AML/CTF Policy - Revision No. 6

Company Name: POINDER B.V.

Registered address: Z/N, ZUIKERTUINTJEWEG, WILLEMSTAD, Curacao

Registered Number: 166111

Main Domain: najahbet.com

Approved by: Managing Director, IGA TRUST B.V.

Compliance Officer: Inna Honcharuk

Effective Date: 28.11.2025

Next Review Date: 28.11.2026

Principal Applicable Regulation: Regulations for the combating of Money Laundering, the Financing of Terrorism and Proliferation of weapons of mass destruction as of January 2025 (binding as of April 10, 2025).

Table of Contents:

1. Policy Statement

POINDER B.V., registered under number 166111 with its office at Z/N, ZUIKERTUINTJEWEG, WILLEMSTAD, Curacao (hereinafter referred to as the ”Company” or “Operator), is committed to combating money laundering (ML), terrorist financing (TF), and proliferation financing (PF) through a comprehensive set of policies, procedures, monitoring tools, and training programs. This policy outlines the measures taken to ensure full compliance with the applicable AML/CTF laws of Curaçao and international standards.

2. Purpose

Historically, criminals across jurisdictions have been using money laundering practices to conceal and alter the true origin and ownership of the proceeds from their illegal activities, with the aim of avoiding prosecution, conviction, and the confiscation of funds derived from unlawful sources. Similarly, terrorist financing schemes have been using funds that may be legitimately sourced, but are intended to support terrorist operations.The ability to launder illicit proceeds through global financial systems is crucial for the success of criminal enterprises. Money serves as the essential resource for terrorist organizations, enabling them to fund and carry out their activities.

To combat these practices, an international AML/CFT framework has been established, and the Company strives to be a part of it by adopting a set of clear standards and procedures outlined in this Policy. The purpose of these Anti-Money Laundering and Counter-Terrorist Financing (AML/CTF) standards and procedures is identifying, preventing, and reporting money laundering, terrorist financing, and other illicit financial activities which may be attempted by using services offered by the Company. This Policy ensures compliance with the applicable laws and regulations of Curaçao.

The definitive legal requirements which the Company adheres to is laid out in the following laws and regulations:

3. Audience and Respective Requirements

This Policy affects all stakeholders of the Company.

3.1. General Stakeholders

The Policy shall be adhered to, carried out by and applied to:

- direct and indirect shareholders,
- directors, managers and other key persons and decision makers,
- any individuals or entities acting on behalf of the Company.

The Policy shall also be applied to third party stakeholders, and in order to have business relations with the Company, they shall agree and be subjected to the procedures outlined in this Policy. These include:

- individual and corporate customers,
- contractors, subcontractors, suppliers and service providers, partners and agents.,

- other parties supporting or benefiting from the Company's operations.

3.2. Employees

The operator shall ensure that its business is conducted at a high ethical standard and that the laws and regulations pertaining to financial transactions are followed. The AML principles and specifically rules set out in this policy are relayed to each employee of the operator who deals to any extent with financial transactions, their execution, review, approval, disputing or maintaining infrastructure for them.

3.2.1. Screening

Each employee of the operator shall undergo a screening conducted by the HR Department or a similar function. Apart from the usual identification and verification of the employee required by the local labour laws and regulations, before starting work and getting access to any of the operator's capabilities and infrastructure, each employee shall provide an official Clear Criminal Record (CCR, Certificate of Good Conduct, Police Report etc.) issued by a relevant authority in each jurisdiction they resided in during the last 12 months.

The document shall be clear of any criminal offences, be issued not earlier than 6 months before start of employment, duly certified and translated into English if not originally in English.

After the initial screening, all employees shall be subject to ongoing screening annually.

The CCR shall be retained for 5 years from the date of employment termination and treated as Confidential Information.

3.2.2. Training Program

The operator shall develop training programs and provide training to all personnel who handle transactions that may be qualified as unusual as per this Policy.

Training includes setting rules of conduct governing employees' behavior and their ongoing education to create and maintain awareness of the operator's policies against money laundering and terrorist financing.

Employees Training includes educating and testing employees on the following elements:

a) New employees, all ranks - Basic AML/CFT training

- Nature and process of ML/TF
- Using gambling for ML/TF
- The need to report unusual transactions to the appropriate designated officer
- Internal AML/CFT policies, procedures and regulations of the operator
- General reporting requirements.
- CDD principles and measures
- Subjective indicators of unusual transactions.

b) Dealers, cashiers and slot department personnel (not applicable for online gambling) - Basic AML/CFT training above and additional elements:

- Goals, objectives and best practices of customer identity verification.
- Special expertise on identify verification across jurisdictions.

c) Audit staff - all of the above and additional elements:

- Changes in regulations,
- Updated money laundering methods and enforcement
- Application of changes to the operator.

d) AML Compliance staff - line AML program personnel - all of the above and:

- Attending specialized AML-specific training, courses, workshops, seminars, presentations to be able to stay on top of new trends or changes that impact the organization and the way it manages risk.

e) Supervisors and Managers - highest level of AML expertise with all of the above.

f) Senior management and board of directors

The Board must be regularly informed by the staff of ML issues and risks.

Refreshment training must be arranged annually to ensure that staff members are kept informed of current and new developments regarding money laundering and terrorist financing techniques, methods and trends.

The operator shall maintain records on staff training including:

- Details on the content of the training programs;
- The names of the staff members who have received the training;
- The date on which the training was provided;
- The results of any testing carried out
- An ongoing training plan.

3.3. Compliance Officer

The Compliance Officer (CO/MLRO) appointed by the company is the key person for managing AML/CFT procedures and this Policy.

The main feature which the CO can be distinguished from other AML-related staff is that the CO acts independently. They are independent from any gaming operations of the operator. They are not directly integrated into the management hierarchy and report directly to the operator's top management and to the financial authorities such as FIU.

To be able to act independently, the CO at all times has direct access to customer identification data and other CDD information, transaction records, and other relevant information without relying on other departments and staff to gain access to them.

The authorities and responsibilities in this regard include:

- To design and implement the AML program;
- To verify adherence to local laws and regulations regarding the detection and deterrence of money laundering and terrorist financing;
- To review compliance with the casino's policy and procedures;
- To organize training sessions for the staff on various compliance-related issues;
- To analyze transactions and verify whether any are subject to reporting according to the indicators mentioned in the Ministerial Decree regarding the Indicators for Unusual Transactions;
- To review all internally reported unusual transactions for their completeness and accuracy with other sources;
- To keep records of internally and externally reported unusual transactions;
- To design an internal procedure about when reporting of unusual transactions will lead to blocking/ freezing of user accounts, taking into account the risk of tipping off the player.
- To execute closer investigation of unusual transactions if necessary;
- To prepare the external report of unusual transactions;
- To make necessary changes to the AML program;
- To remain informed on the local and international developments on money laundering and terrorist financing and to make suggestions to management for improvements;
- To prepare periodic information on the casino's efforts against money laundering and financing of terrorism and financing of proliferation.

These responsibilities shall be included in the job description of the CO. The job description shall be signed off and dated by the officer, indicating his/her acceptance of the entrusted responsibilities.

4. Definitions

- **Compliance Officer (MLRO/CO):** The designated person responsible for implementing the AML/CTF policy, conducting internal investigations, and liaising with regulatory authorities, including the Financial Intelligence Unit (FIU).
- **CDD (Customer Due Diligence):** A standard verification process involving the collection and verification of customer identity, understanding the purpose of the business relationship, and ongoing monitoring of transactions.
- **EDD (Enhanced Due Diligence):** A more intensive form of due diligence applied in higher-risk situations. It includes

collecting additional documentation, verifying the source of wealth/funds, and obtaining approval from senior management.

- **PEP (Politically Exposed Person):**
  An individual who holds or has held a prominent public position, or a close relative or associate of such a person, and therefore presents a higher risk of involvement in bribery or corruption.
- **FIU (Financial Intelligence Unit):**
  A government authority responsible for receiving, analyzing, and acting upon reports of suspicious financial activity to combat money laundering and terrorist financing.
- **SDN (Specially Designated Nationals):**
  Individuals or entities listed on sanctions lists (e.g., OFAC) with whom transactions and business relationships are prohibited.
- **ODD (Ongoing Due Diligence):**
  Continuous monitoring of clients and their transactions after the business relationship is established to detect deviations from normal activity or suspicious behavior.
- **SoW/SoF (Source of Wealth / Source of Funds):**
  Documentation or information used to verify the legal origin of a customer's assets or incoming funds.
- **ML/TF (Money Laundering / Terrorist Financing):**
  Criminal activities aimed at disguising the origins of illicitly obtained money (money laundering) or providing financial support for terrorist operations (terrorist financing).
- **Customer** (**client**):
  A customer who is of the approved age and participates in a game of chance.
- **SAR:**
  Suspicious activity report
- **STR:**
  Suspicious transaction report
- **CRA**
  Customer Risk Assessment
- **BRA**
  Business Risk Assessment
- **CAP**
  Customer Acceptance Policy
- **TDRA**
  Technological developments risk assessment

5. Policy Implementation

5.1. Business Risk Assessment (BRA)

The Company conducts regular business risk assessments (BRA) to identify potential vulnerabilities in its operations, particularly in the context of online gaming. High-risk scenarios include complex financial flows, the use of anonymizing tools, or players from sanctioned jurisdictions. Products and services are reviewed to evaluate their susceptibility to ML/TF.

For the purpose of identification, assessment, and analysis of risks of money laundering and terrorist financing related to their activities, the Company conducts a risk assessment. Steps are taken to identify, assess, and analyze risks that are proportionate to the nature and level of complexity of the economic and professional activities of the Company. The following are taken into account at least in the following risk categories:

- Risks relating to customers.
- Risks relating to countries, geographic areas, or jurisdictions.
- Risks relating to products, services, or transactions.
- Risk relating to communication, mediation, or products, services, transactions, or delivery channels between the Company and customers.

The steps taken to identify, assess and analyze risks must be proportionate to the nature, size and level of complexity of the economic and professional activities of the Company and/or the players. Once the business risk has been assessed, the casino sets a risk appetite: it decides how much risk it is prepared to accept.

The BRA is revised annually by default, and additionally every time the elements of business risks change significantly, including but not limited to the following cases:

- introduction of new payment methods
- introduction of new markets
- adding new games
- regulatory changes, etc.

Each BRA iteration shall be documented and approved by the Board of Directors of the casino and preserved to be available for the relevant authorities. The BRA must include the following aspects:

- The methodology adapted
- The reasons for considering a risk factor as presenting a low, medium or high risk;
- The outcome of the BRA;
- Any information sources used.

All records pertaining to the BRA shall be retained for at least 5 years.

5.2. Customer Risk Assessment (CRA)

The Customer Risk Assessment is a risk management measure implemented to identify and assess the particular risks the casino will be exposed to when providing its services or products to players. It has to be carried out either prior to the carrying out of an occasional transaction, or during establishing a business relationship. It is possible that this initial customer specific risk assessment will have to be revised at a later stage of the business relationship and this may result in a customer's risk rating having to be adjusted.

The information collected to draw up the CRA will formulate the customer's risk profile. On the basis of the CRA, the proper level of CDD can then be applied as stipulated in the Customer Acceptance Policy (CAP).

The CRA is revised annually by default, and additionally every time there are significant changes in elements of the business environment that have substantial influence on the behavior of the customers - and consequently the procedures and outcomes of the CDD. These largely overlap with BRA and technological risks and may include the following:

- mass shifts in the customer behavior
- regulatory changes
- a new product is developed
- a new business practice emerges
- a new delivery mechanism becomes available, etc.

Each CRA iteration shall be documented and approved by the Board of Directors of the operator and preserved to be available for the relevant authorities. The CRA must include the following aspects:

- The methodology adapted
- The reasons for considering a risk factor as presenting a low, medium or high risk;
- The outcome of the BRA;
- Any information sources used.

The Company maintains the following customer risk classification:

Low risk. This risk rating is reserved for players who are found eligible for registration, are not on PEP/FATF/Sanctions lists, have no or negligible Adverse Media. Simplified Due Diligence is applied to players at this risk level. The player retains this risk level until they hit the triggers rendering them Medium or High Risk.

Medium risk. This risk rating is reserved for players who were initially assigned Low Risk and hit the Medium Risk triggers, such as reaching the 4000 XCG threshold of combined withdrawals and deposits. The risk level is retained throughout the further lifecycle of the player unless they hit High Risk triggers.

High risk. This risk rating can be assigned at registration - if the player is listed as a PEP, mentioned in moderately adverse media or resides in a High Risk GEO - as well as at later stage upon hitting the High Risk triggers:

- Player makes a transaction of 5000 XCG or more
- Player makes a deposit in crypto currency
- Operator has suspicions of fraud, ML or FT etc.

Also, any Player for whom an automated alert has been generated, or an inappropriate activity has been detected, will be categorized as High Risk, for which an Enhanced Due diligence procedure is applied.
Upon the player clearing all concerns, their risk rating can be downgraded back to **Medium**.

<table>
<tr><th>Risk Level</th><th>Initiating Registration (Account opening)</th><th>Reaching Threshold of 4000 XCG (withdrawal+deposit) within the last 6 months</th><th>Makiing a Transaction over 5000 XCG/ Crypto Transaction/ ML,FT suspicions</th></tr>
<tr><td>Low - Simplified Due Diligence</td><td rowspan="2">SDD info:
1) Full name
2) Residence Address
3) Date of Birth</td><td rowspan="2">Documents:
1) Photo ID (Passport/ Driver License/ National ID)
2) Proof of Address (Utility bill/ Bank reference/ Tax ID)</td><td rowspan="3">1) Selfie with passport/ Liveness check
2) Documents supporting SOF/SOW in proportion to the size of transaction</td></tr>
<tr><td>Medium - Standard Due Diligence</td></tr>
<tr><td>High - Enhanced Due Diligence</td><td>Info:
1) Full name
2) Residence Address
3) Date of Birth

Documents:
1) Photo ID (Passport/ Driver License/ National ID)
2) Proof of Address (Utility bill/ Bank reference/ Tax ID)
3) Selfie with passport/ Liveness check</td><td>Update if necessary</td></tr>
</table>

The specific measures applied to each risk rating are listed in the table below:

All records pertaining to the CRA shall be retained for at least 5 years.

5.3. Technological developments risk assessment (TDRA)

Technological developments risk assessment (TDRA) is another aspect of the comprehensive AML/CFT complex implemented by the operator which is aimed at preventing the misuse of technological developments for the purpose of money laundering or the financing of terrorism. As a technology-reliant business, the operator shall identify and assess the money laundering or terrorist financing risks that may arise whenever:

- A new product is developed;
- A new business practice emerges;
- A new delivery mechanism becomes available;
- A new or developing technology is used for both new and pre-existing products.

In those cases, a risk assessment takes place prior to the use of new technological developments including launch of the new products, business practices, delivery mechanism or the use of new or developing technologies. This is done to determine whether the innovation creates a weakness that can be misused by money launderers or those seeking to finance terrorism.

The TDRA is revised annually by default, and additionally every time one of the cases above arise.

Each TDRA iteration shall be documented and approved by the Board of Directors of the operator and preserved to be available for the relevant authorities. The CRA must include the following aspects:

- The methodology adapted
- The reasons for considering a risk factor as presenting a low, medium or high risk

- The outcome of the TDRA
- Any information sources used.

All records pertaining to the TDRA shall be retained for at least 5 years.

5.4. Customer Acceptance Policy (CAP)

The Company risk appetite is pertinent in understanding the parameters the levels of risk the Company is willing to undertake. The Company currently has an array of appetite depending on the nature of the risk.

Appetite meaning that the residual risk of any product or service has to have sufficient controls in place to mitigate such risk to be within controllable boundaries and for which the Company has control over the behavioural pattern and relationship with the customer. The company shall have a zero tolerance policy of any sort of financial crime or supporting any terrorist activity. For each risk identified, the risk committee shall establish risk management arrangements. The arrangements established must be proportional to the risk tolerance established by the Company.

The AML/CFT unit including the MLRO, shall assess, on a yearly basis, the adequacy and effectiveness of the Company's risk management arrangements, processes and mechanisms as established and approved by the Board of Directors.

Risk appetite shall be divided into 3 levels:

Low Risk

The effect of low risk is negligible when the threat emanates from the customers, hence due diligence will be applied to reflect the risk of ML/FT the customer is likely to pose towards the Company. The term low risk may also be interpreted towards other facets of the Company meaning that the risk can be easily remediated, hence, the loss and damage, and supervisory action is negligible.

Medium Risk

Medium risk in relation to the customer will mean that a substantial level of due diligence has to be entertained and the monitoring against such a customer has to be reflective of the level of risk. In relation to the business, medium risk means that the loss or damage, and minor supervisory action should be remediated within the short term. Also, such risk may be assigned where products for which the entry level of the customer shall be at a minimum of Customer Due Diligence level, meaning all documentation will need to be verified.

High Risk

High risk shall mean that the customer risk is to be monitored and further documentation and review of the customer needs to be more frequent. This may present itself either due to the profile of the risk score or as suspicion may arise due to the activity of the customer.

High risk may also be assigned to various parts of the business meaning that attention is required or that a certain level of ongoing monitoring or further technical amendments are required in order to mitigate the risk.

In any of the above, the Supra National Risk Assessment and the National Risk Assessment are taken into consideration and the assigned rating is given to products that after evaluation of the said reports the relevant level score has been assigned.

The Customer Acceptance Policy of the Company is based on what is required under applicable legislation. The following persons are not accepted as customers:

- Under 18
- Individuals on the FATF, UN, EU, UK, or OFAC sanctions lists
- Residents in countries classified and/or prohibited as high risk by the applicable competent authorities
- Individuals suspected of ML/ TF involvement or other types of criminal activity
- Self-excluded customers
- Individuals who have submitted documentation or information which we have reasonable grounds to suspect is fake or fraudulent

Categories of customers whose activities may indicate a higher risk include:

- customers who have multiple sources of income
- customers with irregular income streams
- PEPs
- high spenders (however, if the amount of confirmed SOW/SOF covers the transaction, the customer can retain a lower risk rating)
- disproportionate spenders (triggers transaction monitoring with a request to provide information supporting the transaction. Failure to do so may result in blocking the customer).

All records pertaining to the CAP and CDD shall be retained for at least 5 years.

5.5. Non-Acceptable Customers

The following list pre-determines the type of customers who are not acceptable or who operate within non-acceptable lines of business as indicated whether establishing a business relationship or an execution of an occasional transaction with the Company.

The list has been compiled throughout the operation of the Company and is not exhaustive. It shall be updated on instances where the board of directors deem new and evolving lines of business, and a high and unacceptable risk towards the Company. Such instances shall be raised to senior management for approval or decline, and an analysis will also be made in the case where an SAR is to be raised:

- Individuals who fail or refuse to submit the requisite data and information for the verification of their identity and the creation of their economic profile, without adequate justification
- Individuals who have been convicted of criminal acts either by the relevant courts of Curacao, the Netherlands or in any other part of the world

- Individuals who have not reached the legal age of 18+
- Individuals who attempt to open account with fraudulent information, fictitious names or identity theft matters
- Individuals attempting to register from non-reputable jurisdictions (as per internal jurisdiction scoring)
- Individuals who are PEPs
- Individuals with intent to launder money or terrorist financing
- Individuals who are involved in business activities which are illegal, unethical or involve actions which are contrary to public order or moral standards
- Individuals who are sanctioned by international or governmental organisations
- Individuals involved in business structures that make it impossible to verify the ultimate beneficial owner/s
- Customers/business structures that make it impossible to verify the legitimacy of their activities or the source of funds
- Applicants for business involved in child pornography, illegal drug paraphernalia, pyramid sales, the production or trade in radioactive materials and or arms of mass destruction, the production or trade in weapons and munitions or spare parts of war related vehicles, the production or activities involving harmful or explosive forms, forced/harmful child labour activities, and in any form of counterfeit goods
- Applicants who use payment processors which are registered in non-reputable jurisdictions and which are not licensed or authorised to operate in the EU
- Individuals or entities linked to pseudo-chivalric orders or self-styled orders which are not officially recognised
- Verification or reason to believe that funds were obtained illegally or are derived from illicit purposes
- Customers for whom an SAR/STR has been raised
- Any customer who activates fraud or transactional triggers and upon analysis are found to be in a serious violation of the said account
- Customers who refuse to explain unusual or suspicious access or who do not sufficiently explain unusual or suspicious activity
- Customers flagged by payment providers, verification providers, law enforcement bodies or other industry collaborative platforms as potentially suspect customers or engaging in fraud, money laundering, terrorist financing etc.

Reference shall also be made to the dual use products or customers involved in the trading of: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:L:2019:338:FULL&from=EN

5.6. Low Risk Customers Attributes

- Customers registered from a country not considered to have a high risk of money laundering, terrorist financing, corruption, fraud and having completed registration with plausible identification details and complete profile information.
- Verified at least the contact email or phone as applicable.
- Has deposited less than XCG 4,000 in the last 6 months for low risk payment methods.
- Customers using a limited number of payment methods which are in the customer's name.
- Placed reasonable bets on the Company's remote gaming website/s in line with "normal" gaming activity seen from regular customers with the same registration country or funding patterns.
- effect closed-loop withdrawals whereby the withdrawals are requested to the same payment method from which those funds originate and are not substantially higher than those deposited by the customer.
- Customer has completed Customer Due Diligence ('CDD') successfully.

5.7. Medium Risk Customer Attributes

- Customers with valid-looking registrations who register from unusual countries not targeted by the company but that are not countries with high risks of money laundering, terrorist financing, corruption, fraud, etc.
- Customers who reach the threshold of XCG 4,000 in deposits within the last 6 months, using low risk payment methods or reaching XCG 4,000 in deposits within the last 6 months using low to medium payment methods.
- Customers whose betting activity is above average for a similar playing customer but not alarming.
- Customers who request withdrawals to a different payment method due to payment method inability to receive withdrawals which has been confirmed to be true.
- General customers due to the nature of the product and method of interaction.

5.8. High Risk Customer Attributes

If any of the attributes are identified and verified, the customer will be blocked:

- Invalid or suspicious registration details, origin IP address not matching the customer's country, verification of email or phone not performed.
- Identity theft.
- Multiple accounts registered.

- Customer accounts used from multiple locations within an unreasonable time frame or change of pattern from normal usage.
- Customer deposits using third party payment methods or uses high risk payment methods such as quasi-cash payment methods.
- Customers that deposit unreasonable amounts in relation to their online gaming activity or when they would still have funds within their account which were available for online gaming.
- Customers who have deposited more than XCG 4,000 over the previous year and have not yet provided a basic source of wealth information.
- Customers whose online gaming activity is beyond expected online gaming behaviour in relation to similar customers and own funding sources or wealth.
- Customers who demonstrate signs of problem gambling.
- Customers who request withdrawals to alternate payment methods rather than to the origin of customer funds or request withdrawals to third party payment methods.
- Customers who refuse to provide due diligence documentation, or provide invalid or fake documentation.

5.9. Mandatory EDD Customers

The instances below are those where acceptance of the said customers requires mandatory EDD. The Company shall reserve the right, when suspicion, knowledge or reason to believe is established to further enforce Enhanced Due Diligence ('EDD') on those customers where it is deemed necessary via an override function on the account.

- Those customers residing, registering or place of birth is within a non-reputable jurisdiction or the provenance of funds emanates from said jurisdiction.
- Those customers who have been classified as a high risk.
- Those customers who have been found to be associated with any negative media.
- Customers whose source of wealth and funds are deemed to be complex.

The Company also takes into consideration geographical risks, which are assessed by the location of the player and the source of wealth in the business relationship. Nationality, residence, and place of birth of the player are taken into account.

6. Customer Due Diligence (CDD)

The Company applies Customer Due Diligence (CDD) not as a one-time obligation, but as a continuous process throughout the entire customer relationship lifecycle. By embedding periodic reviews and dynamic risk evaluations into its broader compliance framework, the company ensures sustained alignment with Anti-Money Laundering (AML), Counter-Terrorist Financing (CTF), and Counter-Proliferation Financing (CPF) requirements. This practice forms

part of the Company's overarching risk-based strategy, which is designed to adapt to emerging risks and maintain the integrity of its operations.

The Company enforces Customer Due Diligence (CDD) measures swiftly and in alignment with established obligations under Anti-Money Laundering (AML), Counter-Terrorist Financing (CTF), and Counter-Proliferation Financing (CPF) regulations. These measures are designed to ensure that all customer identities are accurately established and verified before significant financial interaction occurs.

The principal CDD measures taken by the operator are as follows:

a. Identifying the player and verifying that customer's identity using reliable, independent source documents, data or information;

b. Identifying the beneficial owner, and taking reasonable measures to verify the identity of the beneficial owner, such that the operator is satisfied that it knows who the beneficial owner is. For legal persons and legal arrangements this should include understanding the ownership and control structure of the customer;

c. Understanding and obtaining information on the purpose and intended nature of the business relationship;

d. Conducting ongoing due diligence on the business relationship and scrutiny of transactions undertaken throughout the course of that relationship to ensure that the transactions being conducted are consistent with the operators's knowledge of the player, its business and risk profile, including, where necessary, its source of funds.

To ensure that these objectives are met continuously, the operator implements a number of practices and techniques below.

CDD begins at account opening and is fully completed at XCG 4,000 threshold.

Based on the results of the CRA the following levels of Customer Due Diligence are applied to customers with different risk levels:

- **Low-Risk Clients:** Simplified due diligence. The law mandates that until the client reaches a XCG 4000 threshold within the last 6 months, the obligation is to obtain information pertaining to the client being:
  - Full name
  - Permanent residential address
  - Date of birth
- **Medium-Risk Clients:**
  Subject to **Standard CDD** procedures, including identity verification, verification of the beneficial owner (if applicable), and transaction monitoring. Ongoing Due Diligence (ODD) is performed **once every 24 months**
- **High-Risk Clients:**
  Subject to **Enhanced Due Diligence (EDD)** measures. This includes the collection of additional documentation (e.g., source of wealth), senior management approval, and enhanced monitoring. ODD is carried out every 12 months

The decision to accept or continue a relationship with high-risk clients must be approved by the Compliance Officer (MLRO) and documented accordingly. All risk ratings are reviewed periodically and adjusted based on the client's activity, transactional behavior, or external changes such as updated sanctions or regulatory status.

Risk Level	**CDD Type**	**Ongoing Review**
Low Risk	Simplified Due Diligence	Once every 36 months
Medium Risk	Standard CDD	Once every 24 months
High Risk	Enhanced Due Diligence (EDD)	Once every 12 months

6.1. Simplified CDD

Upon the creation of a player account, the Company collects key identity details from each user, including:

- Full legal name
- Residential address
- Date of birth

Based on these data, the Customer is then screened against PEP Status, Sanctions and Adverse Media, country of residence, etc. - to check if there are any factors that will assign them to a risk rating higher than low - triggering Standard CDD or Enhanced CDD measures.

If none of the above triggers a higher risk rating, the Customer is only subject to confirming their contact email or phone number - until a change in their risk rating is triggered later on. This exhausts the Simplified CDD.

Simplified CDD measures are not acceptable whenever there is any suspicion of money laundering or terrorist financing.

6.2. Standard CDD

Standard CDD is applied to medium risk Customers. Upon obtaining this risk rating, the following data must be requested and verified by photo ID and a valid Proof of Address as a Standard CDD measure **in addition to those requested at the Simplified CDD stage**:

- Place of birth
- Nationality
- Identity number
- Politically Exposed Person (PEP) status

- Sanctions screening
- Adverse media screening

As part of the company's risk-based compliance framework, identity verification is initiated prior to processing any financial transaction that meets or exceeds a threshold of XCG 4,000. This threshold is applied in the following scenarios:

- A single transaction equal to or above XCG 4,000
- A combination of transactions (such as multiple deposits, withdrawals, or internal transfers) that cumulatively reach this amount
- If the single or cumulative transaction exceeds XCG 5000, apart from triggering an SCDD, it also triggers manual reporting

Daily transaction data is monitored and aggregated per customer, enabling the company to identify when thresholds are met and respond in real time. Once the XCG 4,000 mark is reached, a full risk evaluation of the customer is conducted, and any remaining Standard CDD steps are completed without delay.

The Company emphasizes early completion of CDD. This preemptive strategy is intended to prevent the entry of illicit funds into the system by ensuring that no user is granted full platform access without having first undergone due diligence.

6.2.1. Operational Limits for Incomplete CDD

In situations where a player reaches the XCG 4,000 threshold prior to completing CDD, specific limitations are imposed:

- If triggered by a deposit: Further deposits and withdrawals are restricted; however, the customer may continue to participate in gaming using their current account balance.
- If triggered by a withdrawal request: The player's account is temporarily frozen, and all gameplay is suspended until full verification is completed.
- These safeguards help preserve the integrity of the platform and prevent unauthorized movement of funds during the verification window.

6.3. Enhanced Due Diligence (EDD)

For high-risk scenarios, EDD measures are applied, including:

- In-depth investigation into the player's background.
- Verification of the source of funds and wealth.
- Close examination of transaction patterns.
- Photo verification by requesting a selfie with the Customer's photo ID
- Regular updates of identification information.

EDD also applies to politically exposed persons (PEPs), requiring thorough risk assessments and ongoing monitoring.

6.4. Politically Exposed Persons (PEPs) Handling

The company's AML/CTF/CPF policy requires heightened scrutiny for PEPs, their family members, and close associates. Enhanced Due Diligence (EDD) measures include obtaining senior management approval, understanding the source of funds and wealth, and conducting rigorous ongoing monitoring. Political exposure will be for a term of 12 months after termination and shall consider both local and international political involvement

6.5. Identification of the Beneficial Owner

The principle which the operator maintains is that the player is engaged into gaming and transitioning on their own behalf. However, there may be cases when the operator may need to identify the real beneficiary of the relations.

6.5.1. Syndicates

When a person is registering an account to play and transact, the registering player must explicitly accept, together with a declaration in the form of a tick box that a player is registering to play on his/her own behalf. This is stipulated by Terms and Conditions, Policies, CDD measures, etc. The operator does not rely merely on said declaration, but ensures that their ongoing procedures allow for the detection of possible instances where the player is actually playing on behalf of third parties.

Although not common, instances of playing on behalf of other parties cannot be excluded completely as the operator may be maintaining business relations with one or more players funded by a syndicate. In such circumstances, where the funds being wagered are collected from multiple persons who will eventually share in any winnings, the particular transaction will not only be considered as having been undertaken by the customer but undertaken also for the benefit of those persons providing the necessary funding. These persons would be considered as beneficial owners and the operator assigns a high risk rating to such customers and would therefore have to identify them and verify their identities and SOF.

The identification of such cases is made through ongoing compliance, analyzing the players' deposit and withdrawal patterns, temporal coincidences in gaming activity etc.

6.5.2. Corporate Accounts

Although the operator's business model does not allow registered player accounts used by companies (corporate accounts), some companies do engage in activities, thus the operator has a CDD toolset in place for such instances.

The key feature applicable to such clients is to - among and in addition to the CDD measures in place - identify the beneficial owners of such accounts.

The CDD in such cases is augmented by analyzing corporate documents, public and paid corporate registers and other reliable sources - for each of the entity in the customer's ownership chain up to the beneficial owner.
Upon identification of the beneficial owners, each of them is subject to CDD as per the risk rating assigned to them. At the minimum identification information, verification and evidence must be gathered for all persons holding 25% or more of the shares or voting rights or a person who otherwise exercises ultimate effective control of the customer in question.

Where no natural person is identified under the 3 items mentioned above, the natural person who holds the position of senior managing official should be identified and subjected to CDD.

7. Reliance on third parties

The operator has a right to rely on third parties when performing the CDD measures, if the third party follows all the principles, meets and carries out all the procedures set in the respective policies adopted by the operator to which the operator itself is subject.

Furthermore, the third party shall not be engaged unless there is an existing business relationship with the customer, which is independent from the relationship between the operator and its customers.

In any case, the ultimate responsibilities for CDD measures remain with the operator, and this prevails over any agreements with a third party.

To be engaged with a third party for CDD functions, the criteria to be met are as follows:

The operator obtains the information concerning elements of the CDD measures immediately from the third party it is relying upon;

The operator should have an agreement with the third party being relied upon that copies of

identification data or other relevant documentation relating to CDD requirements are available upon request (this arrangement must be tested from time to time to ensure that it

functions as intended)

Regardless of such engagement, the operator remains responsible for the following functions that cannot be outsourced:

- Customer-based risk assessment,
- The decision whether to on-board a customer or to continue a business relationship
- Determining whether the customer is a PEP
- Conducting on-going monitoring;
- Monitoring the third-party's compliance, record-keeping requirements and associated country risks.

In the outsourcing/agency scenario, the outsourced entity applies the CDD measures on behalf of the delegating casino, in accordance with its procedures, and is subject to the

delegating casino's control of the effective implementation of those procedures by the outsourced company.

In any case, the ultimate responsibilities for CDD measures remain with the operator, and this prevails over any agreements with a third party. Annual assessments of quantitative and qualitative obligations fulfilling shall be performed on each of such third parties.

Any activity performed by an agent or group company is to be considered as an activity performed by the operator. As such, any customer on-boarded by the agent or group company has to undergo the same checks and controls as customers on-boarded by the operator itself. It is therefore the responsibility of the casino to ensure that its AML/CFT controls, policies, measures and procedures are applied by the agent or group company.

8. Product, Service, and Transaction Risks

Certain gaming services, financial instruments, and transaction types inherently present greater risks of being exploited for money laundering and terrorism financing. Criminal actors often target weak points within gaming ecosystems to manipulate outcomes or obscure the origins of illicit proceeds.

Illicit funds derived from activities such as fraud, narcotics trade, or theft may be funneled through gambling platforms to disguise their origin. The use of anonymous payment tools—such as prepaid cards and digital assets like cryptocurrencies or tokens—presents heightened risks due to limited traceability.

The misuse of player accounts for non-gaming purposes, such as acting as temporary repositories for financial transactions, also raises compliance concerns. Similarly, peer-to-peer transfers among players can facilitate unauthorized movement of funds.

Criminals may attempt to exploit third-party financial instruments, such as bank accounts or cards registered under different identities, or transfer funds across multiple gaming accounts, further complicating traceability. Financial services linked to gambling, such as currency exchanges, credit facilities, or the use of multi-operator platforms, present an additional layer of risk.

To counter these threats, the Company enforces stringent transaction monitoring protocols, applies EDD processes where appropriate, and maintains full compliance with global AML/CTF/CPF regulations.

9. Sanctions

The company's AML/CTF/CPF policy mandates rigorous compliance with both international sanctions and regulatory standards. To ensure we meet these obligations, we implement comprehensive procedures focused on adhering to all sanctions imposed by national and international authorities. This process involves conducting thorough due diligence on every client and transaction to prevent any interactions with sanctioned individuals, entities, or regions.

Monitoring and reporting are critical components of the company's AML/CTF/CPF policy. The company continuously observes all transactions for any suspicious activities that could breach sanctions. Any anomalies detected are reported immediately to the relevant authorities. Furthermore, the company's commitment to compliance is reinforced through ongoing staff training, which ensures that all personnel are up-to-date with current sanctions regulations. This approach safeguards our operations and helps mitigate potential risks.

In addition, the company is dedicated to ensuring that all client interactions and transactions are meticulously checked against the most recent Sanctions Lists. Where applicable, automated systems may perform real-time verifications, and our database is regularly updated to reflect the latest sanctions information. When a match or suspicious activity is identified, it is promptly reported to the appropriate authorities. The company takes decisive action, such as freezing accounts or blocking transactions, to address and manage compliance risks.

The company's sanctions compliance procedures are subject to frequent reviews and updates to align with evolving legislation. This includes monitoring lists such as:

- Sanctions National Ordinance (SNO, N.G. 2014, no. 55); Kingdom Sanction Act (N.G. 2016, no. 54); GCB announcements.
- EU Sanctions.
- UK OFSI Sanctions.
- UN Security Council Consolidated List.
- US List of Foreign Terrorist Organizations.
- OFAC Sanctions.

10. Geographical Risk:

Geographical risk refers to the potential money laundering (ML), terrorism financing (TF), and proliferation financing (PF) risks associated with the player's location and the origin of their financial resources. A player's nationality, country of residence, and place of birth are key factors in determining risk exposure, as some jurisdictions pose higher financial crime risks than others.

Countries are considered high-risk if they:

- Lack a robust AML/CFT framework.
- Have high levels of corruption.
- Are subject to international sanctions due to terrorism financing or involvement in the proliferation of weapons of mass destruction (WMDs).
- Are known to harbor terrorist organizations or provide financial support for terrorism.

Trusted Sources for Identifying High-Risk Jurisdictions

To assess geographical risks, the Company refers to reputable international regulatory bodies and recognized independent organizations, including:

- Financial Action Task Force (FATF) Reports
- High-Risk Jurisdictions Subject to a Call for Action.
- Jurisdictions Under Increased Monitoring.
- Caribbean Financial Action Task Force (CFATF) Public Statements.
- U.S. Department of State – International Narcotics Control Strategy Report (INCSR):
- Identifies Jurisdictions of Concern and Primary Concern.
- European Commission's List of High-Risk Third Countries:
- Highlights jurisdictions with strategic deficiencies in AML/CFT regulations.
- Office of Foreign Assets Control (OFAC) Sanctions List:
- Includes countries subject to U.S. financial restrictions due to terrorism, proliferation activities, or other national security threats.
- Reports from Credible Global Organizations:
- Countries identified as sponsors of terrorism or as hosting terrorist organizations.
- Transparency International's Corruption Perceptions Index (CPI), which ranks countries based on their levels of corruption.

11. Risk Categorization and Policy Implementation

To effectively manage geographical risk, the Company maintains a structured risk classification system, categorizing countries into high-risk and low-risk groups. This classification is used to:

Apply enhanced due diligence (EDD) measures for players from high-risk jurisdictions.

12. Consequences of CDD Non-Compliance

If a customer fails to submit the required documentation within 30 days after reaching the transaction threshold, the following measures are taken:

- The business relationship is terminated.
- If there are grounds for suspicion of ML or TF, a Suspicious Transaction Report (STR) is filed with the Financial Intelligence Unit (FIU);
- In the absence of suspicion, any remaining funds are returned to the source of deposit (e.g., the original bank account or digital wallet);
- Where suspicion persists, internal policies determine whether funds should be frozen pending further investigation, ensuring compliance with applicable law.
- Records of the terminated relationship are securely stored for at least 5 years.

13. Preventing Tipping-Off

The Company is conscious of the legal prohibition against tipping-off under AML/CTF legislation. Measures such as account restrictions or termination are assessed carefully to avoid alerting customers prematurely. Internal procedures guide staff on how to manage communication and actions in a way that respects confidentiality and regulatory obligations.

By integrating timely, risk-based, and proactive CDD practices into its operations, the Company ensures comprehensive adherence to AML/CTF/CPF standards, minimizes exposure to financial crime, and fosters a secure and transparent environment for both digital and physical gaming channels.

14. Ongoing Due Diligence

CDD procedures are actively applied to both new and existing customers. Central to this approach is the ongoing monitoring of transactions and the periodic reassessment of client risk profiles to ensure that the customer's activity remains within acceptable parameters.

14.1. Remediating Gaps in Historical Due Diligence

In cases where clients were initially onboarded without full CDD being completed—often due to historical onboarding practices—the Company undertakes corrective action as follows:

- Customers classified as high-risk are given priority for immediate identity and risk reassessment.
- Full CDD is applied systematically at intervals based on the specific risk rating assigned to the customer.

By ensuring that customer profiles are consistently reviewed and verified over time,The Company strengthens its AML/CTF/CPF compliance posture, mitigates exposure to financial crime, and maintains a secure and transparent environment within its gaming operations.

The company's due diligence efforts are designed to uncover indirect or covert attempts to engage with sanctioned parties or jurisdictions. Any discovered evasion tactics are swiftly reported to the relevant authorities, and corrective actions, including transaction suspensions and account reviews, are promptly implemented. Regular audits and ongoing staff training further ensure that the company remains vigilant and compliant with the latest legislative requirements and best practices for preventing sanctions evasion.

15. Ongoing Monitoring

Ongoing Monitoring is a critical component of the Company's AML/CTF framework and serves to ensure that customer activity remains consistent with their known risk profile, financial behavior, and source of funds, while their identification information is up-to-date and adequate. The scope of ongoing monitoring is to ensure that the client identification is held up to date and that transactions are also in line with the profile of the client.

15.1. Objectives of Ongoing Monitoring:

- Ensure that transactions conducted are consistent with the customer's known profile, source of funds, and gaming behavior.
- Detect unusual, complex, or structured transactions that may indicate money laundering, terrorist financing, or other financial crime.
- Identify changes in customer behavior that may warrant a re-assessment of risk level and the application of Enhanced Due Diligence (EDD) measures.
- Prevent misuse of outdated or falsified documentation
- Fulfill regulatory obligations under Curaçao's AML legislation and guidance from the Financial Intelligence Unit (FIU).

15.2. Monitoring Customer Identity

The Company implements a range of proactive measures to ensure that identification records remain valid and trustworthy:

- Based on a customer's risk rating, the Company may require updated identification documents at regular intervals.
- This includes resubmission of personal ID, proof of address, and payment method confirmation.

The Company initiates re-verification of identity data upon key events such as:

- Change of address or contact information;
- Addition of a new payment instrument;
- Reclassification of the customer to a higher risk;
- Expiry of previously submitted documents.

Not all changes require full re-verification. The Compliance Department assesses, on a **risk-sensitive basis**, whether an update in identification data is:

- **Minor** (e.g., phone number update), which may be logged without further action;
- **Substantial** (e.g., name change, new jurisdiction), requiring re-confirmation of identity, possible re-onboarding, or enhanced scrutiny.

15.3. Transaction Monitoring

The Company performs continuous surveillance of transactions, account activity, and behavioral indicators to promptly detect any unusual or suspicious patterns.

Monitoring is both automated and manual, utilizing predefined thresholds, behavioral analytics, and IP analysis to identify the following red flags in the customer behavior:

- Unusual betting patterns with players placing large bets on low-risk games or frequently changing betting patterns.
- Frequent large transactions.
- Rapid deposit and withdrawal cycles with criminals depositing large sums to their accounts and withdrawing them quickly.
- Multiple accounts and IP addresses for conducting transactions
- Activities inconsistent with declared income or location

High-risk customers are subject to more frequent and in-depth reviews, with monitoring cycles conducted monthly, while medium- and low-risk customers are reviewed semi-annually or annually, respectively. In cases where anomalies are detected, such as activity inconsistent with declared income or geographic risk indicators, transactions may be temporarily suspended, escalated to the Compliance Officer (MLRO), and, where necessary, reported to the Financial Intelligence Unit (FIU).

Enhanced Ongoing Monitoring is also applied to clients associated with high-risk jurisdictions, PEPs, or those under investigation for previously flagged behavior. This approach ensures early detection of suspicious activity and enables timely intervention in accordance with applicable laws and internal risk mitigation procedures.

15.4. Tailored Risk-Based Measures

For customers who were initially onboarded with incomplete or minimal due diligence, the Company conducts retrospective reviews. This includes:

- Re-evaluating and updating records for customers identified as having elevated risk;
- Scheduling routine updates to ensure that all stored data reflects the latest regulatory requirements and customer status.

The Company re-applies full CDD measures in any of the following circumstances:

- A significant shift in the customer's behavior or profile, such as initiating unusually large or complex transactions, moving into a high-risk jurisdiction, or being reclassified as a Politically Exposed Person (PEP);
- Regulatory or legal updates requiring refreshed or additional customer information;
- When a pre-existing customer initiates a transaction or series of transactions that meet or exceed the company’s defined threshold of XCG 4,000, thereby activating the full CDD requirement under the firm’s AML policy.

16. Reporting of Unusual Transactions

The Company is required to abide by the National Ordinance for Identification of Services and also required to detect and report either intended or completed unusual transactions. The Company pays attention to any activity which they regard as likely, by its nature, to be related

to money laundering and/or terrorist financing, and in particular to complex or unusually large transactions, and all unusual patterns of transactions which have no apparent economic or visible lawful purpose, and any relationships or monetary operations with customers from third countries in which, based on the information officially published by international intergovernmental organizations, money laundering and/or terrorist financing prevention measures are insufficient or do not correspond to international standards. The Company examines the basis for and purpose of the execution of such operations or transactions and the results of the investigation that must be recorded in writing.

Compliance Officer (MLRO) must report to the Financial Intelligence Unit Curaçao any suspicious or unusual monetary operations or transactions. The Company and its employees and/or representatives and/or the person who acted on their behalf are not liable for damage caused to a person or customer participating in a transaction made in economic or professional activities, in performing a professional act on the provision of a professional service:

- upon performance of duties and obligations arising from AML and TF regulations in good faith, from failing to make the transaction or from failing to make the transaction within the prescribed time limit.
- in connection with the performance of the duty to report in good faith.

The following transactions or intended transactions are deemed unusual:

- cases where it is aware of, obtains information concerning, has suspicions or has substantial grounds to suspect that money laundering and/or terrorist financing was, is, or will be performed, or it has been attempted.
- cases where they have suspicion or sufficient grounds to suspect that the customer's funds have been obtained from criminal activity.
- cases where they have a suspicion or sufficient grounds to suspect that the transactions or activities are related to terrorist financing.
- transactions by or on behalf of a person who is named on a list adopted by virtue of the Sanctions National Ordinance (N.G. 2014 no. 55).
- transactions in the amount of XCG 5,000 or more (such a transaction may be a single transaction or a series, combination or pattern of transactions involving a total amount of the monetary equivalent of XCG 5,000 or more and is considered per gaming day.

There are indicators helping to identify unusual transactions. Indicators describe when a transaction (executed or intended) is to be labeled as unusual and thus must be reported to the Financial Intelligence Unit Curaçao without delay. The term "without delay" is interpreted as follows:

The Compliance Officer (MLRO) should send unusual transaction reports without delay after the transaction has been executed, or after there has been an intention of a transaction.

In individual cases, the reporting to the Financial Intelligence Unit Curaçao might be extended to a maximum of 5 working days. A request for extended reporting should be directed in writing to the Financial Intelligence Unit Curaçao, stating the reasons for the extension.

The Financial Intelligence Unit Curaçao will inform the respective reporting entity in writing of its decision within 24 hours.

The time period between the execution of the transaction (or the intention to execute a transaction) and the moment the Compliance Officer (MLRO) receives the report should not exceed 24 hours.

As of the moment that the Compliance Officer (MLRO) receives the transaction report, he has to complete the relevant research with regard to a possible Money Laundering/Terrorism Financing immediately without delay.

If, after the research period (maximum of 10 working days), there is a suspicion of Money Laundering/Terrorism Financing, the Compliance Officer (MLRO) must report the transaction immediately without delay to the Financial Intelligence Unit.

In the case it is not possible to comply with the above-mentioned time periods, the Compliance Officer (MLRO) shall send a request for reporting extension in writing to the Financial Intelligence Unit Curaçao, stating the reasons for this extension.

The Financial Intelligence Unit Curaçao will evaluate objective grounds and inform the reporting entity of its decision in writing within 48 hours upon receiving the request.

There are two kinds of indicators: objective and subjective.

In case of an objective indicator, it describes the mandatory conditions under which circumstances a transaction is to be considered unusual.

In case of a subjective indicator, the transaction is considered unusual if the reporting entity (based on its knowledge of its clients, their income and their business activities, and any other circumstance that may be relevant) has reasonable indications to presume that a transaction is related to money laundering or terrorism financing. For subjective indicators, red flags can be suggested by the supervisors and/or the FIU Curaçao that indicate such possible presumptions.

A report to the FIU is submitted via GoAML reporting portal (link to register in GoAML - https://portal.fiucuracao.cw/goAMLWeb_PRD/Home)

The structural unit of the Company, a member of a management body and an employee are prohibited to inform a person about a report submitted on them to the Financial Intelligence Unit, a plan to submit such a report or the occurrence of reporting as well as about any precept made by the Financial Intelligence Unit or about the commencement of criminal proceedings.

The Company shall establish a system of measures ensuring that the employees and representatives of the entity reporting of a suspicion of money laundering or terrorist financing to the Financial Intelligence Unit are protected from being exposed to threats or hostile action by other employees, management body members or customers of the Company, in particular from adverse or discriminatory employment actions.

17. AML Compliance Program

The Company has established a formal, risk-based Anti-Money Laundering (AML) Compliance Program that sets the minimum operational and ethical standards for the prevention of money laundering, terrorist financing, and proliferation financing. The program is designed in line with Curaçao's regulatory requirements and relevant international frameworks and reflects the company's proactive approach to financial crime prevention within the gaming industry.

Program Architecture and Principles:

- **Risk-Based Design:**
  The AML program is structured to allocate resources and apply control measures commensurate with the assessed level of risk. Customer, product, geographic, and transactional risks are evaluated continuously to determine the appropriate level of due diligence, oversight, and intervention.

- **Regulatory Alignment:**
  The program is specifically built to comply with the following Curaçao legislative instruments:op
  - The National Ordinance on Identification of Clients when Rendering Services (N.G. 2017, no. 92)
  - The National Ordinance on the Reporting of Unusual Transactions (N.G. 2017, no. 99)
  - The Sanctions National Ordinance (N.G. 2014, no. 55)
  - The Kingdom Sanction Act (N.G. 2016, no. 54)

- **Governance and Accountability:**
  Oversight of the AML Program is entrusted to the appointed Compliance Officer (MLRO), who reports directly to senior management. The Compliance Officer (MLRO) ensures implementation, conducts internal reviews, maintains communication with regulators, and oversees internal reporting channels.

- **Internal Controls and Independence:**
  AML compliance controls are embedded across key operational functions and are supported by independent monitoring. Systematic checks are enforced on transactions, onboarding, and payments to detect anomalies before escalation is required.

- **Escalation and Account Blocking Protocols:**
  When there is a reasonable suspicion of money laundering, the Company has a zero-

tolerance policy. The Compliance Officer is empowered to:

- Immediately block the account.
- Suspend access to funds,
- Initiate a full internal investigation, and
- If necessary, report the case to the Financial Intelligence Unit (FIU) as per legal obligation. These steps are taken without notifying the customer, in accordance with anti–tipping off provisions.

- **Program Review and Adaptation:**
  The AML Compliance Program undergoes a formal review annually or upon any significant legal, technological, or business model change. Feedback from internal audits, staff training assessments, and regulatory inspections are used to enhance the policy's effectiveness and relevance.

18. Independent Audit of the AML/CFT Framework

By default, the AML program of the operator shall be monitored and evaluated annually by an outside independent organization specializing in AML audits or an independent department of the operator duly qualified to carry out such functions.

The minimum expertise requirements to the auditor are:

- 2 years of experience in AML/CFT compliance
- bachelor’s degree
- relevant AML certification. - such as the CAMS or CAMS-Audit certification from the ACAMS or AMLFC certification from the AML Foundation & Compliance Institute.

In any case, to be recognized as independent, the audit shall be performed by people not involved with the formulation and execution of the operator’s AML or being influenced by AML compliance staff.

The auditing entity/department reports directly to the Board of Directors and specially designated supervisory officers.
Subjects of the independent AML audit:

- Evaluation of AML/CFT policies and manuals;
- Customer file;
- Compliance management;
- Performance of transaction;
- Employee training adequacy;

- Compliance with applicable laws and regulations;
- Unusual activity monitoring systems;
- Transaction handling staff and management;
- Cases of EDD due to unusual transactions on and beyond the threshold and the subsequent actions;
- Record retention measures;
- Measures taken to resolve previously found issues.

19. Examination by the Gaming Control Board

The operator shall be at all times ready for an inspection by the Curacao Gaming Control Board - both as a comprehensive examination, preparation to one or as a standalone request throughout the year.

The following information must be readily available for such occasions:

- A written and approved AML Compliance Program on money laundering, terrorist financing and financing of proliferation;
- Records of its Business Risk assessment;
- The name of each Compliance Officer responsible for the casino's overall money laundering and terrorist financing policies and procedures and his/her designated job description;
- Records of reported unusual transactions;
- Records of unusual transactions which required closer investigations;
- Records of frozen accounts;
- Schedule of the training provided to the casino's personnel regarding money laundering, terrorist financing and proliferation of weapons;
- The assessment report on the casino's policies and procedures on money laundering, terrorist financing and financing of proliferation by the internal audit department or an external auditor;
- The customer's files including customer risk assessment, CDD, customer acceptance and transaction information.

The operator is fully committed to cooperate with Curacao Gaming Control Board in the course of its AML/CFT examinations and cooperate with them to full extent.

20. Compliance and Consequences of Non-Compliance

The Company enforces a strict culture of compliance to ensure adherence to applicable laws, including Curaçao's AML and sanctions regulations, and to protect its operations from financial crime, legal exposure, and reputational damage. Compliance with this AML/CTF Policy is

mandatory for all employees, officers, agents, contractors, and third parties acting on behalf of the Company. Any failure to comply with AML/CTF obligations—whether intentional or due to negligence—may result in serious consequences.

Internally, such breaches can lead to disciplinary action up to and including termination of employment or contract.

From a regulatory standpoint, non-compliance may trigger financial penalties, regulatory sanctions, license revocation, civil litigation, or criminal prosecution against the Company or individuals involved.

Additionally, failure to act upon or report suspicious activity may result in personal liability for the employee or officer responsible. The Company is committed to proactively identifying, investigating, and remedying compliance breaches and will fully cooperate with relevant authorities in any enforcement proceedings.

Employees are therefore required to immediately report any actual or suspected violations of this policy to the Compliance Officer (MLRO) without delay.

21. Related Information

This policy should be read in conjunction with the following legal, regulatory, and operational frameworks, which provide the basis for the Company's AML/CTF obligations and activities:

21.1. International and Regional Legal Instruments

- **EU Directive 2015/849:** *Directive of the European Parliament and of the Council of 20 May 2015 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing.*
- **EU Regulation 2015/847:** *Regulation on information accompanying transfers of funds.*
- **EU Sanctions Framework:** *Various regulations imposing sanctions or restrictive measures against persons and embargo on certain goods and technologies, including all dual-use goods.*

21.2. National Legislation – Curaçao (CW)

- Regulation for the combating of ML/FT and Proliferation of weapons of mass destruction
- The National Ordinance on Identification of Clients when Rendering Services (N.G. 2017, no. 92)
- The National Ordinance on the Reporting of Unusual Transactions (N.G. 2017, no. 99)
- The Sanctions National Ordinance (N.G. 2014, no. 55)
- The Kingdom Sanction Act (N.G. 2016, no. 54)

21.3. National Legislation – Belgium (BE)

- **Law of 18 September 2017:** *Law on the prevention of money laundering and the limitation of the use of cash.*

21.4. Other Reference Tools and Systems

- **goAML Portal:** https://portal.fiucuracao.cw
- **UN Sanctions Overview:** https://www.un.org/securitycouncil/sanctions/information
- **OFAC Sanctions Lists:** https://www.treasury.gov/ofac
- **EU Sanctions Portal:** https://www.sanctionsmap.eu
- **OFSI UK Sanctions Implementation:** https://www.gov.uk/government/organisations/office-of-financial-sanctions-implementation

22. Contact Information

For any questions regarding this policy, please contact:

Compliance Department, POINDER B.V.
Address: Z/N, ZUIKERTUINTJEWEG, WILLEMSTAD, Curacao
Email: support-en@najahbet.com

23. Approvals

Managing director

IGA TRUST B.V.

Compliance Officer

Digitally signed by INNA HONCHARUK
Date: 2025.12.05 15:57:02 +02'00'

Inna Honcharuk

24. Version History

Revision No.	Effective dates
6	28.11.2025 (current)
5	14.08.2025
4	26.07.2025
3	05.02.2025
2	09.09.2024
1	30.01.2024

List of changes:

3.2.1. - Added Employee Screening

3.2.2. - Added Employee Training

3.3. - Expanded Compliance Officer

5.1 - Expanding the BRA section and contents

5.2 - Expanding the CRA section and contents

5.3 - Added Technological developments risk assessment

6.1 - Expanded Simplified CDD

6.5.1. - Added Syndicates

6.5.2. - Added Corporate Accounts

7 - Added Reliance on 3rd parties

18 - Added Independent Audit of the AML/CFT Framework

19 - Added Examination by the Curacao Control Board

other - 48 hours timeline for reporting changed to immediately without delay

28.11.25 - AML CTF POLICY (REVISION 6) - POINDER B.V. - E-SIGNED I. HONCHARUK (1)

Final Audit Report 2025-12-12

Created:	2025-12-12
By:	Mónica Paola Botero (monica@igatrust.com)
Status:	Signed
Transaction ID:	CBJCHBCAABAA39s8YMdBstuFP7CkqKoGUxY3mwbL660b

"28.11.25 - AML CTF POLICY (REVISION 6) - POINDER B.V. - E-SIGNED I. HONCHARUK (1)" History

Document digitally presigned by INNA HONCHARUK (innahoncharuk78@gmail.com)
2025-12-05 - 1:57:02 PM GMT- IP address: 161.22.50.199

Document created by Mónica Paola Botero (monica@igatrust.com)
2025-12-12 - 2:19:49 PM GMT- IP address: 161.22.50.199

Document emailed to Claire Godschalk (Claire@igatrust.com) for signature
2025-12-12 - 2:20:40 PM GMT

Email viewed by Claire Godschalk (Claire@igatrust.com)
2025-12-12 - 3:55:14 PM GMT- IP address: 161.22.50.199

Document e-signed by Claire Godschalk (Claire@igatrust.com)
Signature Date: 2025-12-12 - 3:55:39 PM GMT - Time Source: server- IP address: 161.22.50.199

Agreement completed.
2025-12-12 - 3:55:39 PM GMT