosing** to the customer or to any third party that a report has been or will be made. Such disclosure (known as "tipping off") is strictly forbidden and constitutes a criminal offence.

The Company is **registered with the goAML reporting portal** operated by FIU Curaçao and uses it to submit external reports electronically. Reports are made **without delay** once an unusual transaction is confirmed.

The Compliance Officer is responsible for reviewing all internal reports and deciding whether they must be submitted to the FIU. The officer maintains records of:

- internally submitted reports;
- reports filed externally via goAML;
- supporting documents and notes relating to the transaction or player profile;

- reasons for not reporting externally (if applicable), which must be signed and retained.

If appropriate, the Compliance Officer may initiate **freezing of the player account** in accordance with internal procedures, taking into account the risk of tipping off. All actions related to the SAR must be properly documented.

5.2 Working Procedure

The Company reviews players' spend and gameplay to check for suspicious activity. Before any withdrawal is processed the following procedures are carried out:

- a) The customer's deposit history is reviewed to confirm that no suspicious payments have been made to the customer's account. The frequency and amount of deposits are checked to ensure they are within normal range for the customer based on his depositing history and the general depositing range throughout our network.
- b) The customer's turnover is reviewed to ensure that they have played in the casino and are not using the Company as a method to move money.
- c) When possible, funds must always be refunded back to the original payment method used by the player to make a deposit. See Terms & Conditions for more information.

5.3. WITHDRAWAL AND REFUND POLICIES

5.3.1. Withdrawals:

When withdrawing funds, the Company may request additional information from the user to confirm the identity of the user and the ownership of his/her account for withdrawal of funds. For example, the Company has the right to request a photo of a user with an open passport against the background of his face (the document should be readable) and photo of the bank card on the front side (5 first and 4 last digits, owner's name and date of expiry shall be readable) and similar documents and information. The User must provide the documents and information requested by the Company within a period not exceeding 72 hours, otherwise the withdrawal request will not be executed.

If this is the user's first withdrawal, it may take up to 72 hours for the data to be verified. If the user has previously verified their account and withdrawn funds, subsequent withdrawals will be made without delay within 24 hours, unless circumstances arise as provided by the AML and/or the law and require additional verification of the user's identity, bank card ownership or risk management by analysis of gaming behavior.

In such cases, **withdrawals will be suspended until completion of verification**, which may take up to 72 hours from the moment all required documents and information have been received. In cases presenting a higher ML/TF risk, including but not limited to irregular gaming activity, usage of third-party payment methods, or detection of possible structuring, the Company may extend the review period up to 30 days and temporarily **freeze the account** in accordance with internal AML procedures.

Upon receipt of a withdrawal request, the Company will only process withdrawals via the same **payment methods previously used by the player to deposit** (either individually or by group of



users – by currency, residence country, or other risk-based criteria). No withdrawal will be processed to a third-party account.

When deposits were made using combined payment methods (e.g. multiple virtual assets and/or currencies), the Company retains the right to return funds in one of the currencies or virtual assets previously used, at its discretion, based on risk factors and operational constraints.

All documentation collected during the verification process will be stored in accordance with Curaçao AML record-keeping obligations (minimum 5 years).

In line with Curaçao regulatory expectations, if the customer fails to submit the requested KYC documents within thirty (30) days of reaching the NAf. 4,000 threshold, the Company shall terminate the business relationship and consider filing a report to the FIU Curaçao. If there is no suspicion of ML/TF, any remaining funds must be returned to the original payment method used.

5.3.2. Refund:

A refund can be requested by the user from the moment funds are credited to the user's account. To make a refund, the user must submit a refund request to the Company's support service and attach a photo with an open passport against the background of their face (the document should be readable), and a photo of the bank card on the front side (5 first and 4 last digits, owner's name and date of expiry shall be readable), or account details certified by a financial institution confirming ownership.

If the user has not provided all the documents required for the refund within 72 hours from the date of the request, the application will not be processed.

Verification of the provided data may take up to 72 hours, unless AML law or internal policies require additional verification. In such cases, the period extends from the moment all requested information has been received.

The Company also reserves the right to request from the user confirmation of the **source of funds**, including but not limited to:

- proof of earnings (Payslip, Director remuneration, Dividends, Pension);
- bank statement or savings account showing consistent incoming transactions from a clear source;
- a Trust deed demonstrating entitlement to funds;
- dated proof of an award or legal compensation.

Refund requests are processed only upon **successful completion of the full verification procedure**, including evaluation of potential AML risk.

The Company maintains a log of all attempts made to request and collect the required KYC information and documentation. If documents are submitted after account suspension or closure, the Company will assess whether the delay increases the ML/TF risk associated with the customer relationship before reinstating the account. Reluctance to provide documents is not in itself proof of unlawful behavior but shall be treated as a high-risk factor.



6. EMPLOYEES

6.1 Senior Management

Senior management is fully committed to and responsible for the implementation of this policy. Senior management is made aware of their individual personal liability for consenting to, or conniving in, the commission of offences under the Regulations, or where such offence is attributable to any neglect on his part.

Management ensures that the AML program is supported with adequate resources, internal controls, and monitoring tools, and that the policy is reviewed at least annually. Senior management is responsible for formally approving the AML/CFT policy and risk assessments, as required by Curaçao regulations.

6.2 MLRO

A designated Money Laundering Reporting Officer takes responsibility for SARs in respect of the prevention and detection of money laundering, counter terrorism financing and our obligations.

The nominated MLRO has responsibility for:

- making reports to senior management on anti-money laundering (AML) and countering terrorist financing (CTF) activity;
- receiving disclosures from employees;
- and if appropriate, making such external reports to the Financial Intelligence Unit (FIU) Curaçao via goAML.

The MLRO is formally appointed by senior management and acts **independently from gaming operations**. The MLRO must have timely **access to all customer identification and verification data**, transaction history, internal SARs, and business risk documentation.

The MLRO's responsibilities are included in a **written job description**, signed and dated by the officer as confirmation of acceptance. The MLRO must also stay informed on local and international developments in AML/CTF, and suggest policy updates accordingly.

6.3 Staff training

All staff will receive training on their obligations in respect of money laundering reporting and are aware of the procedures in place for escalation of any suspected incidents to the MLRO. As part of this process, staff are made aware that personal disregard for the legal requirements, for example, turning a blind eye to a customer spending criminal proceeds, may result in criminal or regulatory action.

Relevant employees receive training on how to follow house policies and procedures for:

- client due diligence (CDD), including enhanced requirements for high risk clients, which includes PEPs;
- reporting suspicious activity to the nominated officer where necessary, seeking appropriate consent to allow participation in gaming and to conduct gaming and other business transactions.

The Company maintains a **staff training log**, which includes:



- names of staff trained,
- dates and content of training sessions,
- results of any assessments or tests,
- a forward-looking training plan based on role and department.

Refresher training is provided at least annually or when regulatory updates require.

Staff are also trained to recognize when customers attempt to bypass AML controls by splitting transactions, using third-party accounts, or accessing services from high-risk jurisdictions. Practical scenarios involving such risks, including non-face-to-face interactions and fraudulent ID usage, are included in periodic training modules.

7. HIGH RISK JURISDICTIONS

High risk countries are those countries identified as such by publications issued from time to time by the Financial Action Task Force (FATF), or additionally those so identified by the Curaçao Gaming Control Board and the Caribbean Financial Action Task Force (CFATF). Clients registered in High Risk Countries are always subject to Enhanced Due Diligence (EDD).

Players from the FATF list of jurisdictions seen to threaten the international financial system from ongoing and substantial money-laundering or terrorist financing activities, as identified in FATF publications, will be refused.

The Company considers as high risk any jurisdiction that appears on one or more of the following:

- **FATF's "High-Risk Jurisdictions subject to a Call for Action"**
- **FATF's "Jurisdictions under Increased Monitoring"**
- **CFATF Public Statements**
- **Countries sanctioned by the Office of Foreign Assets Control (OFAC)**
- **Countries on the EU Sanctions Map**
- **Countries appearing on Transparency International's Corruption Perceptions Index with critical ratings**
- **Any jurisdiction explicitly listed in Curaçao national law or regulations**

The list of high-risk jurisdictions is maintained by the Compliance Officer and is **reviewed and updated quarterly**, or immediately upon publication of new FATF/CFATF statements or changes in sanctions legislation. The Company also maintains a list of low-risk jurisdictions, used for determining when Simplified Due Diligence may be applied.

In case a player is found to be **residing in or originating from a high-risk country**, the Company will:

- automatically assign a "high-risk" rating to the player profile;
- apply Enhanced Due Diligence (EDD), including verifying source of funds and wealth;
- refuse the business relationship where required by law or internal policy;
- block access to services or withdraw access rights when applicable.

The Company evaluates customers' country of birth, citizenship, and residence for geographic risk. Nationalities associated with jurisdictions listed by FATF, OFAC, EU, or Transparency International's Corruption Perception Index are flagged for review. The Compliance Officer maintains an updated risk map incorporating these data points.

8. RECORD KEEPING

We ensure that there is an audit trail to assist in any financial investigation by a law enforcement body.

In accordance with the AML/CFT regulations applicable in Curaçao, the Company maintains comprehensive records of its customers and transactions, ensuring that:

- all records are **retained for a minimum of five (5) years** after the end of the business relationship or the date of the transaction, whichever is later;
- records are stored securely and are accessible to the **Compliance Officer** and competent authorities upon request;
- documents are kept in a manner that allows for the **reconstruction of individual transactions**, including the origin, nature, and destination of the funds.

The Company keeps:

- **customer identification data and verification documents** (e.g. passport, utility bills, bank cards);
- **copies of Customer Due Diligence (CDD) and Enhanced Due Diligence (EDD)** checks and supporting materials;
- **records of transactions**, both deposit and withdrawal, regardless of whether they are linked to gaming activity or not;
- **internal and external Suspicious Activity Reports (SARs)** and all related internal communication or documentation;
- **business correspondence** (including customer support conversations, risk assessments, and any AML-related escalation);
- **a log of account status** (open/closed/frozen), including changes and justifications.

All records may be stored electronically, provided that integrity, readability, and retrievability are preserved.

9. OFFENCES

All employees are made aware of their risk of committing the following related offences:

- **Failing to report suspicious activity:** where an employee fails to comply with the obligation to make disclosures to the nominated officer as soon as practicable after obtaining relevant information, they may be subject to criminal prosecution.
- **Tipping off:** employees may commit an offence if they disclose information that a Suspicious Activity Report (SAR) has been submitted, or disclose the fact that an investigation is being conducted, in a way that is likely to prejudice that investigation.
- **Obstruction or sabotage of an investigation:** employees and other associated persons commit an offence if they knowingly falsify, conceal, destroy, or dispose of documents which are relevant to an AML/CTF investigation, or otherwise hinder a competent authority's ability to conduct an effective investigation.
- **Corporate liability:** the Company as a legal entity may also be held criminally or administratively liable for failures to implement adequate AML/CFT controls, including failure to appoint a Compliance Officer, conduct proper due diligence, or report suspicious activities as required under the Curaçao AML/CFT legislation.



All employees and representatives are expected to cooperate fully with the Company's internal procedures and any external investigation conducted by the authorities.

However, where an employee or the Company acts **in good faith and in compliance with applicable procedures and policies**, they shall be **protected from criminal or civil liability** for reporting suspicions or filing SARs, even if the reported activity ultimately turns out to be lawful.

10. VETTING PROCEDURES FOR NEW EMPLOYEES

The Company undertakes a number of vetting procedures when staff are employed. We will ensure the employee is not a minor through proper identification checks. We will also look to verify any further personal information or background information, and screen for criminal records where permitted by applicable law.

Each new employee must confirm in writing their understanding of the Company's AML/CFT obligations and agree to follow all compliance procedures.

11. PROTECTING OUR EQUIPMENT FROM INTERNAL CRIME AND CRIMINAL MISUSE

The company is very aware that a key way to combat fraud is to first identify where the company's most valuable assets are. Processes and controls have been built into the routine business of the company to minimize the chances of any of the key assets being misused.

Our server equipment are located at Curacao who have in place necessary policies around protection of equipment, for example, a visitors management procedure, fire alarms, shredding of confidential documents, locked cabinets, testing, a security team etc. Company also implements such policies at our offices.

Access to critical systems and infrastructure is considered a part of our AML internal control framework, and is reviewed as part of the Company's internal audit procedures. All equipment and data systems relevant to customer transactions, identity verification, and AML monitoring are protected from unauthorized internal or external access.

12. ENSURING THE COMPANIES WE DEAL WITH ARE TRUSTWORTHY AND REPUTABLE

The Company promotes strong principles of business and professional ethics at every level. When selecting suppliers, there are a number of criteria we consider:

- financial strength (for long term sustainability);
- legal and regulatory compliance;
- commitment to a wider corporate responsibility program; and
- desire and ability to deliver quality and value.

All new suppliers must go through a rigorous approvals process where all information put forward by them is verified.

This information is then assessed internally to consider the risks associated with the supplier; taking into account all of the above criteria. If rejected, the supplier will be informed. The Company ensures that all organisations we contract with understand the compliance obligations under the relevant player jurisdictions.



In particular, where third parties are involved in Customer Due Diligence (CDD), payment processing, or customer interaction on behalf of the Company, additional due diligence is conducted to ensure that such parties:

- are subject to equivalent AML/CFT regulations in their home jurisdiction;
- maintain appropriate policies and procedures consistent with Curaçao standards;
- have signed written agreements specifying their AML obligations;
- provide timely access to customer identification and verification data upon request.

The Company periodically reviews the compliance performance of key partners and may suspend or terminate cooperation in case of material AML/CFT violations.

13. INTERNAL RECORD KEEPING

The below key principles: know your customer, internal record keeping and reporting, ensure our compliance with laws and regulations.

The Company maintains comprehensive internal records in accordance with Curaçao AML/CFT regulations and licensing conditions. Specifically, we ensure that:

- **Records of all customer transactions** — including but not limited to deposits, withdrawals, and internal transfers — are retained for a minimum of **five (5) years** from the date of the transaction, regardless of whether the transaction was related to gaming activity.
- **Records of customer identity and verification** — including full KYC documentation (ID, proof of address, bank card photo, source of funds) — are stored for a minimum of **five (5) years** after the termination of the business relationship or the last activity on the account.
- **Records of AML investigations, internal SARs, and compliance escalations** are retained for a minimum of **five (5) years** from the closure of the investigation or the decision not to escalate.

All such records are:

- stored securely and backed up digitally;
- readily accessible to the **Compliance Officer** and authorized personnel;
- made available **upon request by the Gaming Control Board or the Financial Intelligence Unit (FIU Curaçao).**

The Company ensures that internal record-keeping systems allow for the **complete reconstruction of customer activity and decision-making**, including risk assessments and AML-related decisions.



II. KYC Policy

(Know Your Customer)

INTRODUCTION

By agreeing to the Terms you authorize us to undertake any verification checks we may require or that may be required by the third parties (including, regulatory bodies) to confirm your identity and contact details (the "Checks").

During this Checks we may restrict you from withdrawing funds from Your Account.

If any information that you have provided is untrue, inaccurate, misleading, does not match your ID or otherwise incomplete we reserve the right to terminate your account immediately and/or prevent you from using the services, in addition to any other action that we may choose to take

If a fact that you were under the Legal age at the time you made any gambling or gaming transactions, then:

- your Account will be closed;
- all transactions made during that time will become void, and all related funds deposited by you will be returned in amount;
- any winnings which you have accrued during that time will be forfeited from you and you will be required to return to us all funds that were withdrawn from Your Account. In the event of any change in your personal details You are required to inform us by contacting Support.

In case of any changes in your personal data, you must inform us about this by contacting the support service.

KYC checks form part of our Customer Due Diligence (CDD) measures and must be applied before allowing transactions that cumulatively equal or exceed NAf. 4,000. However, certain checks — including sanctions screening and preliminary risk assessment — may be performed before this threshold is reached, in accordance with Curaçao AML regulations.

As part of our onboarding process, the user must confirm that they are registering and using the gaming services on their own behalf and not on behalf of any third party. This declaration must be accepted explicitly by checking a mandatory box during registration, and forms part of the Terms and Conditions.

1. OBJECTIVE OF THE POLICY

The Company shall request verification of the user of its Services at the following situations:

- suspicion of fraud, money laundering, criminal activity, or sanction risk;
- doubts about the authenticity or completeness of the provided documents;
- violation of the Company's Terms of Service or AML/KYC policies;
- reaching or intending to reach the cumulative transaction threshold of **NAf. 4,000** (approx. USD 2,200);
- any other situation the Company deems appropriate under Curaçao AML/CFT regulations.

To determine the level of verification and due diligence required, the Company conducts a **Customer Risk Assessment (CRA)** for each user before entering into a full business relationship.



The outcome of the CRA defines the user's risk rating (low, medium, or high) and determines whether Simplified, Standard, or Enhanced Due Diligence will be applied.

During onboarding, each customer is also screened for:

- **Sanctions lists** (UN, EU, OFAC, and any Curaçao-specific lists);
- **Politically Exposed Person (PEP) status**, using open sources and specialized databases.

If the user is classified as high-risk or PEP, **Enhanced Due Diligence** measures are applied, and approval from senior compliance staff may be required to maintain the relationship.

The Company reserves the right to **temporarily block transactions or restrict account access** during the KYC verification process or at any time if there is suspicion of AML/CTF violation, until full clearance is obtained.

2. OBLIGATIONS

Due Diligence (DD): Customers of the Company shall be subject to a due diligence process, including identification, verification, risk assessment, and record keeping, in accordance with Curaçao AML/CFT requirements.

Duplicate / Multiple Accounts: Many customers wish to operate parallel accounts in order to segregate their gambling spend. Notwithstanding this activity, the Company shall identify and associate all **linked accounts** that may belong to, or be under the control of, the same person. This includes shared devices, IP addresses, email patterns, or funding methods.

The Company is entitled to cancel additional accounts, or all accounts of the player in question, cancel winnings obtained from such accounts, and return deposits to the rightful account owner. Any suspicious activity associated with account duplication will be reported internally for compliance review and, if necessary, escalated to the FIU.

Politically Exposed Persons (PEP):

The Company is required to screen all customers for PEP status **at the time of onboarding and on a regular basis throughout the business relationship**. PEPs include:

- individuals currently or previously holding prominent public office (including within the last year);
- their immediate family members and known close associates.

A **risk-based approach** is applied depending on the level and location of the PEP, as well as the nature and volume of transactions. Enhanced Due Diligence measures are applied where necessary, including source of wealth and source of funds checks.

Sanctions Screening:

The Company screens each customer against sanctions lists maintained by the **United Nations, European Union, OFAC**, and any Curaçao-specific sanctions regulations. Sanctions screening is performed both at onboarding and periodically thereafter, using automated systems and manual controls.

The Company reserves the right to apply automated risk scoring and trigger alerts, place accounts under review, suspend transactions, or terminate the relationship entirely based on PEP/sanctions status or other high-risk factors.



The Company also reserves the exclusive right to unilaterally decline any client's application and/or terminate provision of services without further explanation in case of breach of the KYC procedure or AML risk assessment.

3. VERIFICATION REQUIREMENTS AND DOCUMENTATION

To comply with Curaçao AML/CFT regulations, the Company conducts customer identification and verification procedures as part of its Customer Due Diligence (CDD) and Enhanced Due Diligence (EDD) framework.

The following data and documents may be requested during the onboarding process or at any point thereafter, based on the customer's risk level, transactional behavior, or upon reaching the cumulative transaction threshold of **NAf. 4,000**.

3.1 Minimum personal information collected upon registration:

- Full legal name
- Date of birth
- Citizenship
- Permanent residential address

3.2 Required identification documents (for CDD):

- Valid government-issued passport or national ID card
- Proof of address (e.g. utility bill, bank account statement) not older than 6 months

3.3 Additional documents (subject to EDD or risk triggers):

- Secondary ID (e.g. driver's license, military ID)
- A photo of the user holding the open passport or ID next to their face (document must be legible)
- Photo of the front side of the payment card used (showing only 5 first and 4 last digits, name, and expiry date)

The Company may also request documents to verify the **source of funds** used for gaming or deposits, including but not limited to:

- Payslip, pension certificate, dividend statement, or director remuneration
- Bank statement or savings account showing regular income from an identifiable source
- Trust deed confirming entitlement to funds
- Proof of an award, grant, or legal compensation paid to the user

3.4 Submission and verification timelines:

The user must provide all requested documents and information **within 72 hours** of receiving the request. Verification of submitted documents is normally completed **within 72 hours**, unless additional time is required due to legal, technical, or AML-related reasons.

In case of a full compliance procedure (including EDD or internal investigation), the process may take up to **ten (10) working days**. During this period, the Company reserves the right to **block bets, deposits, or withdrawals** from the user's account until verification is complete.



3.5 Reasons for non-approval of documents:

Documents may be rejected on the following grounds:

- Address or name mismatch between documents and account details
- Illegible scans or copies
- Unacceptable document type (e.g. envelope instead of utility bill, expired ID)
- Any other valid reason assessed by the Company's compliance staff based on regulatory obligations

3.6 Final assessment and decision:

Upon review of the documents and information submitted, the Company will make a decision in accordance with its **Terms and Conditions, Privacy Policy, License Agreement**, and applicable law. If risk remains high or documentation is insufficient, the Company may request additional verification (including video call or phone verification using the number provided during registration).

4. ONGOING MONITORING AND DATA UPDATES

The Company conducts **ongoing monitoring** of the customer relationship to ensure that customer activity remains consistent with the information obtained during onboarding and the customer's assigned risk profile.

This includes:

- **Monitoring transactions** to identify unusual patterns or activities that may indicate a change in customer behavior or ML/TF risk;
- **Reassessing the customer risk rating** if there are material changes, such as changes in funding behavior, geolocation, or transaction volume;
- **Tracking the expiry dates** of identity documents and requesting updated copies as needed;
- **Updating customer data** upon notification or detection of changes, such as name, address, source of funds, or payment method.

The Company may request updated documents or re-verification at any time during the business relationship, especially in the following cases:

- Changes to customer profile or personal data (e.g. new ID, change of address);
- Unusual transaction behavior inconsistent with known customer profile;
- Use of new or suspicious payment methods;
- Return from an inactive status after a prolonged period;
- Regulatory changes or updates to internal risk models.

If a customer fails to respond to a request for updated information within the specified period (usually 72 hours), the Company reserves the right to restrict certain functionalities of the account (e.g. deposits, withdrawals, bets) until the verification is complete.

Ongoing monitoring is performed both **automatically**, using transaction monitoring systems, and **manually**, based on triggers or alerts detected by the AML/compliance team.

5. FAILURE TO COMPLETE KYC / TERMINATION OF BUSINESS RELATIONSHIP



If the customer fails to provide the requested identification documents or other required KYC information within the time period specified by the Company, the following measures may be taken:

5.1 Temporary Restrictions

Until the requested verification is completed, the Company reserves the right to:

- block deposits and withdrawals;
- block the placement of bets or wagers;
- restrict access to the account or selected features.

These restrictions remain in effect until satisfactory completion of the KYC process.

5.2 Account Suspension and Termination

If the user **fails to complete verification within 30 days** from the initial request — or within an extended time limit granted by the Company for justified reasons — the Company may:

- permanently suspend or close the customer's account;
- cancel any pending transactions;
- return any remaining balance (if legally permitted) to the **same payment method originally used**, provided no suspicion of ML/TF exists;
- refuse the refund and block funds **if there is a presumption of money laundering or terrorist financing**, and file a report to the Financial Intelligence Unit (FIU) Curaçao.

All attempts to obtain the missing documents and the reasons for account closure are **recorded internally** and made available to competent authorities upon request.

5.3 AML/CTF Concerns

The Company shall not establish or continue a business relationship, and shall not execute any transaction, if:

- the customer fails to complete KYC verification;
- doubts remain as to the customer's identity or legitimacy of funds;
- the customer's behavior or documents raise red flags under the Company's risk framework.

Where suspicion of ML/TF or sanctions evasion arises, the Company will immediately escalate the case for internal review and, if appropriate, file a **Suspicious Activity Report (SAR)** to the FIU.

The Company may decide to freeze the account fully or partially **without prior notice**, based on risk factors and internal procedures, taking into account the risk of tipping off.

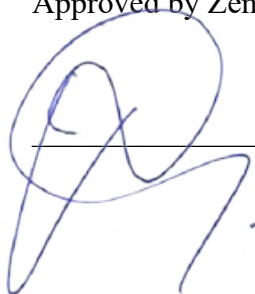
5.4 Reopening or Appeal

Customers whose accounts were closed due to non-compliance with KYC requirements may request reopening only by submitting the full set of required documents. The Company reserves the right to refuse reinstatement based on the outcome of the previous review or if the risk remains high.



Version 1.7, dated 14.05.2025

Approved by Zeno Club B.V. CEO

A handwritten signature in blue ink, consisting of a large, stylized 'Z' followed by a long horizontal stroke and a final downward stroke.