

POLIGON ENTERTAINMENT N.V.

Anti-Money Laundering and Counter-Terrorist Financing Policy

AML/CFT Policy

Poligon Entertainment N.V. (the "Company")

Company registration number: 132517

Curaçao Gaming Control Board B2C License holder OGL/2024/815/0653

Issued on January 10th, 2025

Expires on February 23rd, 2027

Table of Content

Section	Title	Page
1	Policy Statement	4
2	Purpose	5
3	Audience	6
4	Definitions	7
5	Policy Implementation	8
5.a	Business Risk Assessment	9
5.b	Customer Risk Assessment	11
5.c	Customer Acceptance Policy	13
5.d	Customer Due Diligence	15
5.e	Ongoing Monitoring	17
5.f	Reliance on Third Parties for Customer Due Diligence	18
5.g	Reporting of Unusual Transactions	20
5.h	Anti-Money Laundering Compliance Program	22
6	Compliance and Consequences of Non-Compliance	25
7	Related Information	26
8	Contact Information	27
9	Policy History	28

Senior Administrator responsible for approving this policy – The Board of Directors of the Company, in line with Section V.2 of the AML Regulations, is responsible for reviewing and approving this Policy and ensuring it reflects the Company's commitment to AML/CFT compliance.

Officer responsible for policy dissemination, updates, and reviews – Kalina Kichukova - The designated AML/CFT Compliance Officer of the Company, appointed in accordance with Section V.3 of the AML Regulations. This officer is a senior management-level person, independent from gaming operations, and responsible for the implementation, communication, and updating of the policy.

Effective date – January 10th, 2025.

Next review date – January 10th, 2026, or earlier if triggered by a significant change in operations, regulations, or risk profile, in line with Section II.2.1 of the AML Regulations which requires at least annual review or ad hoc updates upon material changes.

1. Policy statement

The Company is committed to preventing the use of its operations for money laundering, terrorist financing, or any other form of financial crime. This Anti-Money Laundering and Counter-Terrorist Financing (AML/CFT) Policy sets out the Company's internal framework for identifying, managing, and mitigating risks associated with financial crime across all areas of its business.

This Policy applies to all directors, officers, employees, and any third parties acting on behalf of the Company. It governs the Company's approach to customer due diligence, transaction monitoring, internal reporting, and regulatory compliance in accordance with applicable laws, including the NOIS and NORUT.

2. Purpose

The purpose of this Anti-Money Laundering and Counter-Terrorist Financing (“AML/CFT”) Policy is to set out the framework adopted by the Company (“the Company”) to prevent the use of its platform for money laundering, terrorist financing, and other forms of financial crime.

This Policy reflects the Company’s commitment to maintaining integrity in its licensed online gambling operations, and ensuring full compliance with applicable laws and regulatory expectations, including:

- The **National Ordinance on the Reporting of Unusual Transactions (NORUT)**;
- The **Regulations for the combating of Money Laundering, the Financing of Terrorism and Proliferation of weapons of mass destruction** applicable to Curaçao casinos and providers of other online games (the “AML Regulations”)
- The **National Ordinance on the Identification when Rendering Services (NOIS)**;
- The **Ministerial Decree on Indicators for Unusual Transactions**;
- The **Curaçao Gaming Control Board (GCB) Requirements for Compliance Officer**, dated January 15, 2025;
- Relevant **Financial Action Task Force (FATF) Recommendations**.

The Company applies a **risk-based approach** to managing its AML/CFT obligations, focusing controls where risks are greatest and maintaining proportionate systems to detect, mitigate, and report unusual or suspicious activity. This Policy also outlines the Company’s ongoing risk assessment procedures, customer due diligence requirements, internal reporting channels, transaction monitoring mechanisms, and governance structures, including the designation of a qualified and independent Compliance Officer.

The Policy is binding on all Company personnel and business units. It serves to:

- Guide operational decisions that may affect AML/CFT compliance;
- Educate staff on their roles, responsibilities, and reporting duties;
- Ensure that the Company meets its legal and regulatory obligations;
- Protect the Company, its employees, and stakeholders from reputational and legal risk.

The Policy is reviewed at least annually and updated as necessary to reflect changes in legal requirements, regulatory guidance, and business operations.

3. Audience

This Policy applies to all employees, directors, contractors, and outsourced service providers of the Company who are involved in any aspect of customer onboarding, payment processing, risk management, compliance, or operational decision-making. For the avoidance of doubt, it also extends to any person performing AML/CFT functions or oversight on behalf of the Company.

4. Definitions

Term	Definition
AML	Anti-Money Laundering
AML Regulations	Regulations for the combating of Money Laundering, the Financing of Terrorism and Proliferation of weapons of mass destruction. Applicable to Curaçao casinos and providers of other online games, January 2025.
Beneficial Owner	A natural person who ultimately owns or controls a customer or on whose behalf a transaction is being conducted, as defined in Article 1(g) of the AML Regulations.
BRA	Business Risk Assessment
CAP	Customer Acceptance Policy
CDD	Customer Due Diligence
CRA	Customer Risk Assessment
CTF	Counter-Terrorist Financing
EDD	Enhanced Due Diligence
FIU Curaçao	The Financial Intelligence Unit of Curaçao, responsible for receiving, analyzing, and disseminating reports of unusual transactions under NORUT.
GCB	Curaçao Gaming Control Board
KYC	Know Your Customer
ML	Money Laundering
NOIS	National Ordinance on the Identification when Rendering Services
NORUT	National Ordinance on the Reporting of Unusual Transactions
PEP	Politically Exposed Person
SAR	Suspicious Activity Report
TF	Terrorist Financing
Unusual Transaction	Any transaction that deviates from the customer's normal pattern, has no economic rationale, or appears to involve criminal proceeds.

5. Policy Implementation

a. Business Risk Assessment

The Company conducts a comprehensive and structured Business Risk Assessment (“BRA”) on at least an annual basis, and ad hoc whenever significant changes occur in its operations, products, markets, or regulatory environment. The BRA enables the Company to identify and assess its exposure to money laundering and terrorist financing (“ML/TF”) risks across all areas of its business and to allocate appropriate resources to mitigate those risks in line with the AML Regulations and relevant guidance issued by the GCB.

Scope of the BRA

The BRA assesses inherent and residual risks associated with:

- **Products and Services Offered.** The Company evaluates the relative ML/TF risk of each product vertical, such as online casino, virtual games, slots, and table games. Products allowing rapid turnover, frequent wagering, or anonymous play are considered higher risk than those with slower transaction cycles or enhanced verification requirements.
- **Customer Base and User Profile.** The BRA takes into account the composition of the customer base, including the percentage of users classified as high-risk, PEPs, or those from high-risk jurisdictions. The presence of corporate customers, legal entities, or intermediaries is also factored in.
- **Geographic Exposure.** Jurisdictional risk is assessed based on the countries in which the Company markets, onboards, or transacts with customers. This includes review of FATF grey- and black-listed jurisdictions, countries with limited AML oversight, and those subject to sanctions issued by the United Nations, European Union, OFAC, Kingdom of the Netherlands, and any other competent authority applicable to the Company under Curaçao law.
- **Delivery Channels.** Particular consideration is given to the risk of remote onboarding and digital access. Delivery via mobile apps, browser interfaces, and integration with third-party platforms (such as affiliates and skins) increases exposure to impersonation, document fraud, and high-speed abuse.
- **Payment Methods and Funding Channels.** The Company reviews all deposit and withdrawal mechanisms, including crypto-assets, prepaid vouchers, e-wallets, and card payments. Greater weight is placed on methods offering low traceability or speed of fund transfers.
- **Distribution and Outsourcing Arrangements.** The Company considers the risks posed by its use of white-label partners, affiliates, agents, and any outsourced providers involved in onboarding, marketing, or payments. Reliance on third parties for customer-facing roles presents specific due diligence and audit risks.
- **Technology and Infrastructure**
The BRA assesses whether back-office systems, automated controls, and data security infrastructure are sufficient to detect and mitigate ML/TF risks arising from customer behavior or transaction anomalies.

Methodology and Classification

Each risk category is scored based on:

- **Likelihood** (1 to 5): the probability of occurrence, based on historical data and typologies.
- **Impact** (1 to 5): the financial, reputational, and regulatory severity if the risk materializes.

Risk Score = Likelihood × Impact (1 to 25)

Risk Score	Risk Level
1–4	Low
5–14	Medium
15–25	High

For each domain, the Company assigns both an **inherent risk** score and a **residual risk** score, the latter reflecting mitigating controls already in place (e.g., KYC systems, transaction monitoring, geo-blocking tools).

Documentation and Approval

All BRA assessments are:

- Documented in a dedicated risk register maintained by the Compliance Officer;
- Reviewed and approved by the Board of Directors or a designated AML Governance Committee;
- Updated at least once per year, or upon material changes (e.g., introduction of crypto payment rails, expansion into new territories, integration of new B2B partners).

The BRA forms the basis for the Company’s AML/CFT risk appetite, operational procedures, and resourcing decisions (including the use of automated screening and monitoring systems).

b. Customer Risk Assessment

The Company conducts a comprehensive Customer Risk Assessment ("CRA") for every customer prior to the establishment of a business relationship, and updates the assessment as necessary throughout the lifecycle of the relationship. The CRA forms a critical part of the Company's risk-based approach, in line with Curaçao's AML Regulations, and is used to determine the level and nature of due diligence and ongoing monitoring required.

Purpose

The CRA aims to identify customers who may pose a higher risk of being involved in money laundering, terrorist financing, or other financial crime. It ensures that resources are proportionately allocated and that higher-risk relationships are subject to enhanced scrutiny.

Factors Considered

The Company applies both qualitative and quantitative factors in assessing customer risk, including:

- **Geographic Risk:** Whether the customer is a resident or national of, or maintains connections to, a jurisdiction identified by FATF as high-risk or non-cooperative; or subject to sanctions issued by the United Nations, European Union, OFAC, Kingdom of the Netherlands, and any other competent authority applicable to the Company under Curaçao law.
- **Customer Profile Risk:** Nature of the customer (natural person or legal entity), occupation, anticipated gaming activity, and income/funding sources.
- **Delivery Channel Risk:** Use of online onboarding, VPNs, or third-party agents increases risk exposure.
- **Product Use Risk:** Customers accessing high-turnover games (e.g., instant-win games or slots) or using multiple product verticals.
- **Payment Method Risk:** Use of prepaid cards, e-wallets, crypto assets, and mismatched or third-party payment instruments.
- **PEP and Sanctions Risk:** Whether the customer is a politically exposed person ("PEP"), or associated with individuals/entities listed on sanctions lists or adverse media.

Risk Rating Methodology

The Company employs a structured scoring system to calculate a customer's risk profile based on likelihood and impact:

- **Likelihood:** 1 (Rare) to 5 (Frequent)
- **Impact:** 1 (Negligible) to 5 (Severe)

Risk Score = Likelihood × Impact (Range: 1 to 25)

- Low Risk: 1–4

- Medium Risk: 5–10
- High Risk: 11–25

Customers are assigned a risk level based on their final score and grouped accordingly:

- **Low-Risk Customers:** Residents of low-risk countries with full KYC documentation, limited transactional volume, and no red flags. These customers are subject to simplified monitoring.
- **Medium-Risk Customers:** Those exhibiting moderate-risk features such as inconsistent identification details, moderate deposit volumes, or payment from certain high-risk methods. Subject to standard CDD and transaction monitoring.
- **High-Risk Customers:** Include PEPs, those with connections to high-risk jurisdictions, unclear source of funds, adverse media flags, or use of anonymous or high-risk financial instruments. These customers are subject to Enhanced Due Diligence ("EDD"), stricter transaction monitoring, and approval by the Compliance Officer.

Review and Escalation

Customer risk classifications are reviewed:

- Periodically, based on the customer's transactional behavior;
- Upon specific trigger events (e.g., large or unusual transaction, failed verification, sanctions hit);
- When new information comes to light affecting the customer's profile.

Risk level upgrades and overrides may only be performed by senior compliance personnel, and the rationale must be documented and logged. All assessments and decisions are retained for at least five years in accordance with the Company's record-keeping obligations.

CRA outputs are integrated into the customer's profile and drive the applicable level of CDD, EDD, and transaction monitoring.

c. Customer Acceptance Policy

The Company operates a strict Customer Acceptance Policy ("CAP") to prevent access to its services by high-risk or unverified customers and to ensure that all onboarding is conducted in line with Curaçao AML/CFT obligations. The CAP sets out the minimum standards and decision criteria for determining whether a prospective customer may be permitted to open and maintain an account with the Company.

General Requirements

The Company shall not establish or maintain a business relationship with any individual or entity unless:

- Full Customer Due Diligence ("CDD") has been completed;
- The customer has passed identity verification and sanctions/PEP screening;
- There are no material inconsistencies between customer-supplied information and documentary evidence;
- The customer is not located in, or a national of, a jurisdiction subject to sanctions issued by the United Nations, European Union, OFAC, Kingdom of the Netherlands, and any other competent authority applicable to the Company under Curaçao law

Risk-Based Acceptance Controls

Acceptance decisions are made on a risk-sensitive basis:

- **Low-Risk Customers** may be accepted upon successful completion of standard CDD checks.
- **Medium-Risk Customers** are subject to additional scrutiny (e.g., confirmation of source of funds, enhanced screening).
- **High-Risk Customers**, including PEPs or individuals flagged for adverse media or sanctions exposure, require senior Compliance Officer approval before onboarding.

Examples of Disqualifying Factors

The Company will not accept customers who:

- Use proxy services, or TOR browsers to conceal their location or identity;
- Present forged, altered, expired, or unverifiable documentation;
- Provide inconsistent or evasive answers when questioned about personal or financial background;
- Attempt to use third-party payment instruments, unless permitted under verified family or business arrangements;
- Are under the legal age for gambling under applicable laws;
- Are residents of jurisdictions where the Company is not authorized to offer services.

Customer Screening and Review

All prospective customers are screened at onboarding using automated tools and reviewed for:

- Sanctions lists (sanctions issued by the United Nations, European Union, OFAC, Kingdom of the Netherlands, and any other competent authority applicable to the Company under Curaçao law);
- PEP status, including relatives and close associates;
- Negative news or adverse media indicators (manual and automated sources);
- Country of origin, IP address, and geolocation consistency.

Maintenance and Offboarding

Account access remains conditional on continued compliance with the Company's verification requirements. A customer's account may be suspended or closed if:

- KYC documents expire or become invalid and are not refreshed timely;
- New information arises that materially changes the customer's risk profile;
- Requests for personal identity documents, updated source of funds, source of wealth or other KYC documentation are ignored and not provided within 30 days as of the request;
- The customer breaches the Company's AML policies or terms of service.

All onboarding and offboarding decisions are recorded in the customer file with detailed reasoning and supporting evidence.

Acceptance Principles:

- Customers must undergo full identity verification ("KYC") before any deposit or gambling activity.
- Players from sanctioned, embargoed, or otherwise prohibited jurisdictions are rejected.
- Customers flagged by screening tools (PEP/sanctions/adverse media) are reviewed by the Compliance Officer before onboarding.

Examples of unacceptable onboarding:

- Accounts using proxy IP addresses or anonymizing services.
- Customers presenting forged or altered documents.
- Registration data inconsistent with submitted documentation.

Account maintenance is also conditional. Users who fail to comply with KYC refreshes, ongoing verification, or source of funds inquiries may have their accounts suspended or terminated.

d. Customer Due Diligence

The Company performs Customer Due Diligence measures prior to the establishment of a business relationship and in any circumstance required under the appropriate regulations, including the AML Regulations, and when:

- A customer requests account activation or initiates any gameplay;
- A single transaction or series of linked transactions equals or exceeds NAf. 5,000;
- The Company suspects money laundering or terrorist financing, regardless of amount;
- The reliability of previously collected customer data is called into question.

Standard CDD Measures

CDD procedures consist of the following:

- **Identification and verification** of the customer's full name, date of birth, nationality, and residential address using reliable, independent source documents (e.g., government-issued ID and recent utility bill);
- **Verification of payment method ownership**, ensuring payment instruments are held in the customer's name;
- **Screening for PEPs, sanctions, and adverse media**, using automated and manual tools;
- **Identification of the beneficial owner**, where the customer is acting on behalf of another person or is a legal entity;
- **Understanding the nature and intended purpose** of the business relationship (e.g., entertainment, recreational gambling, professional play).

CDD is considered complete only when all required documents are collected, validated, and retained. Customers who fail to complete verification are restricted from accessing gambling services.

Risk-Based Application

CDD is applied with reference to the customer's risk classification. The depth of documentation and verification procedures corresponds to the customer's risk level as determined by the Customer Risk Assessment:

- **Low-Risk Customers:** May be subject to streamlined verification if permitted by law;
- **Medium-Risk Customers:** Require full documentation and positive verification before account use;
- **High-Risk Customers:** Automatically escalate to Enhanced Due Diligence.

Enhanced Due Diligence

EDD is conducted when:

- The customer is classified as high-risk or has links to high-risk jurisdictions;
- The customer is identified as a PEP, a close associate, or a family member of a PEP;
- There are doubts as to the customer's source of funds or source of wealth.

EDD Measures include:

- **Obtaining additional information** on the customer and the intended nature of the relationship;
- **Requesting Source of Funds ("SOF") and Source of Wealth ("SOW")** documentation (e.g., salary slips, company statements, inheritance records);
- **Conducting enhanced ongoing monitoring** of transactions and behavior;
- **Senior management approval** before initiating or continuing a relationship with the customer;
- **Manual verification of payment instruments** and adverse media search expansions.

In all cases, CDD and EDD documentation is retained securely and made available to the Gaming Control Board ("GCB") and Financial Intelligence Unit ("FIU") upon lawful request. CDD records are retained for at least five years after the business relationship ends or from the date of the last transaction.

e. Ongoing Monitoring

Ongoing monitoring is conducted through a combination of automated tools and manual analyst reviews. Monitoring ensures that customer activity remains consistent with their risk profile.

Monitoring Focus:

- Transaction velocity, frequency, and amounts
- Irregular deposit-to-withdrawal ratios
- Inactive or low game participation despite high deposits
- Use of new or unverified payment methods
- Access via flagged jurisdictions or anonymization tools

Monitoring Techniques:

- Real-time alerts and threshold-based flags
- Behavioral anomaly detection systems
- Daily and weekly transaction pattern reports

Escalation:

- Analysts flag events exceeding risk thresholds to the Compliance Officer
- Compliance Officer evaluates whether the event warrants a suspicious activity report ("SAR")

Monitoring outcomes may lead to:

- Account freezing or restriction
- KYC re-verification
- Risk rating escalation
- Reporting to the FIU Curaçao

f. Reliance on third parties to perform customer due diligence

The Company may rely on third parties to perform elements of CDD, provided that such reliance is fully compliant with the AML Regulations applicable in Curaçao, specifically Article 5 of the AML Regulations and relevant provisions of the National Ordinance on the Identification when Rendering Services ("NOIS").

Conditions for Permissible Reliance

Reliance is permitted only where all the following conditions are met:

- The third party is a regulated entity subject to AML/CFT supervision in a jurisdiction with equivalent standards to those of Curaçao;
- The Company is satisfied, through documented assessment, that the third party has adequate procedures for identification, verification, record-keeping, and reporting;
- A **written agreement** is in place requiring the third party to:
 - Immediately provide, upon request, copies of all identification and verification documents;
 - Cooperate in any internal or regulatory investigation concerning the customer;
 - Maintain records in accordance with applicable retention requirements;
 - Notify the Company promptly of any anomalies or red flags identified during onboarding or monitoring.

Internal Oversight and Due Diligence

Prior to relying on any third party, the Compliance Officer shall conduct a formal evaluation of the provider's:

- Licensing (if applicable) and regulatory standing;
- Corporate governance and independence from the customer;
- Track record in AML compliance, including any regulatory findings or sanctions;
- Control framework, including use of screening tools, document validation systems, and ongoing monitoring.

This evaluation is documented and retained for audit purposes. Third parties shall be reviewed periodically (at least annually) to ensure continued reliability.

Scope of Reliance

Reliance may extend to:

- Collection and initial verification of identity documents;
- Screening against PEP and sanctions databases;
- Collection of source of funds information where appropriate.

However, reliance **does not extend** to:

- Ultimate responsibility for the adequacy of CDD;
- Decision-making regarding the acceptance or rejection of the customer;
- Transaction monitoring or escalation of suspicious activity.

These remain the exclusive responsibility of the Company and its appointed Compliance Officer.

Record-Keeping and Audit Trail

The Company maintains a **register of all third-party CDD providers** and logs:

- Dates of reliance arrangements;
- Types of customers verified through each provider;
- Copies of service agreements and audit summaries;
- Results of periodic quality assurance checks or sampling.

All reliance arrangements are subject to internal audit, and deficiencies result in immediate suspension of reliance privileges. In all cases, the Company remains ultimately accountable for compliance with its AML/CFT obligations under Curaçao law.

g. Reporting of Unusual Transactions

The Company complies fully with its legal obligation under the National Ordinance on the Reporting of Unusual Transactions ("NORUT") and the Ministerial Decree on Indicators for Unusual Transactions. All employees, management, and third-party service providers engaged by the Company are obligated to identify, escalate, and support the reporting of any unusual or suspicious transactions or attempted transactions.

Definition of an Unusual Transaction

A transaction is deemed "unusual" if it:

- Deviates significantly from the customer's expected behavior or risk profile;
- Has no clear economic or lawful purpose;
- Involves unusually large amounts or structured transactions designed to avoid regulatory thresholds;
- Transactions in the amount of NAF 5,000 or the equivalent in other currencies or payment forms, whether conducted in a single transaction or through a series, combination, or pattern of transactions aggregated within a 24-hour period, shall be flagged for review under the Company's transaction monitoring system. All flagged transactions shall be reviewed by the Compliance Officer to determine whether they constitute an unusual transaction under applicable law and whether reporting to the Financial Intelligence Unit (FIU) is required. The existence of the threshold shall not automatically trigger reporting; however, it shall trigger mandatory compliance assessment and documentation;
- Raises suspicion of being linked to criminal proceeds, terrorist financing, or circumvention of AML controls.

Indicators may be quantitative (e.g., size, frequency, velocity) or qualitative (e.g., reluctance to provide documents, contradictory explanations, adverse media).

All unusual transactions or intended unusual transactions shall be reported internally to the Compliance Officer without delay, together with all relevant supporting documentation and transaction information.

The Compliance Officer shall review internally reported transactions and assess whether there are knowledge, suspicion, or reasonable grounds to suspect money laundering or terrorist financing (ML/TF).

Where such grounds exist, the transaction shall be reported externally to the FIU through the prescribed reporting channel (e.g., goAML) without undue delay.

Where the transaction is determined not to require external reporting, the Compliance Officer shall document the assessment, record the rationale for the decision, and formally approve and sign off on the file.

Internal Escalation Procedure

1. Employee Duty to Report

All relevant personnel are trained to recognize red flags and must escalate concerns to the Compliance Officer immediately upon detection. This applies to:

- Transactions that match typologies from the Ministerial Decree;
- Behavior inconsistent with the customer's known source of funds or declared profile;
- Use of forged or altered identity documents;
- Deposits followed by no gameplay and immediate withdrawal;
- Use of high-risk or anonymous funding methods (e.g., crypto, prepaid cards).

2. Completion of Internal SAR The employee completes an internal SAR using the Company's approved form. The SAR must include all relevant transaction details, KYC file information, and a brief narrative explaining the reason for suspicion.

3. Compliance Officer Review and Assessment

The Compliance Officer must review the SAR within a reasonable timeframe and determine whether the transaction meets the threshold for reporting to the FIU Curaçao. In cases of urgency or risk of asset flight, the Compliance Officer may recommend temporary suspension of the customer account pending investigation.

External Reporting to the FIU

Where an unusual transaction meets the reporting threshold under Curaçao law, the Compliance Officer must submit a report via the system maintained by FIU Curaçao.

All reports must:

- Be submitted promptly and in the prescribed format;
- Include supporting documentation, transaction records, and customer profile information;
- Be retained in a secure register for a period of no less than five years.

The Compliance Officer maintains a log of:

- All internal SARs (regardless of whether they are reported externally);
- The outcome of each review;
- Dates of submission to the FIU Curaçao and relevant reference numbers.

Prohibition on Tipping-Off

Tipping-off is strictly prohibited. No employee or third party may disclose to the customer, or any unauthorized individual, that a report has been made or that their transactions are under investigation. Violation of this rule may result in disciplinary action and may constitute a criminal offense under Curaçao law.

Training and Testing

The Company provides specific training to all relevant staff on how to identify, escalate, and handle unusual transactions, including real-case simulations, red flag indicators, and procedural walk-throughs. The effectiveness of the reporting framework is assessed annually through internal audit reviews and Compliance Officer compliance assessments.

h. Anti-Money Laundering Compliance Program

1. The Company's AML/CFT Compliance Program is governed by the appointment and oversight of a designated **Compliance Officer**, in line with the Curaçao Gaming Control Board's January 2025 guidance. The Compliance Officer:
 - May not simultaneously serve in any conflicting operational roles, including UBO, CEO, CFO, COO, Casino Manager, or Internal Auditor, in order to preserve independence and avoid conflicts of interest;
 - Must receive a minimum of **10 hours of AML-specific training annually**, including GCB workshops and industry updates;
 - Has direct access to customer identification and transaction data, the authority to act independently, and the obligation to advise management of compliance weaknesses.
2. The Compliance Officer is responsible for:
 - Verifying adherence to local laws and regulations regarding the detection and deterrence of money laundering and terrorist financing;
 - Reviewing compliance with the casino's AML/CFT policies and procedures;
 - Analyzing transactions and determining whether any meet the reporting thresholds under the Ministerial Decree on Indicators for Unusual Transactions;
 - Maintaining records of unusual transactions reported both internally and externally;
 - Developing internal procedures for determining when the reporting of unusual transactions should result in account blocking or freezing, while mitigating the risk of tipping off the player.
 - Designing, implementing, and revising the AML/CFT program;
 - Conducting internal investigations into unusual transactions;
 - Coordinating employee training and awareness campaigns;
 - Submitting reports to the FIU and maintaining a complete record of SARs and internal reporting;
 - Issuing periodic internal reports to management on AML/CFT controls and risks;
 - Recommending account freezing or blocking procedures for suspect accounts, as needed;
 - Monitoring global AML/CFT developments and updating internal frameworks accordingly.
3. Employee Screening Program
 - Verifying that prospective employees do not have a criminal record prior to hiring;
 - Conducting periodic background checks on existing employees;

- Initiating background checks whenever suspicion arises regarding an employee's conduct or suitability.

4. Employee Training Program

New Employee Training:

- Identifying and reporting unusual transactions;
- Understanding money laundering typologies relevant to online gaming;
- Applying customer due diligence and enhanced due diligence procedures;
- Familiarization with this AML/CFT Policy.

Audit Staff Training:

- Monitoring regulatory developments;
- Identifying emerging money laundering risks and enforcement trends;
- Assessing the impact of such developments on the Company.

AML Compliance Staff Training:

- Monitoring regulatory developments;
- Identifying emerging money laundering risks and enforcement trends;
- Assessing the impact of such developments on the Company;
- Participating in AML-focused conferences, both in-person and online.

Supervisors and Managers Training:

- Understanding and implementing this AML/CFT Policy.
- Senior Management and Board of Directors Training:
- Receiving regular and comprehensive briefings on AML/CFT-related risks and obligations.

Refresher Training:

- Delivered periodically based on regulatory updates, market developments, and internal incidents or assessments.

5. Record Keeping

- Maintaining a register of trained personnel, including dates of training and the subjects covered.

6. Independent Audit Function to Test the AML Compliance Program

- Conducted at least annually;
- Performed by an independent party;
- Auditor qualifications must meet the requirements of Section V.5 of the AML Regulations.

7. Examination by the GCB

- Subject to oversight and examination by the Gaming Control Board in accordance with applicable regulations.

6. Compliance and Consequences of Non-Compliance

The Company will ensure that the appointed Compliance Officer adheres to the **mandatory qualifications, independence rules, and reporting functions** under the appropriate legislation and regulation, as well as the AML regulations.

The Company will take appropriate disciplinary measures against employees who fail to comply with AML obligations or internal policies.

7. Related Information

This Policy should be read in conjunction with:

- **The National Ordinance on the Reporting of Unusual Transactions**
- **The National Ordinance on Identification for Services**
- **The Curaçao Gaming Control Board AML/CFT Compliance Guidance (January 2025)**
- **FATF Recommendations and Guidance**

8. Contact Information

Designated Compliance Officer

Name: Kalina Kichukova

Email: compliance@poligonentertainment.com

Phone: 359895549907

9. Policy History

Version	Effective Date	Approved By	Summary of Changes
1.0.	10 th of January 2025	Victoria Vlahova-Koleva and Kalina Kichukova	
1.1	23 rd of February 2026	Kalina Kichukova	• Addition of a Transaction Threshold in Section (g). • Amendment of Transaction Threshold in Section (d), point 2.

