

Anti-Money Laundering and Counter-Terrorism Financing (AML/CTF) Policy

1. Policy Statement

Progress Path Co N.V. (Casino) is firmly committed to preventing its platform, services, and operations from being used for money laundering, terrorist financing, or any activity that facilitates financial crime. This Anti-Money Laundering and Counter-Terrorism Financing (AML/CTF) Policy (Policy) outlines the principles and procedures implemented to ensure full compliance with all applicable laws and regulations in Curaçao, including the National Ordinance on the Prevention and Combating of Money Laundering and Terrorist Financing (NOIS) and the National Ordinance on the Reporting of Unusual Transactions (NORUT).

The Policy applies to:

- All employees across all departments and levels;
- Subcontractors, third-party service providers, and affiliates;
- All aspects of the Casino's products, services, and customer interactions.

The scope of this Policy covers:

- Customer due diligence (CDD) and enhanced due diligence (EDD);
- Risk assessment and risk-based approach;
- Ongoing monitoring of transactions and business relationships;
- Detection and reporting of unusual activities to the FIU Curaçao;
- Employee training, internal controls, and record-keeping procedures.

By enforcing this Policy, the Casino seeks to protect its business integrity, uphold its licensing obligations, and contribute to the global effort to combat financial crime. Compliance with this Policy is mandatory and non-negotiable.

2. Purpose

The purpose of this Anti-Money Laundering and Counter-Terrorism Financing (AML/CTF) Policy is to establish a clear and structured framework that enables the Casino to detect, prevent, and report any activity related to money laundering, terrorist financing, and proliferation financing. The Policy sets out the minimum standards, roles, and responsibilities required to ensure compliance with all relevant legal and regulatory obligations under the jurisdiction of Curaçao.

This Policy is designed to ensure full compliance with:

- The National Ordinance on the Prevention and Combating of Money Laundering and Terrorist Financing (NOIS) (N.G. 2017 no. 92);
- The National Ordinance on Identification of Clients when Rendering Services (N.G. 2017, no. 92);
- Ministerial Decree with general operation of November 11, 2015, laying down the indicators as mentioned in article 10 of the National Ordinance on the Reporting of Unusual Transactions (Regulation Indicators Unusual Transactions) (N.G. 2015, no. 73);

- The National Ordinance on the Reporting of Unusual Transactions (NORUT) (N.G. 2017, no. 99);
 - Regulatory requirements of the Financial Intelligence Unit (FIU) Curaçao;
 - Sanction National Ordinance (N.G. 2014, no. 55);
 - Kingdom Sanction Act (N.G. 2016, no. 54);
 - Regulations for the combating of Money Laundering, the Financing of Terrorism and Proliferation of weapons of mass destruction;
 - International standards issued by the Financial Action Task Force (FATF).
- These laws and standards obligate the Casino to adopt risk-based procedures for customer due diligence (CDD), monitoring of transactions, and reporting of unusual activities.

By implementing this AML/CTF Policy, the Casino aims to:

- Ensure all employees understand and fulfill their legal and regulatory obligations;
- Apply a risk-based approach to customer due diligence, transaction monitoring, and reporting of unusual activity;
- Foster a culture of compliance, transparency, and accountability across all levels of the organization.

This Policy is integral to the Casino's overall risk management strategy and contributes to the global effort to combat financial crime.

From a business perspective, this Policy aims to:

- Protect the integrity of the Casino's operations by preventing the platform from being exploited by criminal actors;
- Safeguard the Casino's reputation with customers, financial institutions, and regulatory authorities;
- Maintain eligibility for operating licenses and business partnerships by demonstrating compliance;
- Ensure business continuity by mitigating legal, financial, and operational risks associated with AML/CTF breaches.

This Policy applies to all employees, departments, third-party partners, and contractors involved in the operation of the Casino. It covers the full range of products and services offered and is integrated into every phase of the customer lifecycle—from onboarding to transaction monitoring and exit.

By clearly outlining legal obligations and internal procedures, this Policy ensures that the Casino remains vigilant, compliant, and aligned with both national and international expectations in the fight against financial crime, applying a risk-based approach to customer due diligence, transaction monitoring, and reporting of unusual activity.

This Policy is integral to the Casino's overall risk management strategy and contributes to the global effort to combat financial crime.

3. Audience

This Anti-Money Laundering and Counter-Terrorism Financing (AML/CTF) Policy applies to all individuals and entities involved in the operation and delivery of services by the Casino. The following persons are required to adhere to the Policy and its related procedures:

3.1. All Employees

- Frontline staff (e.g. customer support, finance, and operations) who may interact directly with customers or handle transactions;

- Compliance personnel responsible for risk assessments, due diligence, and reporting;
- Management and executives overseeing strategic decisions and regulatory compliance;
- IT and security teams who support transaction monitoring, data protection, and system controls.

3.2. Subcontractors and Consultants

- Individuals or firms engaged to perform services on behalf of the Casino, particularly those involved in compliance support, identity verification, payments processing, or AML audits.

3.3. Third-Party Service Providers

- Vendors and partners delivering KYC/EDD solutions, payment gateway services, AML screening tools, or transaction monitoring systems;
- Any outsourced function that involves access to customer data or transaction records.

3.4. Business Partners and Affiliates

- Agents, marketing affiliates, and other business intermediaries who refer or onboard customers on behalf of the Casino;

All persons listed above are required to:

- Understand and comply with the provisions of this Policy
- Participate in AML training where appropriate
- Report any unusual activity or breaches in accordance with the procedures outlined herein

Failure to comply with this Policy may result in disciplinary actions, contract termination, or legal consequences, as detailed in the “Compliance and Consequences of Non-Compliance” section.

4. Definitions

Key definitions include:

Casino means Progress Path Co N.V. (company number 164185, registered address Emancipatie Boulevard, Dominico F. "Don" Martina 31, Willemstad, Curaçao) which is a holder of an Orange Digital Seal “Certificate of Operations” (application OGL/2024/1113/0517).

CFATF means the Caribbean Financial Action Taskforce. An organization of twenty-four (24) states of the Caribbean Basin, Central and South America, which have agreed to implement common countermeasures to address money laundering.

Compliance Officer means a senior officer at management level and independent from the games’ operations, responsible for the detection and deterrence of money laundering and terrorist financing.

Customer Due Diligence or CDD means the process of identifying and verifying customers and assessing their risk.

FATF means the Financial Action Task Force. An independent intergovernmental body, established in 1989 and mandated by its Member Jurisdictions to develop and promote policies to protect the global financial system against money laundering, terrorist financing and the financing of proliferation of weapons of mass destruction.

FATF Recommendations means a framework of recommendations on policies and measures, issued by the FATF, to combat money laundering, terrorist financing and the financing of proliferation of weapons of mass destruction;

Financial Transactions means deposits and withdrawals (bonusses are not included). Amounts wagered and winnings are considered as gambling transactions. Gambling transactions are not considered as financial transactions.

FIU means the Financial Intelligence Unit Curaçao, referred to in art. 2 of the NORUT.

Kingdom Sanctions Act means the National Ordinance also known as the “Rijkssanctiewet”, published under N.G. 2016 no. 54.

NOIS means National Ordinance on Identification of Clients when rendering Services (Landsverordening identificatie bij dienstverlening, N.G. 2017, no. 92).

NORUT means National Ordinance on the Reporting of Unusual Transactions (Landsverordening Melding Ongebruikelijke Transacties, N.G. 2017, no. 99).

Money Laundering or **ML** means the process of disguising the illicit origin of funds.

Politically Exposed Persons or **PEPs** means individuals who are or have been entrusted with prominent public functions by a foreign country and the direct family members or close associates of such persons. Examples are: Heads of State or of government, senior politicians, senior government, judicial or military officials, senior executives of state owned corporations, important political party officials.

Sanctions National Ordinance means the National Ordinance also known as the “Sanctielandsverordening”, published under N.G. 2014 no. 55.

Source of Funds refers to how the funds for a particular transaction were obtained by the player, like personal savings, pension release, property sales, share sales and dividends, gambling winnings, gifts, compensation from legal rulings.

Source of Wealth means the origin of all the money a person has accumulated over their lifetime, like employment income, inheritances, investments, business ownership interests.

Terrorist Financing or **TF** means providing funds for terrorist activity or organizations.

Unusual transaction means a transaction that is considered as such on the basis of certain indicators, pursuant to Article 10 of the NORUT.

Ultimate beneficial ownership or **UBO** means the natural person who ultimately owns or controls a customer and/or the person on whose behalf a transaction is being conducted. It also incorporates those persons who exercise ultimate effective control over a legal person.

5. Policy Implementation

Policy implementation involves a risk-based approach to detect and mitigate ML/TF/FP risks. It includes Business Risk Assessment, Customer Risk Assessment, Customer Acceptance Policies, Due Diligence procedures, Ongoing Monitoring, and Reporting mechanisms. Detailed processes and responsible departments are outlined in the sub-sections below.

Approving Official(s):

Senior Management / Board of Directors

Responsible Office:

Compliance Department

Effective Date:

April 10, 2025

Next Review Date:

April 10, 2026

5.1 Business Risk Assessment

5.1.1. Introduction.

This Business Risk Assessment (BRA) section outlines the Casino's approach to identifying and managing the money laundering (ML), terrorist financing (TF), and proliferation financing (PF) risks to which it is exposed. The purpose of the BRA is to ensure that the Casino's policies, procedures, and internal controls are robust, risk-based, and proportionate to the level of exposure faced by the business.

This BRA is conducted in compliance with the AML/CFT (Anti-Money Laundering and Countering the Financing of Terrorism) regulatory framework of Curacao, and takes into account international standards such as those set out by the Financial Action Task Force (FATF).

This Business Risk Assessment ensures that the Casino maintains a proactive, structured, and proportionate approach to managing ML/TF risks. By aligning with Curacao's regulatory expectations and international AML standards, the Casino strengthens its defenses against financial crime and protects the integrity of its operations

5.1.2. Purpose of the Business Risk Assessment

The objective of the BRA is to:

- Identify, assess, and understand the risks of ML/TF and PF specific to the Casino.
- Develop and implement appropriate AML/CFT policies, procedures, and internal controls.
- Ensure that resources are allocated efficiently to areas of higher risk.
- Demonstrate a proactive and risk-based approach to compliance, as required by Curacao's legislation and licensing conditions.

5.1.3. Risk Categories Assessed

The Casino evaluates ML/TF risks across the following primary categories:

a) Product/Service Risk

Some Casino's products and services could be exploited for illicit purposes, e.g.:

- Online gaming platforms: May be used to deposit illicit funds, gamble to create a “layering” effect, and withdraw funds as “winnings.”
- High-value transactions: Customers may attempt to deposit or withdraw unusually large sums of money without a clear gaming rationale.
- Bonus abuse: Exploiting sign-up or loyalty bonuses to mask the origin of funds.

b) Delivery Channel Risk

- Remote access: Online platforms allow customers to remain anonymous or use false documentation, increasing the risk of fraudulent identities.
- Third-party payments: Customers using bank accounts, cards, or e-wallets not registered in their name.
- Cryptocurrency (if accepted): High-risk due to anonymity, speed of transfer, and lack of central oversight.

c) Geographic Risk

Customers from jurisdictions identified as high-risk by FATF or under international sanctions pose elevated exposure.

The Casino assesses countries based on:

- AML/CFT effectiveness of local laws.
- Known prevalence of corruption or criminal networks.
- Political instability or links to terrorism.

The Casino undertakes to have a list of countries that are considered as high risk and of those that are considered low risk.

While geographic risk assessment the variety of sources of information is considered, including:

- Countries on the FATF list of High - Risk Jurisdictions subject to a Call for Action;
- Countries on the FATF list of Jurisdictions under Increased Monitoring;
- Countries on the CFATF Public Statement;
- Countries identified as Jurisdictions of Concern or Primary Concern in the U.S. Department of State’s annual International Narcotics Control Strategy Report (INCSR);
- Countries on the European Commission’s list of third countries having strategic deficiencies in their AML/CFT regime;
- Countries sanctioned by the OFAC;
- Countries identified by credible sources as providing funding or support for terrorist activities or having terrorist organizations operating within them;
- Countries on the Corruption Perception Index compiled by Transparency International.

d) Customer Risk

- Politically Exposed Persons (PEPs): Due to their access to public funds, PEPs are considered high-risk.
- Unverified customers or incomplete CDD: Customers who provide insufficient or suspicious information during onboarding.
- High-roller or VIP clients: These clients may transact in large volumes with limited scrutiny if proper procedures are not in place.

e) Transaction Risk

Unusual transaction patterns, such as:

- Deposits and withdrawals with minimal or no gaming activity.
- Structured transactions below reporting thresholds.
- Use of multiple accounts or identities.

5.1.4. Risk Assessment Methodology

The Casino uses a structured methodology to assess and rate each risk factor:

- **Inherent Risk:** The level of risk present before the application of controls.
- **Control Effectiveness:** How well current policies, procedures, and systems reduce or mitigate the identified risk.
- **Residual Risk:** The remaining level of risk after controls are applied.

Each risk is assigned a score (e.g., Low / Medium / High) and ranked accordingly. This ensures prioritization of mitigation strategies for higher-risk areas.

5.1.5. Mitigation Measures and Controls

To address the risks identified through the BRA, the Casino implements the following controls:

- **Customer Due Diligence (CDD):** Including Enhanced Due Diligence (EDD) for high-risk customers.
- **Transaction Monitoring:** Real-time and retrospective monitoring of transactions for unusual or suspicious patterns.
- **Sanctions and PEP Screening:** Automated systems to screen customers and transactions against updated international lists.
- **Ongoing Staff Training:** Regular AML training for all staff to recognize unusual behavior and escalate appropriately.
- **Record Keeping:** Maintenance of all relevant documentation for at least **five** years.
- **Unusual Activity Reporting (UAR):** Established procedures for filing UARs with the appropriate regulatory body.

5.1.6. Ongoing Review and Update of the BRA

The Business Risk Assessment is a living document and will be:

- Reviewed and updated at least **annually**.
- Immediately reassessed in the event of:
 - Introduction of new products, services, or delivery channels.
 - Significant changes in customer base or transaction volumes.
 - Regulatory updates from local or international bodies.

The review process is overseen by the Casino's Compliance Officer and senior management, who are responsible for ensuring that the BRA remains relevant and effective.

5.1.7. Documentation and Availability

A full record of the Business Risk Assessment, including supporting data and rationale for risk scores, is maintained and made available to:

- Curacao regulatory authorities upon request.
- Internal audit and compliance reviews.
- Senior management for strategic and compliance decision-making.

5.2 Customer Risk Assessment

In accordance with the laws and regulations of Curacao, a comprehensive Customer Risk Assessment (CRA) is a critical component of the Anti-Money Laundering (AML) Policy for casinos. The CRA will be conducted at the time of establishing a business relationship with a player or before any gaming or financial transaction is provided. The purpose of this assessment is to identify and evaluate the risks associated with each customer, including potential exposure to money laundering and terrorist financing.

5.2.1. Customer Risk Assessment (CRA) Process

Under Curacao's AML regulations, the Casino is required to perform a Customer Risk Assessment **during the onboarding process**. This involves collecting a variety of information to determine the risk profile of the customer. Key elements include:

- **Identity Verification:** Basic personal details (e.g., full name, date of birth, nationality or permanent residential address) must be collected and verified to ensure the customer is who they claim to be.
- **Geographic Risk:** Players from high-risk jurisdictions (countries with high levels of corruption, inadequate AML regulations, or ongoing conflicts) will be considered as higher risk. Additional scrutiny should be applied to these customers.
- **PEP identification:** an individual who holds or has held a prominent public function, as well as their immediate family members and close associates will be monitored by using the screening tools and databases.
- **Sanctions Screening:** the customers will be screened against the lists to identify any individuals or entities that are subject to sanctions.
- **Source of Funds:** in cases the customers are PEPs the Casino undertakes to assess the funds origin. This may involve asking for documentation such as bank statements, proof of income, or business ownership.

5.2.2. Risk Profiling and Categorization

The information collected will be used to create a risk profile for each customer. Based on the data, while onboarding, the customers can be classified into one of the following categories:

- **Low Risk:** customers from low-risk jurisdictions, not preliminary identified as PEP or sanctioned persons.
- **Medium Risk:** customers from jurisdictions with a moderate risk of money laundering or terrorist financing, not preliminary identified as PEP or sanctioned persons
- **High Risk:** customers from high-risk countries and customers preliminary identified as PEP or sanctioned persons.

5.2.3. Transaction Monitoring and Unusual Activity Reporting

Casino undertakes to implement transaction monitoring systems to identify and flag any unusual or suspicious activities. These systems should be capable of detecting:

- **Large or Unusual Transactions:** Transactions that are inconsistent with the customer's profile, such as sudden large deposits or withdrawals that cannot be explained by the customer's source of income.
- **Frequent or Unexplained Gaming Patterns:** If a customer is making irregular bets, wagering large sums with no apparent source of funds, or withdrawing winnings without clear justification.
- **Multiple Accounts:** The use of multiple accounts by a single individual or attempts to conceal their identity could signal potential money laundering.

Whenever unusual activity is detected, the Casino is obliged to file Unusual Activity Reports (UAR) with the relevant authorities in Curacao.

This reporting is essential for compliance with local regulations and international anti-money laundering standards.

5.2.4. Customer Risk Re-assessment

The risk profile of each customer should not remain static. The Casino undertakes to regularly reassess the risk level of its customers, especially if there are changes in their behavior, transactions, or the geopolitical environment that could affect the customer's risk status. The risk assessment should be updated whenever there is:

- A change in the customer's personal or financial circumstances.
- The emergence of new information that may indicate higher risk.
- A significant change in the regulatory environment of the customer's home country.

While Risk Re-assessment, the customers can be classified into one of the following categories:

- **Low Risk:** customers with a clear and traceable source of funds, from low-risk jurisdictions, and with a consistent gaming history not identified as PEP or sanctioned persons.
- **Medium Risk:** customers who show some signs of irregularities in their behavior or come from jurisdictions with a moderate risk of money laundering or terrorist financing, not identified as PEP or sanctioned persons
- **High Risk:** customers identified as PEP or sanctioned persons and customers whose behavior or background presents a higher likelihood of being involved in money laundering or other illicit activities. This could include players from high-risk countries, those with unusual or suspicious transaction patterns, or those who provide insufficient information regarding their source of funds.

5.2.5. Record Keeping and Documentation

The Casino undertakes to maintain thorough records of all customer risk assessments, including:

- **Personal Information:** All data used to assess the customer's identity and financial status.
- **Risk Assessment Documentation:** Records of the risk profile assigned to each customer, including the rationale for the classification.
- **Monitoring Logs:** Documentation of any ongoing monitoring of the customer's activity, including flagged transactions and follow-up actions.

These records should be kept for a minimum of **five years** to comply with Curacao's AML laws and regulations, and they must be readily available for review by regulatory authorities.

5.3 Customer Acceptance Policy

5.3.1. Introduction

The Customer Acceptance Policy (CAP) outlines the procedures and criteria for accepting customers into the Casino, ensuring that the Casino complies with Curacao's Anti-Money Laundering (AML) regulations and international standards. This Policy is designed to protect the Casino from being used for illegal activities, including money laundering and the financing of terrorism, by ensuring that each customer undergoes a thorough risk assessment and is subject to appropriate Customer Due Diligence (CDD) measures.

The CAP is developed based on the results of the Customer Risk Assessment (CRA) and provides clear guidance on how to apply the appropriate level of CDD, taking into account the customer's risk profile, their potential to be involved in money laundering or terrorist financing, and other relevant risk factors. It also addresses the necessary protocols for handling Politically Exposed Persons (PEPs) and Sanctions Screening.

The Customer Acceptance Policy ensures that the Casino conducts thorough due diligence on each customer to minimize exposure to financial crimes, such as money laundering and terrorist financing. By adhering to the principles of this Policy, the Casino will ensure compliance with the AML regulations set forth by Curacao, as well as international best practices regarding Politically Exposed Persons and Sanctions Screening.

5.3.2. Customer Acceptance Criteria

The Casino will only accept customers who pass the Customer Risk Assessment (CRA) process. Customers must meet the following criteria before a business relationship is established:

- **Identity Verification:** All customers must undergo a thorough identity verification process, where the casino will collect and verify essential personal details, such as the customer's full name, date of birth, permanent residential address. For residents without a permanent address, additional identification may be required.
- **Geographic Risk Assessment:** The Casino will assess the country of origin of each customer. Customers from high-risk jurisdictions or countries with weak anti-money laundering regulations will be subject to more stringent checks.
- **Source of Funds Verification:** in case the customer was identified as a Politically Exposed Person the customer must disclose and provide sufficient evidence regarding the source of their funds. This includes documentation that proves the legitimate origin of their financial resources, such as bank statements, salary slips, or business ownership details.

5.3.3. Politically Exposed Persons (PEPs)

The Casino undertakes special care to identify PEPs at the time of customer onboarding.

Customers identified as PEPs will undergo Enhanced Due Diligence (EDD). This involves:

- Verifying the source of their wealth and funds through more in-depth documentation.
- Scrutinizing their transaction patterns to identify any suspicious or irregular activities.
- Assessing their family members and close associates, as they may also be subject to higher risks.
- Obtaining approval from senior management before proceeding with establishing a business relationship.

PEPs will be subject to ongoing monitoring and re-assessment. Any changes in their status or circumstances should be flagged for review and potential adjustment of their risk profile.

5.3.4. Sanctions Screening

Sanctions List Screening: The Casino will conduct regular screenings of all customers against national and international sanctions lists, including the United Nations Security Council Sanctions List, the European Union Sanctions List, and the United States Department of Treasury's Office of Foreign Assets Control (OFAC) list, among others.

Screening Process: During the customer onboarding process, and periodically throughout the relationship, customers will be screened against these lists to identify any individuals or entities that are subject to sanctions. Customers found to be on any sanctions list will be immediately prohibited from engaging in any gaming or financial transactions with the Casino.

Immediate Action for Sanctions Hits: If a customer matches any sanctioned individual or entity, the Casino will immediately freeze their account and report the match to the relevant authorities, as required by Curacao's AML regulations.

5.3.5. Risk-Based Approach

The CAP adheres to a risk-based approach, where the level of due diligence applied to a customer is proportional to the identified risk level. Factors influencing the level of CDD include:

- The customer's risk profile (low, medium, or high risk).
- The customer's jurisdiction of origin and whether it is considered high-risk.
- The nature and volume of the customer's transactions.
- The customer's history with the casino and any prior unusual or suspicious activity.

5.3.6. Ongoing Monitoring and Review

The Casino will implement continuous monitoring to ensure that the business relationship remains in compliance with AML regulations throughout the customer's engagement. This includes:

- Regular reviews of customer transactions to detect any unusual or suspicious activity.
- Periodic re-assessment of customer risk profiles based on changes in their behavior or the geopolitical environment.
- Continuous monitoring of PEP status and sanctions lists to identify potential changes.

5.3.7. Record Keeping

The Casino will maintain detailed records of all customer risk assessments, identity verification documents, and any due diligence conducted. These records will be stored securely and retained for a minimum of **five years**, as required by Curacao's AML regulations, and will be made available for inspection by regulatory authorities upon request.

5.4 Customer Due Diligence

5.4.1. Introduction

Casinos are prohibited from keeping anonymous accounts or accounts in obviously fictitious names. The Casino must identify the player and ask for the player's name and other relevant information to determine the purpose and nature of the business relationship. Customer Due Diligence (CDD) is a core element of the Casino's Anti-Money Laundering and Counter-Terrorism Financing (AML/CTF) framework. The purpose of CDD is to verify the identity of customers, assess and monitor their risk level, and ensure that the Casino does not facilitate money laundering, terrorist financing, or other illicit activities. This Policy outlines the measures used to perform CDD, including the

treatment of Politically Exposed Persons (PEPs), sanctions screening, and the procedure for freezing funds and reporting to the relevant authorities in Curacao.

5.4.2. When CDD is applied

CDD is carried out in the following situations:

- a. players engage in financial transactions equal to or above Cg. 4,000*;
- b. carrying out occasional transactions above the monetary equivalent of Cg. 4,000;
- c. there is a suspicion of money laundering or terrorist financing; or
- d. the Casino has doubts about the veracity or adequacy of previously obtained customer identification data.

* The Casino is also obliged to carry on CDD procedures when a series of linked transactions executed which, though individually below the applicable threshold, would cumulatively meet or exceed the Cg. 4,000 threshold. Transactions are considered as linked if, for example, they are carried out by the same player through the same game or in one gaming session

The threshold is to be calculated on a daily basis taking into account all deposits and withdrawals made by the player since the establishment of the business relationship, including any peer-to-peer transfers. Once the threshold is reached, the Casino must carry out a customer risk assessment and meet their remaining CDD obligations.

In carrying out the CDD measures, customers may be allowed to continue using their gaming account while the Casino obtains any necessary information from the customer concerned.

If the Cg. 4,000 threshold is reached because of a deposit of the player, he cannot further deposit funds into the account or withdraw funds from the account. He still will be able to play, using the funds already in his account. However, if the Cg. 4,000 threshold is reached because the customer wants to withdraw his money, a complete freezing of the account should occur. In this case it will not be possible for the customer to continue playing. Besides that, if the requested information and documentation is not received within 30 days from the moment the Cg. 4,000 threshold was reached, the Casino has to terminate the relationship with the player and report the transaction to the FIU if a presumption of money laundering or terrorist financing exists. If no presumption of money laundering exists, the funds should be transferred to the same bank account or wallet it was deposited from. If presumption of money laundering or terrorist financing exists, internal procedures should indicate whether the funds are blocked or not. Consideration should be given to the fact that by blocking the account, the customer may be tipped off.

5.4.3. CDD Measures

The following measures are applied during the Customer Due Diligence process:

a. Identity Verification

Collection and verification of:

- Full name
- Date of birth
- Place of birth
- Nationality
- Permanent residential address
- Identity number

Verification of identity must be carried out by referring to an unexpired government-issued document containing photographic evidence of the customer's identity (e.g. passport, identity card). Where such a document does not allow verification of the player's residential address, the Casino can obtain other documents like a bank statement, utility bill, letter from a public authority or rental agreement, which should not be more than six months old, to verify the residential address. The Casino can also contact the player by letter, e-mail or telephone to verify the information supplied. It can also send a verification code to the e-mail address to verify that the address is current and genuine. Verification can also be done by checking social media, telephone directories, companies' registries or media and news sources. Biometric checks can also be used to confirm that the individual providing the document is the one described therein.

Verification is carried out by the Casino to determine to its own satisfaction that the player is who he declared himself to be. The documents should be clear, legible and of good quality. When the Casino does not have sufficient comfort that it knows its player, the Casino may take additional measures to do so. Some of these measures include requesting additional identification documents, asking the player to provide a photo of himself holding the ID, requiring a first payment through an account held in a reputable jurisdiction, using systems which generate codes for transmission to customers through a verified mobile phone and requiring it to be returned.

Verification of identity must be conducted when engaging in financial transactions equal to or in excess of **Cg. 4,000**. This implies that all CDD measures must have been conducted at the time the threshold is reached.

The Casino undertakes to apply a minimum level of CDD measures prior to reaching the threshold. **Simultaneously with the opening of an account**, the Casino undertakes to identify the customer by collecting the minimum personal details:

- Full name
- Date of birth
- Permanent residential address

b. Source of Funds and Wealth

CDD measure requires the development of a customer risk profile to have sufficient information available to allow the detection of unusual activity in the course of a business relationship. To this end, the Casino undertakes to collect sufficient information and, where it is necessary, documentation to establish a customer's source of wealth and expected level of activity.

Customers must provide information and supporting documentation to confirm the legitimacy of their funds. Additional scrutiny is applied to high-value transactions or high-risk jurisdictions.

c. Risk Profiling

- Customers are classified into risk categories (Low, Medium, High) based on information collected during onboarding.
- Risk profiles determine the level of ongoing monitoring and due diligence required.

5.4.4. Customer Due Diligence (CDD) Levels

Based on the outcome of the CRA, the Casino will apply different levels of Customer Due Diligence (CDD) measures:

- **Simplified Due Diligence (SDD):** This applies to customers who are classified as low risk. The verification of identity will be sufficient, with no need for enhanced measures unless unusual activity is detected.

- **Enhanced Due Diligence (EDD):** This applies to customers who are classified as medium or high risk. Additional documentation and information will be required to verify the source of funds. Enhanced monitoring and more frequent re-assessments of the customer's activities will be conducted. Customers falling into the high-risk category will be subject to closer scrutiny, including monitoring all transactions for unusual activity.

5.4.5. Politically Exposed Persons

In relation to politically exposed persons (PEPs), in addition to performing normal customer due diligence measures, the Casino is required to:

- a. have appropriate risk-management systems in place to determine whether the customer or the beneficial owner is a politically exposed person;

- b. obtain senior management approval to service the PEP (for establishing the business relationship for new customers, continuing the business relationship for existing customers or for conducting the occasional transaction). The approval can also be obtained from the manager of the Compliance department;

- c. take reasonable measures to establish the source of wealth and the source of funds. The investigation must then determine whether the player's spending pattern matches his legal source of funds. The Casino requests a statement from the player about the source of funds and verifies that by consulting independent and reliable sources. Depending on the risk in specific cases, these can in the first place be public sources. When public sources cannot, or can insufficiently verify the received information, the Casino can request the customer to provide additional documents;

- d. conduct enhanced ongoing monitoring of the business relationship.

The Casino is required to take reasonable measures to determine whether a customer is a domestic PEP or a person who is or has been entrusted with a prominent function by an international organization. In cases of a higher risk business relationship with such persons, the Casinos is required to apply the measures referred to in items b, c and d.

Identification of PEPs may be conducted by screening tools and databases that are used to identify PEPs during onboarding and on an ongoing basis, (e.g. Transparency International Corruption Perceptions Index, or on www.knowyourcountry.com.)

The PEP customers' due diligence does not have to be the same for every PEP. The measures are tailored to the risk of the PEP, with the following being taken into consideration:

- the type of public function of the PEP;
- the country from which the PEP originates;
- the transactions that the PEP carries out.

The measures taken can be tailored to the risks identified in a specific case.

The requirements for all types of PEPs should also apply to family members or close associates of such PEPs.

Screening for PEP status has to be carried out at **onboarding**. In addition, the Casino undertakes to regularly screen for PEP status during the business relationship. Should a player who had not been identified as a PEP at onboarding stage become one, the Casino is required to implement the measures described above within the thirty-day window

of observing that the person is a PEP. Failing with these, shall result in the Casino terminating the relationship with this customer.

5.4.6. Sanctions Screening

All customers are screened against relevant sanctions lists, including:

- United Nations Security Council Sanctions List (UN Sanctions List <https://main.un.org/securitycouncil/en/content/un-sc-consolidated-list>)
- European Union Consolidated List (EU Sanctions List <http://www.sanctionsmap.eu/#/main>)
- OFAC (Office of Foreign Assets Control) Sanctions List
- UK Sanctions Lists
- All other applicable national and international sanctions and restrictive lists, the complete list of which is maintained and detailed in Appendix 1 to this Policy.

Screening occurs:

- During onboarding
- On a daily basis thereafter, using updated lists

5.4.7. Freezing of Funds and Reporting to Authorities

When a customer is identified as a match to a sanctioned person/entity, or if there is suspicion of money laundering, terrorist financing, or other criminal activity:

a. Freezing of Funds

The Casino will promptly freeze any funds held in the customer's account.

No further transactions will be permitted without authorization from competent authorities.

Internal records of the freezing action are created and retained.

b. Reporting Procedure

An Unusual Transaction Report (UTR) is filed with the FIU Curacao .

The report includes:

- Customer identity and details
- Nature and circumstances of the unusual activity
- Date, time, and amount of the transaction
- Actions taken by the Casino (e.g., freezing, suspension)

All reports and communications with FIU are treated as confidential and in accordance with applicable legal obligations.

5.4.8. Simplified Due Diligence for the Low-Risk Customers

Where the risks of money laundering or terrorist financing are low, the Casino is allowed to conduct simplified CDD measures, which should take the nature of the lower risk into account.

Such measures may include:

- Not collecting specific information. If the risk assessment undertaken indicates a low risk of money laundering or terrorist financing then it is only necessary for the Casino to obtain the player's identity. In this case the Casino may limit identification to: full name; permanent residential address; date of birth;
- Verifying the identity of the customer and the beneficial owner after the establishment of the business relationship;
- Adapting verification to perceived risk. The extent of verification may also vary depending on the risk posed by the particular business relationship. In a low risk situation, the Casino can also use alternative reputable information sources, even where these do not contain photographic evidence of the player's identity (e.g. birth certificates, bank statements etc.);
- Limiting the extent of personal details to be verified. In low risk situations, the Casino has to verify the basic identification details, while the verification of any other personal details is to the discretion of the Casino, as long as it has sufficient comfort that it knows who its customer is;
- Reducing the frequency of customer identification updates;
- Reducing the degree of on-going monitoring and scrutinizing transactions, based on a reasonable monetary threshold.

Simplified CDD measures are not acceptable whenever there is suspicion of money laundering or terrorist financing, or where specific higher-risk scenarios apply.

5.4.9. Enhanced Due Diligence (EDD) for High-Risk Customers

For customers classified as high risk, enhanced due diligence (EDD) measures must be taken. These measures include but are not limited to:

- Detailed Verification: Additional verification of identity and verification of source of funds is required, including documents that trace the origin of funds in details (e.g., tax returns, wealth statements, or proof of business ownership).
- Ongoing Monitoring: High-risk customers should be subjected to continuous monitoring throughout the business relationship. The Casino is required to scrutinize their transactions for signs of unusual or suspicious activity.
- Frequent Re-assessment: High-risk customers should be reassessed on a more frequent basis, ensuring that any changes in their behavior or financial situation are identified early.

Upon the Casino's discretion, depending on the results of the Detailed Verification the High-Risk customers may be declined in the Casino's services provision.

The customers found to be on any sanctions list will be immediately prohibited from engaging in any gaming or financial transactions with the Casino.

5.4.10. Termination of the business relationship

In case the obligations arising from the customer due diligence cannot be met, the Casino cannot establish the business relation or perform the transaction and is obliged to terminate the business relationship with the customer. The Casino undertakes to keep a record of all the attempts made to get the necessary information and documentation. To this end, the Casino may decide to either close the account or to keep it blocked and suspended in its entirety.

In the event the customer makes the requested information and/or documentation available to the Casino following the closure or the suspension and blocking of the gaming account, the Casino has to consider whether the delay in providing the requested CDD documentation and/or information affects the risk of ML/FT associated with the given business relationship.

The Casino is to consider whether there are any grounds giving rise to suspicion of ML/TF/FP. The reluctance of the customer to provide CDD on its own should not be automatically equated to a suspicion of ML/TF/FP. The Casino should consider all factors and information it has at his disposal to decide whether there are grounds to suspect ML/FT/FP. If, however the presumption of ML/FT/FP exists the Casino should submit an unusual transaction report to the FIU with regard to this player.

Where there is no reason for the retention of funds, the funds are to be remitted back to the player. This has to be done through the same channels used to receive the funds.

5.4.11. Record Keeping

The Casino retains all CDD records, including identity documents, risk assessments, and transaction logs, for at least **five years** after the end of the business relationship or the date of the last transaction.

Records are stored securely and are readily accessible for review by the Curacao Gaming Control Board and other regulatory authorities.

5.5 Ongoing Monitoring

5.5.1. Introduction

Ongoing monitoring is a critical element of the Casino's AML/CTF framework. It ensures that customer activity remains consistent with the information obtained during onboarding and throughout the business relationship. The objective is to detect and respond to unusual or suspicious behavior that may indicate involvement in money laundering, terrorist financing, or other criminal activity.

This Policy outlines the procedures and tools used by the Casino to continuously monitor customer identities, assess risk, and track transactions in compliance with the AML/CTF laws of Curacao and international standards (including FATF Recommendations).

5.5.2. Scope of Ongoing Monitoring

The Casino conducts ongoing monitoring in the following areas:

- Customer Identity Monitoring: Ensuring that customer identity data remains accurate, complete, and up to date.
- Transactional Monitoring: Assessing the customer's financial behavior for consistency with their risk profile.
- Risk Reassessment: Re-evaluating customer risk levels when triggers are identified.
- PEP and Sanctions Rescreening: Daily screening against updated PEP and sanctions lists.

5.5.3. Identity Monitoring

The Casino performs periodic reviews of customer data to ensure that information provided at onboarding remains valid. The Customers may be asked to provide updated documentation if:

- Their identification documents expire.
- They change their personal details (e.g. address or payment method).
- There are indicators of increased risk (e.g. unusual behavior or transaction patterns).

Risk-based reviews are scheduled more frequently for high-risk customers, including PEPs and those from high-risk jurisdictions.

5.5.4. Transaction Monitoring

All customer transactions are continuously monitored for:

Unusual patterns, such as:

- High-value deposits or withdrawals without gaming activity.
- Structuring transactions just below reporting thresholds
- Rapid deposit and withdrawal cycles.
- Use of multiple accounts or aliases.

Red flags, including:

- Transactions inconsistent with the customer's known profile.
- Use of third-party payment instruments.
- Transactions involving high-risk jurisdictions or cryptocurrencies (if accepted).

Transaction monitoring is performed via a combination of automated systems and manual reviews conducted by the compliance team. After receiving this information the Casino has to decide whether the transaction is an unusual transaction and need to be reported to the FIU.

5.5.5. Risk-Based Monitoring Frequency

- Low-risk customers: Subject to standard periodic monitoring.
- Medium-risk customers: Monitored more frequently with additional review triggers.
- High-risk customers and PEPs: Subject to enhanced monitoring, including manual transaction reviews and periodic reassessment of risk profile.

The frequency and depth of monitoring are directly proportional to the assessed level of risk.

5.5.6. Ongoing PEP and Sanctions Screening

The Casino screens all active customers daily against updated Politically Exposed Persons (PEP) lists and international sanctions lists (e.g., UN, EU, OFAC).

Automated tools flag any matches, triggering immediate account suspension and compliance review.

If a match with international sanctions lists is confirmed:

- Funds are frozen in accordance with legal obligations.
- A report is filed with the FIU Curacao.

5.5.7. Trigger-Based Reviews

Customer risk profiles and activity are reassessed upon certain triggers, such as:

- Unusual or suspicious transactions
- Significant increase in gaming volume
- Negative media reports or law enforcement alerts
- Customer becoming a PEP or being added to a sanctions list

5.5.8. Unusual Activity Detection and Reporting

If ongoing monitoring reveals unusual activity:

- The case is escalated to the Compliance Officer.
- An Unusual Transaction Report (UTR) is submitted to the FIU Curacao without tipping off the customer.
- Transactions may be blocked, and accounts suspended pending further investigation.

5.5.9. Documentation and Record Keeping

All results of monitoring activities, including alerts, internal investigations, and reports to the FIU, are documented. These records are retained for a minimum of **five years** and are available for audit and inspection by the Curacao Gaming Control Board or other competent authorities.

5.6 Reliance on Third Parties

5.6.1. Policy Statement

As part of its AML/CTF compliance framework, the Casino may, under specific conditions, rely on third parties to perform certain elements of Customer Due Diligence (CDD). This includes identity verification, sanctions and PEP screening, and document authentication. Such reliance is conducted strictly in accordance with the AML legislation of Curacao and relevant FATF Recommendations (Recommendation 17).

Reliance on third parties does not absolve the Casino of its legal responsibility to ensure that CDD measures are correctly applied and that the overall AML/CTF obligations are fulfilled.

5.6.2. Conditions for Third-Party Reliance

The Casino may rely on a third party only if all the following conditions are met:

- The third party is subject to equivalent AML/CTF regulations, particularly in jurisdictions that apply FATF-compliant standards.
- A formal agreement or contractual arrangement is in place to define the roles, responsibilities, and obligations of both parties.
- The third party is willing and able to provide copies of CDD records and supporting documents immediately upon request.
- The third party has a proven record of regulatory compliance and possesses adequate systems and controls to manage ML/TF risks.
- The Casino conducts initial and periodic assessments of the third party's competence and reliability.

5.6.3. Types of Third Parties

Examples of acceptable third parties include:

- Regulated financial institutions (e.g., banks, payment processors) subject to AML supervision.
- Licensed verification service providers offering digital identity and document authentication.
- Affiliated companies or platforms operating under the same AML framework or corporate group policies.

Unregulated or unverified service providers are not accepted for reliance.

5.6.4. Scope of Third-Party Reliance

The Casino may delegate the following CDD tasks to third parties:

- Identity verification (e.g., via biometric checks, ID document validation)
- Proof of address checks
- Sanctions and PEP screening
- Ongoing re-screening services
- Authentication of source of funds documents (if supported by technology providers)

However, the Casino retains responsibility for:

- Final risk assessment and risk classification of the customer
- Ongoing transaction monitoring
- Enhanced due diligence (EDD) in high-risk cases
- Reporting obligations (e.g., to FIU Curacao)

5.6.5. Documentation and Audit Trail

- All third-party arrangements are documented in formal Service Level Agreements (SLAs) or contracts.
- Copies of CDD records obtained by third parties are maintained or made accessible by the Casino and retained for a minimum of five years.
- The Casino ensures that a full audit trail is available for regulatory review, including:
 - Identity verification results
 - Timestamped screening logs
 - Communication records with the third party

5.6.6. Risk Management and Oversight

The Compliance Officer is responsible for approving third-party arrangements and ensuring periodic reviews of their performance and compliance status.

Independent due diligence is conducted before entering into any new third-party relationship.

Third-party reliance is not permitted in cases involving:

- High-risk jurisdictions
- Unusual or suspicious activity
- Politically Exposed Persons (PEPs), unless enhanced controls are in place.

5.7 Reporting of Unusual Transactions

5.7.1. Introduction

In accordance with the National Ordinance for the Reporting of Unusual Transactions (NORUT) of Curacao, the Casino has implemented a clear and effective process for identifying, evaluating, and reporting unusual transactions to the Financial Intelligence Unit (FIU) of Curacao.

This process is a core part of the Casino's AML/CTF framework and ensures compliance with both national regulations and international standards, including the FATF Recommendations.

5.7.2. Definition of Unusual Transactions

An unusual transaction is any transaction or attempted transaction that deviates from normal behavior or may indicate potential money laundering, terrorist financing, or other illicit activity. The following transactions or intended transactions are deemed unusual and as such must be reported to the FIU:

- a. A transaction, which is reported to the police or judicial authorities in connection with money laundering or the financing or terrorism;
- b. An intended transaction carried out by or for the benefit of a natural person, legal person, group or entity which is on a list compiled by virtue of the Sanctions National Ordinance (N.G. 2014 no. 55);
- c. A transaction amounting to Cg. 5,000.00 or more, regardless of whether this transaction is carried out in cash, via a check or another payment instrument or electronically or in any other non-physical manner. This includes but is not limited to:
 1. A cashless transaction in the amount of Cg. 5,000.00 or more.
 2. Accepting or releasing a deposit in the amount of Cg. 5,000.00 or more at the request of the customer;
 3. Sale to a customer of chips in the amount of Cg. 5,000.00 or more. "Chips" include but is not limited to tokens and credits.
 4. A cash out in the amount of Cg. 5,000.00 or more;
- d. Transactions where there is cause to presume that they can be related to money laundering or terrorist financing.

Transactions may be classified as unusual based on:

- Objective indicators, as prescribed by the FIU Curacao, above in a. – c.
- Subjective indicators, determined through internal analysis or suspicion, as prescribed by the FIU Curacao, above in d.

Examples of transaction activity and customer behaviors that could indicate the necessity for a UAR/UTR under the subjective indicator include, but is not limited to:

- Transactions just below reporting thresholds
- Rapid movement of large funds without gaming activity
- Use of multiple accounts or third parties
- Behavior inconsistent with the customer's risk profile
- Involvement of high-risk jurisdictions or cryptocurrencies

5.7.3. Detection Process

The Casino uses a combination of automated monitoring systems and manual reviews to detect unusual transactions:

- Automated rules and thresholds flag potentially unusual activity in real-time.

- Alerts are reviewed by trained compliance staff who assess the context and customer profile.
- If a transaction is deemed unusual or suspicious, it is escalated for further internal investigation.

5.7.4. Internal Escalation and Evaluation

Employees are required to report any unusual activity to the Compliance Officer immediately, but no later than 24 hours after the transaction has been executed. The Compliance Officer conducts a structured assessment of the flagged activity.

The evaluation considers:

- Transaction history and volume
- Customer's known profile and source of funds
- Involvement of PEPs or sanctioned entities
- Connections to high-risk jurisdictions
- Any previous UTRs or unusual behavior

If a more in-depth investigation is necessary, the CO will complete this within ten (10) business days. During this time, the CO may request additional information from relevant departments. If the activity meets the reporting criteria, the transaction is documented and prepared for external reporting within 48 hours.

5.7.5. Reporting to the FIU Curacao

Once an unusual transaction is confirmed, the Casino must:

- File an Unusual Transaction Report (UTR) with FIU Curacao without delay and without alerting the customer.
- Submit the report via the FIU's secure online reporting portal (goAML), including:
 - Full details of the customer and transaction(s)
 - Reasons for suspicion and relevant supporting documentation
 - Actions taken by the Casino (e.g., freezing funds, suspending account)

Reports must be submitted within the timelines specified by local regulation. In any cases whereby the report is made under one of the objective indicators, as defined below, the report must be made to the FIU Curaçao no later than 48 hours after the transaction has been executed

5.7.6. Confidentiality and "No Tipping Off" Rule

All staff involved in the reporting process are trained to observe the prohibition on tipping off the customer.

Any disclosure or suggestion to the customer that an investigation or report has been made is strictly prohibited and may result in legal penalties.

5.7.7. Record Keeping

All internal assessments, alerts, communications, and submitted reports are securely documented.

These records are retained for a minimum of **five (5)** years from the date of reporting or the end of the customer relationship.

Records are made available upon request to the Gaming Control Board, FIU Curacao, or any other authorized authority.

5.7.8. Staff Training and Awareness

Employees are trained regularly on:

- Recognizing red flags and indicators of unusual activity
- Reporting procedures and escalation protocols
- Confidentiality and legal obligations under NORUT

Training is mandatory for all relevant personnel and documented as part of compliance oversight.

5.8 Anti-Money Laundering Compliance Program

5.8.1. Purpose and Scope

The purpose of the Anti-Money Laundering (AML) Compliance Program is to establish a comprehensive, risk-based framework that enables the Casino to identify, assess, prevent, and mitigate the risks of money laundering (ML), terrorist financing (TF), and proliferation financing. This program is designed to ensure full compliance with the AML/CTF laws of Curacao, including the National Ordinance for the Prevention and Combating of Money Laundering and Terrorist Financing (NOIS), the National Ordinance Reporting of Unusual Transactions (NORUT), and the guidelines issued by the Financial Intelligence Unit (FIU) Curacao and the Gaming Control Board.

5.8.2. Risk-Based Approach

The AML Compliance Program is built on a risk-based approach, where higher-risk customers, products, services, and geographic areas are subject to enhanced due diligence and monitoring.

A Business Risk Assessment (BRA) and Customer Risk Assessment (CRA) are conducted and regularly updated to assess exposure to ML/TF risks.

Risk factors include customer profile, transaction behavior, payment methods, jurisdiction, and use of intermediaries.

Mitigation measures are proportionate to the level of assessed risk.

5.8.3. Minimum Standards of the AML Program

The Casino's AML program includes the following core elements:

a. Customer Due Diligence (CDD)

- Verification of identity for all customers before establishing a business relationship.
- Collection and evaluation of the source of funds.
- Enhanced due diligence for high-risk customers, including Politically Exposed Persons (PEPs).

b. Ongoing Monitoring

- Real-time and retrospective monitoring of transactions to detect unusual patterns or suspicious behavior.

- Daily re-screening of customers against updated sanctions and PEP lists.

c. Reporting of Unusual Transactions

- Procedures for identifying and evaluating unusual or suspicious transactions.
- Prompt filing of Unusual Transaction Reports (UTRs) to the FIU Curacao.
- Maintenance of strict confidentiality and enforcement of the no “tipping off” rule.

d. Record Keeping

- Retention of all CDD, transaction, and reporting records for at least five years after the end of the customer relationship.
- Secure and accessible storage of all AML-related documentation.

e. Employee Training

- Regular, documented training on AML laws, red flags, reporting procedures, and internal controls.
- Mandatory training for new hires and ongoing refresher courses for existing staff.

f. Independent Audit

- Periodic, independent reviews of the AML program to assess effectiveness and compliance.
- Audit findings are reported to senior management and used to improve the program.

5.8.4. Blocking and Freezing of Accounts

In the event of suspicion of money laundering or terrorist financing, the Casino follows a strict procedure to block or freeze accounts:

a. Identification and Assessment

- When a transaction or customer behavior is flagged as unusual, the case is escalated to the Compliance Officer for investigation.
- If the suspicion is substantiated, immediate action is taken to mitigate risk.

b. Account Blocking

- The Casino suspends or blocks the customer’s account to prevent further transactions.
- Access to funds is restricted until the case is resolved or further instruction is received from the competent authority.

c. Reporting to FIU

- An Unusual Transaction Report (UTR) is promptly filed with the FIU Curacao, including all relevant data and the reason for suspicion.
- Cooperation with authorities is maintained throughout any investigation or inquiry.

d. Documentation

- A full audit trail of the incident, including internal communications, analysis, and decisions taken, is documented and retained in accordance with legal requirements.

5.8.5. Governance and Oversight

A designated Compliance Officer is responsible for the implementation and oversight of the AML program.

Senior management is fully committed to ensuring that AML obligations are met and that resources are allocated appropriately.

AML compliance is integrated into the overall risk management and corporate governance framework.

6. Compliance and Consequences of Non-Compliance

6.1. Commitment to Compliance

The Casino is fully committed to adhering to all applicable laws and regulations related to Anti-Money Laundering (AML), Counter-Terrorism Financing (CTF), and sanctions enforcement as established by the jurisdiction of Curacao and aligned with international best practices, including the FATF Recommendations.

Compliance with the AML/CTF Policy is mandatory for all employees, officers, agents, and third-party service providers. Failure to comply with the established policies and procedures may expose the organization—and individuals involved—to significant legal, regulatory, and reputational risks.

6.2. Risks of Non-Compliance

Non-compliance with this Policy may result in:

a. Legal and Regulatory Sanctions

- Fines or penalties imposed by Curacao's authorities, including the Gaming Control Board or FIU Curacao.
- Revocation or suspension of the Casino's gaming license.
- Criminal prosecution of individuals involved in willful violations or negligence, leading to fines or imprisonment under Curacao law.
- International enforcement actions and cross-border cooperation from foreign regulators.

b. Reputational Damage

- Loss of customer trust and public credibility.
- Negative media exposure and damaged relationships with banks, payment providers, and other partners.
- Being listed as a non-cooperative entity by financial institutions or regulators.

c. Operational Disruption

- Freezing of funds or closure of accounts due to investigations.
- Loss of access to financial systems and payment processing networks.
- Increased scrutiny from regulators, auditors, and law enforcement agencies.

6.3. Internal Disciplinary Consequences

Employees who violate the AML/CTF Policy—whether through willful misconduct, negligence, or failure to report unusual activity—will be subject to disciplinary actions, which may include:

- Formal warning or reprimand.

- Suspension without pay.
- Termination of employment for serious or repeated breaches.
- Referral to law enforcement where appropriate.

Third-party providers or contractors may have their agreements terminated immediately if they are found to be non-compliant or unwilling to follow the Casino's AML procedures.

6.4. Responsibilities of Employees

All employees must:

- Understand and comply with the AML/CTF Policy and related procedures.
- Participate in mandatory AML training sessions.
- Immediately report any unusual behavior, transactions, or breaches of Policy to the Compliance Officer.

Employees are protected from retaliation for making good faith reports of suspected violations ("whistleblower" protections).

6.5. Enforcement and Oversight

The Compliance Officer and senior management are responsible for:

- Investigating violations.
- Determining appropriate disciplinary or remedial actions.
- Reporting serious breaches to the relevant regulatory and legal authorities.

All enforcement actions are documented, reviewed periodically, and used to improve the compliance program.

7. Related Information

The following laws, regulations, guidelines, and internal policies form the legal and operational foundation of the Casino's AML/CTF framework. All employees and stakeholders should refer to these resources to ensure full understanding and compliance with the applicable rules:

7.1. Legal and Regulatory Framework (Curacao)

- National Ordinance on the Prevention and Combating of Money Laundering and Terrorist Financing (NOIS)

https://gobiernu.cw/wp-content/uploads/2019/07/P.B._2017_no._92.pdf

- National Ordinance on the Reporting of Unusual Transactions (NORUT)

https://gobiernu.cw/wp-content/uploads/2019/07/99_GT_Landsverordening_melding_ongebruikelijke_transacties.docx

- FIU Curaçao Official Website

<http://www.fiucuracao.cw/web/motweb/motweb.nsf/web/about>

- Gaming Control Board of Curaçao – AML Guidelines (Supervisory authority for licensed gaming operators in Curaçao)

<https://www.gamingcontrolcuracao.org>

7.2. International Framework and Best Practices

- FATF Recommendations (Financial Action Task Force)

<https://www.fatf-gafi.org/recommendations.html>

(International AML/CTF standards adopted by Curaçao)

- EU Fourth and Fifth AML Directives (for reference when assessing high-risk third countries and enhanced due diligence obligations)

<https://eur-lex.europa.eu>

7.3. Internal Policies and Procedures

- Customer Due Diligence (CDD) Procedures

(Internal guideline outlining customer verification, PEP screening, risk rating, and documentation requirements)

- Customer Risk Assessment (CRA) Template

(Used to document individual customer risk profiles during onboarding)

- Unusual Transaction Report (UTR) Internal Form

(Internal form used to submit UTRs to the Compliance Officer for review and onward reporting to FIU Curaçao)

- Account Freezing Procedure

(Protocol outlining steps for blocking or freezing customer accounts upon identification of unusual activity)

- Employee AML Training Manual

(Comprehensive training material covering AML responsibilities, red flags, and escalation procedures)

7.4. Contact Points

- FIU Curaçao Contact Email: info@fiu-curacao.com
- Gaming Control Board AML Compliance Unit: aml@gamingcontrolcuracao.org
- Internal Compliance Officer: legal@allstarcasino.com

These documents and links must be readily accessible to all relevant staff. They serve as the foundation for daily compliance operations and provide the tools needed to meet regulatory requirements and uphold the Casino's AML/CTF obligations.

8. Contact Information

Compliance Department
Email: legal@allstarcasino.com

9. Policy History

Initial version. Effective as of April 10, 2025. This Policy supersedes any previous undocumented or informal AML/CTF measures.

10. Policy URL (if applicable)

To be published on the internal Company Policy portal.

APPENDIX 1: COUNTRIES RISK ALLOCATION

This Appendix 1 is an integral and mandatory part of the Anti-Money Laundering and Counter-Terrorism Financing (AML/CTF) Policy of **Progress Path Co N.V.** (hereinafter referred to as the "Policy").

It has been developed and implemented in accordance with **Section 5.1.3(c)** (Geographical Risk) of the Policy and serves as the primary operational tool for determining the level of geographical risk associated with a client's jurisdiction of origin, residence, or activity.

The purpose of this Appendix is to ensure a uniform and Risk-Based Approach (RBA) when making decisions on the application of Standard Customer Due Diligence (CDD) or Enhanced Due Diligence (EDD) procedures for clients.

The risk classification is based on the current recommendations and lists provided by international regulators such as the Financial Action Task Force (FATF), the United Nations (UN), the European Union (EU), the U.S. Office of Foreign Assets Control (OFAC), and relevant sanctions and supervisory bodies.

FATF condemns terrorism in all its forms and shares the view that international terrorism is one of the most important security threats. Aware of the great concern caused by the increase in terrorist offences and the growing terrorist threat, FATF underlines the importance of effective multilateral co-operation to combat international terrorism and participates keenly in the action against terrorism within the framework of the UN, the EU, and the **Council of Europe**, as well as of other international organizations such as the **NATO**, **OFAC**, or the **OSCE**.

I. Low Risk Countries

A. Countries subject to the EU Money Laundering Directive – EU Member States.

B. Countries, recognized by the EU as jurisdictions having regulation “equivalent” to that set forth under the EU Money Laundering Directive.

C. Countries that are members of the FATF (except for Argentina and Turkey). FATF currently comprises 37 member jurisdictions and 2 regional organizations. As of the current day they are the following.

D. Countries that are indicated by the FAFT as jurisdictions that have made significant progress in improving their AML/CFT regime and therefore are no longer subject to an on-going global

Country	FATF member	Based on
Australia	yes	Countries, recognized by the EU as jurisdictions having regulation “equivalent” to that set forth under the EU Money Laundering Directive
Austria (1995)	yes	Countries subject to the EU Money Laundering Directive – EU Member States
Belgium (1952)	yes	Countries subject to the EU Money Laundering Directive – EU Member States
Brazil	yes	Countries, recognized by the EU as jurisdictions having regulation “equivalent” to that set forth under the EU Money Laundering Directive
Canada	yes	Countries, recognized by the EU as jurisdictions having regulation “equivalent” to that set forth under the EU Money Laundering Directive
Czech Republic (2004)	Countries subject to the EU Money Laundering Directive – EU Member States	

Denmark (1973)	yes	Countries subject to the EU Money Laundering
Estonia (2004)		Countries subject to the EU Money Laundering Directive – EU Member States
Finland (1995)	yes	Countries subject to the EU Money Laundering Directive – EU Member States
France (1952)	yes	Countries subject to the EU Money Laundering Directive – EU Member States
Germany (1952)	yes	Countries subject to the EU Money Laundering Directive – EU Member States
Greece (1981)	yes	Countries subject to the EU Money Laundering Directive – EU Member States
Hong Kong, China	yes	Countries, recognized by the EU as jurisdictions having regulation “equivalent” to that set forth under the EU Money Laundering Directive
Hungary (2004)		Countries subject to the EU Money Laundering Directive – EU Member States
Iceland	yes	FATF member
Ireland (1973)	yes	Countries subject to the EU Money Laundering Directive – EU Member States
Italy (1952)	yes	Countries subject to the EU Money Laundering Directive – EU Member States
Japan	yes	Countries, recognized by the EU as jurisdictions having regulation “equivalent” to that set forth under the EU Money Laundering Directive
Korea South Korea (Republic of Korea)	yes	FATF member Countries, recognized by the EU as jurisdictions having regulation “equivalent” to that set forth under the EU Money Laundering Directive
Latvia (2004)		Countries subject to the EU Money Laundering Directive – EU Member States
Lithuania (2004)		Countries subject to the EU Money Laundering Directive – EU Member States
Luxembourg (1952)	yes	Countries subject to the EU Money Laundering Directive – EU Member States
Malaysia	yes	FATF member
Malta (2004)		Countries subject to the EU Money Laundering Directive – EU Member States
Mexico	yes	Countries, recognized by the EU as jurisdictions having regulation “equivalent” to that set forth under the EU Money Laundering Directive
Netherlands (1952)	yes	Countries subject to the EU Money Laundering Directive – EU Member States
New Zealand	yes	Countries, recognized by the EU as jurisdictions having regulation “equivalent” to that set forth under the EU Money Laundering Directive
Norway	yes	FATF member
Poland (2004)		Countries subject to the EU Money Laundering Directive – EU Member States
Portugal (1986)	yes	Countries subject to the EU Money Laundering Directive – EU Member States
Romania (2007)		Countries subject to the EU Money Laundering Directive – EU Member States

Singapore	yes	Countries, recognized by the EU as jurisdictions having regulation “equivalent” to that set forth under the EU Money Laundering Directive
Slovakia (2004)		Countries subject to the EU Money Laundering Directive – EU Member States
Slovenia (2004)		Countries subject to the EU Money Laundering Directive – EU Member States
Spain (1986)	yes	Countries subject to the EU Money Laundering Directive – EU Member States
Sweden (1995)	yes	Countries subject to the EU Money Laundering Directive – EU Member States
Switzerland	yes	Countries, recognized by the EU as jurisdictions having regulation “equivalent” to that set forth under the EU Money Laundering Directive
Thailand		Countries that are indicated by the FATF as jurisdictions that have made significant progress in improving its AML/CFT regime and therefore are no longer subject to an on-going global AML/CFT compliance process of FATF
United Kingdom (1973)	yes	Countries subject to the EU Money Laundering Directive – EU Member States
United States of America	yes	Countries, recognized by the EU as jurisdictions having regulation “equivalent” to that set

II. Medium Risk

A. Countries that are in the process of improving its AML/CFT Legislation and that are subject to FATF on-going monitoring of developments in those countries. Such countries have strategic AML/CFT deficiencies regarding which an action plan was developed with the FATF.

B. Countries that fall neither under Low nor under High risk according to the aforementioned criteria.

C. Countries that are neither FATF members and under EU or UN sanctions related to individual persons and legal entities.

III. Non-Cooperative, High Risk and Other Monitored Countries

A. Countries subject to United Nations sanctions, embargoes or similar measures. OSH Entertainment Group does not provide services to the residents of such countries.

B. Countries identified by the FATF as high risk and non-cooperative jurisdictions due to inadequate AML controls. Oshasino does not provide services to the residents of such countries.

C. Countries identified by the FATF as high risk and other monitored Jurisdictions with strategic AML/CFT deficiencies that have not made sufficient progress in addressing the deficiencies or have not committed to an action plan developed with the FATF to address the deficiencies.

D. Countries identified to have a High or Very High impact of Terrorism according to the Global Terrorism Index, i.e. score of over 6.

Country	Based on
Afghanistan	Countries with High/Very High Terrorism Index
Algeria	Countries identified by the FATF as monitored jurisdictions
Angola	Countries identified by the FATF as monitored jurisdictions
Antigua and Barbuda	Antigua and Barbuda added to EU list of non-cooperative jurisdictions for tax purposes
Barbados	Countries identified by the FATF as monitored jurisdictions
Bolivia	Countries identified by the FATF as monitored jurisdictions
Bulgaria	Countries identified by the FATF as monitored jurisdictions
Burkina Faso	Countries identified by the FATF as monitored jurisdictions
Cameroon	Countries with High/Very High Terrorism Index. Countries identified by the FATF as monitored jurisdictions

	Countries with High/Very High Terrorism Index
China	Countries subject to OFAC, European Union and United Nations sanctions, embargoes or similar measures
Colombia	Countries with High/Very High Terrorism Index
Côte d'Ivoire	Countries identified by the FATF as monitored jurisdictions
Democratic Republic of the Congo	Countries identified by the FATF as monitored jurisdictions
	Countries with High/Very High Terrorism Index
India	Countries with High/Very High Terrorism Index
Iran	High-risk jurisdictions have significant strategic deficiencies in their regimes to counter money laundering, terrorist financing, and financing of proliferation. For all countries identified as high-risk, the FATF calls on all members and urges all jurisdictions to apply enhanced due diligence, and, in the most serious cases, countries are called upon to apply counter-measures to protect the international financial system from the money laundering, terrorist financing, and proliferation financing (ML/TF/PF) risks emanating from the country. Countries subject to OFAC, European Union and United Nations sanctions, embargoes or similar measures Countries subject to OFAC, European Union and United Nations sanctions, embargoes or similar measures
Iraq	Countries with High/Very High Terrorism Index
Israel	Countries with High/Very High Terrorism Index
Haiti	Countries identified by the FATF as monitored jurisdictions
Kenya	Countries identified by the FATF as monitored jurisdictions
Lao People's Democratic Republic	Countries identified by the FATF as monitored jurisdictions
Lebanon	Countries identified by the FATF as monitored jurisdictions
Mali	Countries with High/Very High Terrorism Index
Monaco	Countries identified by the FATF as monitored jurisdictions
Mozambique	Countries identified by the FATF as monitored jurisdictions
	Countries with High/Very High Terrorism Index
Myanmar	High-risk jurisdictions have significant strategic deficiencies in their regimes to counter money laundering, terrorist financing, and financing of proliferation. For all countries identified as high-risk, the FATF calls on all members and urges all jurisdictions to apply enhanced due diligence, and, in the most serious cases, countries are called upon to apply counter-measures to protect the international financial system from the money laundering, terrorist financing, and proliferation financing (ML/TF/PF) risks emanating from the country. Countries subject to OFAC, European Union and United Nations sanctions, embargoes or similar measures Countries with High/Very High Terrorism Index
Namibia	Countries identified by the FATF as monitored jurisdictions
Nepal	Countries identified by the FATF as monitored jurisdictions
Niger	Countries with High/Very High Terrorism Index
Nigeria	Countries identified by the FATF as monitored jurisdictions
	Countries with High/Very High Terrorism Index
Pakistan	Countries with High/Very High Terrorism Index
Russian Federation	Countries subject to OFAC, United Nations and European Union sanctions, embargoes or similar measures
Somalia	Countries with High/Very High Terrorism Index
South Africa	Countries identified by the FATF as monitored jurisdictions
South Sudan	Countries identified by the FATF as monitored jurisdictions
Syria	Countries identified by the FATF as monitored jurisdictions
	Countries with High/Very High Terrorism Index
Terrorism (ISIL; Al-Qaida)	Countries subject to OFAC, United Nations and European Union sanctions, embargoes or similar measures

The Democratic People's Republic of Korea	High-risk jurisdictions have significant strategic deficiencies in their regimes to counter money laundering, terrorist financing, and financing of proliferation. For all countries identified as high-risk, the FATF calls on all members and urges all jurisdictions to apply enhanced due diligence, and, in the most serious cases, countries are called upon to apply counter-measures to protect the international financial system from the money laundering, terrorist financing, and proliferation financing (ML/TF/PF) risks emanating from the country.. Countries subject to OFAC, European Union and United Nations sanctions, embargoes or similar measures
Uganda	Countries identified by the FATF as monitored jurisdictions
Venezuela	Countries identified by the FATF as monitored jurisdictions
Vietnam	Countries identified by the FATF as monitored jurisdictions
Virgin Islands (UK)	Countries identified by the FATF as monitored jurisdictions
Yemen	Countries identified by the FATF as monitored jurisdictions

IV. Operational Requirements: Geographical Risk Mitigation Measures

This section establishes clear, operational steps for applying Customer Due Diligence (CDD) procedures based on the country's risk category.

Country Category	Risk Level	Required Operational Measures
I. Low Risk Countries	Low	Standard Customer Due Diligence (CDD). Simplified Due Diligence (SDD) may be applied in accordance with the internal SDD protocol approved by the Compliance Officer, and/or with their documented authorization, provided no other high-risk factors, specified in the Policy, are present. The decision to apply SDD must be documented within the system.
II. Monitored/Other Risk Countries	Medium / High	Enhanced Due Diligence (EDD). Mandatory approval from the Compliance Officer is required prior to establishing a business relationship. Continuous Enhanced Transaction Monitoring must be applied.
III. Sanctioned/Non-Cooperative Jurisdictions	Highest	Rejection of Business Relationship. It is prohibited to establish or continue business relationships, or process any transactions, associated with the jurisdiction or its nationals, unless specifically authorized by a license.

In witness whereof, Progress Path Co N.V. has caused this Policy to be duly executed this 6th day of November 2025

By: e-Management N.V. as Director of Progress Path Co N.V.