

AML/CFT Policy Curaçao – Bet Pegasus

KEY INFORMATION

1. POLICY STATEMENT

2. PURPOSE

3. AUDIENCE

4. DEFINITIONS

4.1 Money Laundering (ML)

4.2 Terrorist Financing (TF)

4.3 Proliferation Financing (PF)

4.4 Comparison between Money laundering, Terrorist Financing & Proliferation Financing

4.5 Targeted Financial Sanctions

5. POLICY IMPLEMENTATION

5.1 Business Risk Assessment

5.2 Customer Risk Assessment (CRA)

5.2.1 CRA Methodology

5.2.2 Ongoing customer risk scoring and updates

5.2.3 Multiple Payment Methods

5.2.4 Multiple Product Types

5.2.5 Closed-Loop and Non-Closed-Loop Accounts

5.2.6 Scoring Principle

5.2.7 Risk Scoring Score

5.2.8 Combined Customer Risk Score

5.3 Customer Acceptance Policy

5.3.1 Customer Identification Procedure

5.3.2 Risk Classification

5.3.3 High Risk Customers

5.3.4 Compliance Officer Approval for Higher Risk Customers

5.3.5. Due Diligence

5.3.6 Termination of Business Relationship

5.4 Customer Due diligence

5.4.1 Simplified Due Diligence.

5.4.2 Enhanced Due Diligence

5.4.2.1 Customer profiling

5.4.2.2 Outcomes and ongoing monitoring

5.4.3 Politically Exposed Persons (PEPs)

5.4.3.1 Domestic PEPs

5.4.3.2 Foreign PEPs

5.4.3.3 International Organisation (IO) PEPs

5.4.3.4 Known Associates and RCAs

5.4.3.5 Screening for PEP status

5.4.3.6 PEP Log

5.4.4 Sanctions

5.5 Ongoing Monitoring

5.6 Reliance on third parties to perform customer due diligence.

5.7 Reporting of unusual transactions

5.7.1 Reporting of Unusual Transactions

5.7.2 Objective Indicators – Automatic Reporting Requirements

5.7.3 Recognition of Unusual Transactions (Subjective Indicators)

- 5.7.4 Internal Reporting (iSARs)
- 5.7.5 MLRO Review and Decision
- 5.7.6 External Reporting to the FIU
- 5.7.7 Documentation and Non-Submitted iSARs
- 5.7.8 Prohibition on Disclosure (“Tipping Off”)
- 5.7.9 Record Keeping
- 5.8 Anti-Money Laundering Compliance program
 - 5.8.1 Risk Based Approach
 - 5.8.2 Internal policies, procedures and controls.
 - 5.8.3 The AML/CFT Compliance Officer or MLRO
 - 5.8.4 Independent Audit function
 - 5.8.5 Employee Screening and Ongoing Training Program
- 6. COMPLIANCE AND CONSEQUENCES OF NON-COMPLIANCE
- 7. RELATED INFORMATION
- 8. CONTACT INFORMATION
- 9. POLICY HISTORY

KEY INFORMATION

Approving Official: Joaquin Paton

Responsible Office: Customer Operations - VP of Player Protection & Compliance

Effective Date: 01/05/2026

Next Review Date: 01/05/2027

1. POLICY STATEMENT

Bet Pegasus N.V. (the “Company”) is committed to preventing its products, services, systems, and employees from being used for money laundering (ML), terrorist financing (TF), or proliferation financing (PF).

We implement a documented, risk-based AML/CFT program proportionate to our risks and fully aligned with Curaçao’s regulatory framework. The Company will cooperate with all competent authorities and ensure prompt, accurate reporting of required information.

2. PURPOSE

This policy sets the minimum standards, controls, and procedures by which the Company identifies, assesses, mitigates, monitors, and reports ML/TF/PF risks across its Curaçao-licensed operations. It defines responsibilities, prescribes customer due diligence (CDD)

measures, establishes escalation and reporting protocols, and documents training, audit, and recordkeeping requirements.

3. AUDIENCE

This policy applies to all customers allowed to access our site or app under the Curaçao Licence. This Policy applies to all persons working for Bet Pegasus; including employees at all levels, directors, officers, agency workers, seconded workers, volunteers, interns, agents, contractors, external consultants, third-party representatives and business partners, sponsors, or any other person associated with us, wherever located (collectively referred in this Policy as ‘Employees’).

4. DEFINITIONS

4.1 Money Laundering (ML)

Money laundering is the process of taking money derived from criminal activity and disguising its illegal origin so it appears legitimate. It typically involves **three stages**:

Placement

Criminal funds are first introduced into the financial system. In a gaming context, this may include:

- Buying casino chips with cash and redeeming them with little or no play.
- Funding gaming accounts using credit/debit cards, prepaid cards, cheques or cryptocurrency and quickly requesting withdrawals.
- Loading funds into gaming machines and immediately cashing out as credits.

Layering

The launderer then obscures the audit trail by moving or converting funds. This may involve:

- Transfers between accounts, casinos, or jurisdictions.
- Currency exchanges or structured transactions designed to avoid detection.
- Using gambling accounts to store, move, or conceal funds.

Integration

Finally, the funds are reintroduced into the economy as seemingly legitimate assets or transactions, such as:

- Buying luxury goods or financial investments.
- Investing in gaming or commercial businesses.

While drug trafficking is commonly associated with money laundering, **many other offences** can generate illicit funds, including human trafficking, arms trafficking, robbery, fraud, corruption, kidnapping, and tax crimes.

4.2 Terrorist Financing (TF)

Terrorist financing (FT) refers to providing financial support to terrorists, terrorist organisations, or terrorist acts. A terrorist act is any action intended to intimidate a population or to pressure a government or international organisation to take, or refrain from taking, a particular action.

The key difference between FT and money laundering lies in the origin and purpose of the funds. Terrorist financing may involve money from either legitimate or illegitimate sources, whereas money laundering always involves the proceeds of crime. Because of this, terrorists focus on concealing the destination of the funds rather than their origin. In practice, terrorist groups often attempt to hide the connection between themselves and their funding sources, using methods similar to those seen in money laundering. These can include cash smuggling, structuring, wire transfers, purchasing monetary instruments, and the use of debit or credit cards.

4.3 Proliferation Financing (PF)

Proliferation financing (PF) is the provision of funds for the manufacture, acquisition, possession, development, export, trans-shipment, brokering, transport, transfer, stockpiling or use of nuclear, chemical or biological weapons and their means of delivery and related materials.

4.4 Comparison between Money laundering, Terrorist Financing & Proliferation Financing

	Money Laundering	Terrorist Financing	Proliferation Financing
--	---------------------	------------------------	----------------------------

Source of Funds	Internally from within criminal organisations	Internally from self- funding cells (centred on criminal activity)	Often state-sponsored programs but also through fundraising activities by non-state actors
Conduits	Favours formal financial system	Favours cash couriers or informal financial systems such as Hawala and currency exchange firms	Formal financial system preferred up until the point of entry into DPRK, where the money is then taken out in cash in a neighbouring country and carried in to DPRK.
Detection Focus	Suspicious transactions such as deposits uncharacteristic of customer's wealth or the expected activity	Suspicious relationships, such as wire transfers between seemingly unrelated parties	Individuals, entities, states, goods and materials, activities
Transaction Amounts	Usually, large amounts often structured to avoid reporting requirements	Often, small amounts usually below reporting thresholds	Often moderate amounts
Financial Activity	Complex web of transactions often involving shell or front companies,	Varied methods including formal banking system, informal value-transfer systems,	Usually, transactions look like normal commercial activity,

	bearer shares, offshore secrecy havens	smuggling of cash and valuables	structured to hide connection to proliferator or proliferation activities
Money Trail	Circular – money eventually ends up with the person who generated it	Linear – money generated is used to propagate terrorist groups and activities	Linear – money is used to purchase goods and materials from brokers or manufacturers. The money can also move in the opposite direction (i.e. from the broker/ manufacturer to the proliferator).

4.5 Targeted Financial Sanctions

Targeted financial sanctions require the freezing of funds and assets belonging to designated individuals or entities, and prohibit making any funds or assets available to them, directly or indirectly. In Curaçao, all natural and legal persons must freeze such assets immediately and without prior notice, in line with UN Security Council resolutions and EU Common Foreign and Security Policy measures. These obligations are legally binding under the UN Charter and the Kingdom Sanctions Act.

5. POLICY IMPLEMENTATION

The Company maintains a clear governance structure to ensure accountability for AML, CTF and PF compliance.

Senior management is responsible for ensuring that the business identifies, assesses and manages its ML/TF/PF risks, and for approving and overseeing the policies, controls and resources necessary to comply with the Regulations. Senior management is actively engaged in the development, approval and ongoing review of the company's AML/CTF/PF framework.

At Bet Pegasus, the following **senior management** functions form the governance and oversight structure for AML/CTF/PF:

- **The Leadership Team (executive board)** acts as the company's senior governing body and provides strategic oversight of AML/CTF/PF matters.
- **The Chief Operations Officer (COO)** sits on the CXO and has executive oversight of the Company's AML/CTF/PF framework and reports AML/CTF/PF matters to the Leadership Team as appropriate.
- The **Vice President (VP) of Player Protection and Compliance** reports directly to the COO and is responsible for overseeing the Company's compliance and player protection functions, including the implementation and effectiveness of the AML/CTF/PF framework.
- **The AML/CFT Compliance Officer, or Money Laundering Reporting Officer (MLRO)**, is the nominated officer responsible for the day-to-day oversight of the AML/CTF framework, receiving and evaluating internal disclosures, and determining whether Unusual Transaction Reporting (UTR) must be submitted to the FIU Curaçao. The MLRO reports directly to the Vice President of Player Protection and Compliance, who in turn reports to the COO.

The AML/CFT Compliance Officer (Joaquin Paton) is supported by the AML Officer, who deputises in the MLRO's absence, and by the wider Compliance and Operations Teams, including the AML & EDD Team, which assists with investigations, reporting and ongoing monitoring activities across the business.

The AML/CFT Compliance Officer has unrestricted access to all relevant systems, data and information required to fulfil their regulatory duties effectively.

The AML/CFT Compliance Officer conducts an annual review of the AML Policy and the AML/CFT Risk Assessment, and reports the outcomes to the VP of Player Protection & Compliance, who ensures that the Leadership Team is informed of key risks and that these are considered within strategic planning and resource allocation. Both the AML Policy and Risk Assessment are updated at least annually, and more frequently where material changes to Bet

Pegasus' risk profile, business operations or product offering occur. Senior management is informed of any new or emerging key risks.

The AML/CFT Compliance Officer also prepares an **Annual MLRO Report**, outlining the operation and effectiveness of the company's AML/CTF/PF systems and controls and recommending actions to address deficiencies or risks. This report is submitted to and approved by the Leadership Team, ensuring senior management oversight of the AML framework. The AML/CFT Compliance Officer may also provide additional updates to senior management throughout the year where circumstances require.

5.1 Business Risk Assessment

The Company performs an annual risk assessment to identify any new threats, analyse any associated vulnerabilities and assess the effectiveness of its AML/CTF systems and controls. The AML/CFT Compliance Officer is responsible for ensuring the assessment is carried out on an annual basis and/or in the event of material changes to the risk environment and/or when new products, businesses practices or technologies are adopted. The results of the assessment are reported to the Compliance Committee and escalated as appropriate to relevant SLT and CXO boards. The purpose of the risk assessment is to:

- Identify risks relevant to the Company's businesses and analyse associated vulnerabilities and consequences of these risks
- Ensure sufficient controls are in place to mitigate against those risks
- identify gaps or opportunities for improvement in AML/CTF policies, processes and procedures;
- assess and make informed decisions about risk appetite and implementation of controls;
- assess allocation of resources and technology spend;
- develop risk mitigation strategies;
- ensure senior management are made aware of the key risks, control gaps and remediation efforts;
- assist senior management with strategic decisions in relation to AML/CTF;
- assist management in ensuring that resources and priorities are aligned with its risks; and
- ensure, where necessary, the regulator is made aware of the key risks, control gaps and remediation efforts across the Company.

5.2 Customer Risk Assessment (CRA)

A fundamental element is the requirement for all operators to conduct a Customer Risk Assessment on all customers during establishing a business relationship. The initial CRA conducted is constantly revised considering all the activity in the customer's account.

The determination of a customer's risk profile is essential in applying the correct level of CDD to the identified ML/FT risk. The CRA allows us to build a customer profile in order to assess the customers activity to identify any unusual behaviour in the course of the business relationship. The Customer Risk Assessment considers the following information.

- *Age of the Customer*
- *Country of registration*
- *Payment Method used*
- *Products Played and Transactions made*

While the primary purpose of opening a gaming account in the remote gaming sector is recreational, we understand the importance of due diligence in higher-risk scenarios. The information that we request from customers reflects the level of risk identified through the CRA. In low-risk situations a declaration from the customer and/or information obtained through open-source checks would suffice. However, for medium and high-risk customers, additional information regarding the customer's business, occupation, or employment is gathered on a risk-based approach. When the risk of ML/FT is increased and /or if we have doubts regarding the veracity of the information collected, we obtain supplementary information by way of documentation and/or reliable and independent sources of information.

The payment / transactions risk is measured by identifying the payment methods of choice for the customers and the degree to which their specific characteristics may be attractive for the purpose of money laundering or financing terrorism.

The Company evaluates the specific risks associated with doing business in, opening accounts for customers from, or facilitating transactions involving certain geographic locations. This risk is evaluated in the [Country Risk Assessment](#).

Certain gambling products are inherently more attractive to criminals than others. As part of the CRA, we assess product risk by examining the specific type of product used by each customer. The types of products considered include:

- *lotto betting;*
- *sports betting; and*
- *casino-style games*

Each product's risk level is assessed based on its susceptibility to ML/FT, informing the CRA accordingly.

5.2.1 CRA Methodology

CHARACTERISTIC	GAME TYPE	PAYMENT METHOD	COUNTRY RISK (see country risk scoring)	CUSTOMER RISK	ACTIVITY (only highest scoring counts)
Sports	Medium				
Live Casino	Medium				
Blackjack/ Baccarat/ Roulette	Low-Medium				
Slots	Low				
Lotto/ Bingo	Low				
Cash based/ Prepaid card		High			
Ewallet		Medium			
EEA debit card		Low			
Bank transfer		Low			
EEA PSPs		Medium			
Country			Low/Medium/High		

Ages 18-25 and 70+				Medium	
Ages 25+				Low	
Not Closed looped					Medium
Closed looped					Low
Total deposits in past 7 days are over EUR 10k					High

Each metric has its assigned risk score, and only the highest scoring one that is true for the customer is counted.

New customers, where there is no data available, because no play took place or there was no deposits etc, should default as low risk for each attribute as there is insufficient data to complete the calculation. The exception to this is customers flagged as PEPs or those who appear or may appear on a sanctions list, who are always considered high risk regardless of other metrics.

5.2.2 Ongoing customer risk scoring and updates

Each customer is assigned an ongoing risk score, which is reviewed and recalculated on a weekly basis automatically in Comply Radar, covering activity from the previous seven days.

The use of a seven-day rolling review period ensures that customer risk assessments remain accurate and reflective of current behaviour. This approach allows risk scores to adjust dynamically as customer activity changes, avoiding situations where a customer who previously displayed higher-risk behaviour would remain permanently classified as high risk despite sustained lower-risk activity. Historical indicators, such as PEP status, remain permanently recorded and factored into the customer's overall profile, while the seven-day period ensures that behavioural risk is assessed in a timely and proportionate manner consistent with a risk-based approach.

5.2.3 Multiple Payment Methods

Where a customer has used multiple payment methods, the highest depositing payment method during the past seven days is used in the risk calculation.

However, if a higher-risk payment instrument has been used for at least 30 % of total deposits within the same period, the risk score associated with that higher-risk instrument will be applied.

Example:

If a Visa card accounts for 69 % of deposits and a prepaid card for 31 %, the prepaid-card risk score is used for the calculation.

5.2.4 Multiple Product Types

Where a customer has activity across multiple product types, the product with the highest turnover (stakes) over the past seven days is normally used for the risk calculation.

If a higher-risk product represents at least 30 % of the total stakes during that period, the risk associated with that higher-risk product is applied instead.

Example:

If 70 % of a customer's turnover over the past seven days is on Slots and 30 % on Sports, the "Medium (30)" risk score corresponding to Sports is used.

5.2.5 Closed-Loop and Non-Closed-Loop Accounts

For the attributes "closed-loop" and "not closed-loop", each account must fall into one of the two categories.

The logic is binary — if the criteria for "closed-loop" are not met, the account is automatically considered "not closed-loop."

"Closed-loop" refers to the relationship between deposit and withdrawal payment accounts.

Identify the highest depositing and highest withdrawing payment accounts over the past three months.

If these are the same account, the payments are considered closed-loop.

5.2.6 Scoring Principle

Each metric has an assigned risk score, and only the highest-scoring applicable metric is counted in determining the customer's overall risk score.

For **new customers**, where no data is yet available (e.g., no play or deposits), all attributes default to low risk, as there is insufficient data to complete the calculation.

5.2.7 Risk Scoring Score

Individual characteristic	Score
Low	10
Low-Medium	20
Medium	30
Medium-High	40
High	50

5.2.8 Combined Customer Risk Score

The customer risk score is the average of all attributes combined (Attribute 1 +Attribute 2 + Attribute 3 + Attribute 4 + Attribute 5 divided by 5).

Combined (Average of all characteristics) customer risk score	Score (AVG)
Low	10 - 24
Medium	25 - 44
High	45 - 50

5.3 Customer Acceptance Policy

5.3.1 Customer Identification Procedure

When establishing a new business relationship the customer needs to provide the following information as a minimum:

- Full Name
- Date of Birth
- Residential Address

- Phone Number
- Email Address

Customer identification means identifying the customer and verifying his/her identity by using reliable, independent source: documents or data. The Company obtains sufficient information necessary to establish, to our satisfaction, the identity of each new customer.

5.3.2 Risk Classification

The main indicators which the company considers in determining whether a business relationship presents low, medium or high ML/FT risk are: the payment instrument, transactions, product used, behaviour, associated country and the customer's age. As and where more information becomes available for individual customers, usually following specific triggers, this new information is factored in the profile.

The company perceives as low risk a customer who uses a debit card/ bank transfer to fund their gambling, plays recreationally (risks/ wagers multiple times the deposited funds) on products where the player has no influence on the outcome (i.e. lottery), is of age that is not associated with being a student/ on lower income or too senior (therefore likely vulnerable).

A medium risk customer would be a slight deviation of the above profile where some of the attributes would be higher risk, for example the player is younger than 25, is using a digital wallet to fund the account or is placing the majority of his bets on sports, where the risk may be significantly lower.

5.3.3 High Risk Customers

As per the Company's Customer Risk Assessment and Business Risk Assessment, the following is a non-exhaustive list of features of accounts that pose higher than average risk of ML/FT. The more of the below features an account possesses, the higher the associated risk:

- predominant use of payment instruments that can be/ are funded by cash and/or lack customer verification
- demonstrate gambling activity which aims to limit their risk exposure through minimal, low risk or no gameplay
- Attempt to use live casino to transfer funds across to other players, covering all outcomes or other similar activity.
- Have high deposits and/ or account spend is high
- Shows links to countries identified as higher risks, be it based on origin, residency, payment methods, IPs or other.
- PEP Match

5.3.4 Compliance Officer Approval for Higher Risk Customers

The AML/CFT Compliance Officer/Money Laundering Reporting Officer (MLRO) approval is required to continue business relationships with customers identified as high-risk. This includes:

- **Politically Exposed Persons (PEPs):** Due to the elevated risk associated with PEPs, their business relationships require MLRO approval.
- **Customers with Cumulative Lifetime Losses exceeding €300,000:** Significant losses may indicate potential risk factors requiring additional scrutiny and SOF documentation.
- **Any Other Customer Considered High Risk,** including those outlined in **Section 5.4.3.**

5.3.5. Due Diligence

The Company applies a different level of CDD and EDD measures depending on the associated to the business relationship risk.

- For all Low risk customers an in-depth review of the customers' finances and game play will be made when their Net Deposits or Net Losses reach the generic EDD threshold for the licence. This SOW check is specific to that player but can rely on Social Media and open searches to clarify the occupation and wealth of the individual.
- For Medium risk customers this threshold reduces to the average national income (country dependant). The review is specific to that player but can rely on Social Media and open searches to clarify the occupation and wealth of that individual.
- For High risk customers and all PEPs, EDD checks are carried out as soon as they are identified.

All accounts undergo ongoing monitoring also of their deposits, losses and wagering activity, using a combination of EDD Thresholds and AML behavioural Triggers in Comply Radar.

Moreover, any accounts that go through the EDD process are monitored more closely, with additional personalised thresholds based on their expected or anticipated level of activity.

5.3.6 Termination of Business Relationship

The Company declines to serve the following individuals

- Individuals under the age of 18.
- Customers who have fallen into the EDD process (including PEPs) and there isn't sufficient information found through open source or directly from the customer to alleviate the Company's ML/FT concerns.

- Customers confirmed to be on a Sanctions list, or individuals whose reputation in the media seems to be tainted due to connection with criminal activities.
- Customers located in or residents of high risk jurisdictions, such as those on the FATF Black list.
- Customers whose identity cannot be duly verified as per our policies and procedures.
- Customers whose gambling activity leads to an increasing level of suspicion, or actual knowledge of, ML, TF or PF.

The Company will also terminate the business relationship with immediate effect in cases of breach of the general terms and conditions, where the account activity does not comply with the intent and purpose of the business relationship, or for non-compliance with company rules and licensing regulations.

5.4 Customer Due diligence

CDD involves a combination of Simplified Customer Due Diligence (SDD), Enhanced Customer Due Diligence (EDD) and Ongoing Monitoring as further explained below. CDD is a critical element of effectively managing Bet Pegasus' risks and protecting it against potential criminal activity.

By adopting a risk-based approach, Bet Pegasus ensures that measures to prevent or mitigate money laundering and terrorist financing are commensurate with the risks identified. This allows resources to be allocated in the most efficient way.

Know your customer (KYC) is the process used by the company to verify the identity of our customers. There are different levels of due diligence we perform, all of which are determined on a risk-based approach. As per the current regulations, Bet Pegasus will undertake CDD measures when:

1. When players engage in financial transactions equal to or above Naf. 4,000 (€2,000);
2. there is a suspicion of money laundering or terrorist financing; or
3. there are doubts about the veracity or adequacy of previously obtained customer identification data.

In all these scenarios, we will identify and verify the identity of the player and carry out a customer risk assessment.

5.4.1 Simplified Due Diligence.

The Company requires all its customers to register basic details. This is a two stages process:

- **Registration:** account opening processes allow the customer to submit various personal details such as full name, email address, D.O.B., nationality, address and country of residence. All customers must register themselves on our website by filling in the registration form to be allowed to play.
- **Verification of submitted details:** *this is performed when the financial transactions are equal to or above Naf. 4,000 (€2,000 or earlier on a risk sensitive basis, using available third-party databases and/or by manually verifying documents submitted by the customer (e.g. ID and Proof of Address dated within the past 6 months) amongst others.*
 - If a customer's financial transactions reach or exceed €2,000 without providing necessary verification documents, the Risk team will request ID and proof of address. If we do not receive this documentation within 30 days, the account is suspended until the verification is complete.

A risk-based approach is followed to keeping customer data up-to-date. This includes:

- Obtaining fresh identification documents for those expired based on specific trigger events that may indicate a heightened risk profile. This includes reaching AML/EDD thresholds or large withdrawals.
- Regularly reviewing and updating customer information, even for non-expired documents, to ensure continued accuracy. This may be prompted by internal reviews of the account activity or when the Risk team identifies potential concerns during their daily BI report reviews.
- Promptly investigating any inconsistencies found in existing customer data.

Where the company discover that a customer has provided false or stolen identification documentation or information, and/or where the information held by the company differs from that of the customers transaction patterns, the relationship will be terminated, and consideration given to whether it is appropriate to submit a SAR/UTR. Any customer account closed on these circumstances, will be added to the internal SAR log.

5.4.2 Enhanced Due Diligence

Enhanced Due Diligence (EDD) is completed when a customer hits any internal AML/EDD thresholds and/or at any point of the player journey in order to ascertain the legitimacy of the funds deposited, or general queries on the operation of the player account. The Company does

not solely rely on threshold events and the following cases will also trigger EDD reviews and enhanced ongoing monitoring in order to manage and mitigate any potential ML/TF risks:

- *Where there is a high risk of money laundering or terrorist financing;*
- *Where the customer is high risk as per CRA*
- *Where the customer is medium risk but spend is above the average national income for his country of registration*
- *Where a customer or potential customer is a PEP, or a family member or known close associate of a PEP;*
- *In any case where a transaction is complex or unusually large, or there is an unusual pattern of transactions, and the transaction or transactions have no apparent economic or legal purpose*
- *In any other case which, by its nature, can present a higher risk of money laundering or terrorist financing.*

The EDD measures could include, but may not be limited to:

1. Undertaking additional identification checks via further documents, data or information (for example, requesting copy of ID, proof of address (POA), SOF, SOW, etc.); or
2. Supplementary measures to verify or certify documents (for example, requesting certified copies of POI, POA, etc.); or
3. Making sure that payments “in” (deposits) and/or “out” withdrawals, are paid from/to the same accounts and/or payment method (e.g. debit card etc.).
4. Identifying the use of multiple payment methods for funding an account and evaluating the associated risk.
5. Carrying out SOF and SOW checks (as outlined below)
6. Examining the background and purpose of the transaction, as far as reasonably possible;
7. Determining the expected level of customer activity through EDD review, aligning with affordability checks and the SOF documents submitted by the customer, by implementing monthly Net Loss Limits on customer accounts.
8. Increasing the degree and nature of monitoring of the business relationship which the transaction is made, to determine whether the transaction or the relationship appear to be suspicious;
9. Seeking additional independent, reliable sources to verify information provided or made available to the company;

10. Taking additional measures to understand better the background, ownership and financial situation of the customer, and other parties to the transaction, i.e; payslip, savings, inheritance, bank statement;
11. Where customer activity raises concerns, taking further steps to be satisfied that the transaction is consistent with the purpose and intended nature of the business relationship;
12. Increasing the monitoring of the business relationship, including greater scrutiny of the transaction.

5.4.2.1 Customer profiling

As part of the profiling, customers are reviewed by the AML team, taking into account any affordability and ML, TF & PF risks.

Accounts then undergo a selection of EDD checks, which are documented in a report, including but not limited to: open-source searches for adverse or source of income information and review for any ML, TF & PF red flags of the betting activity, login history, payments and linked accounts. In majority of the cases the information we hold may not be sufficient to confirm the potential source of the funds used, so where deemed necessary, customers are contacted to request further information about the source of the funds they use and documents to confirm their admissions.

The aim of Customer Profiling is to gain understanding of the source of the funds used for the account activity and satisfy us that the funds being used for gambling are not the proceeds of crime, or above what is deemed affordable for the customer.

Source of Funds (SOF) refers to the origin of the particular funds used in the business relationship (the amounts being deposited).

Source of Wealth (SOW) goes beyond that, as it refers to the total wealth of a client and how that wealth was initially derived. The total wealth of the client should make sense; i.e. it should be commensurate with the client's background, activity with the company, and should be verifiable from independent sources, including documents provided by the client.

Documents for verification of the above are reviewed and accepted on a case by case basis, ensuring that they mitigate any risk factor identified.

If throughout the customer due diligence process a customer is flagged as high-risk and we are unable to obtain sufficient information from the player to understand the origin of their funds and their legitimate origin the business relationship would be terminated and where there is suspicion of ML, TF & PF an external disclosure to the FIU would be made.

5.4.2.2 Outcomes and ongoing monitoring

The information gathered from these checks gets summarised and analysed by the AML team and where necessary escalated to senior management and the MLRO.

Where the sources of funds identified for the B2C customer are not commensurate with the account activity, or the information found leads to further concerns, and the customer is unable/unwilling to provide further sufficient information/evidence to confirm the legitimacy of the funds used, the account is closed and a SAR/UTR is considered.

Where the information gathered is deemed satisfactory to alleviate ML/ TF concerns the account is signed off to a level of activity corresponding to the amounts evidenced by the investigation. These accounts would then remain active, subject to ongoing monitoring by all standard triggers and specific monitoring limits in line with the customer profile.

As indicated in the Company's business risk assessment in addition to the above mentioned processes, the Company also relies on a number of customer behaviour alerts actioned by the Fraud (Risk) department. The actions taken by the Fraud Analysts have been deemed sufficient to help mitigate some AML risks (for example confirming payment card ownership and dealing with a mismatch in country of residence and bank country) if further ML/TF concerns arise, Fraud Analysts are trained to escalate their concerns to the AML team.

5.4.3 Politically Exposed Persons (PEPs)

A PEP generally presents a higher risk of potential involvement in bribery and corruption by virtue of their position and the influence that they may hold. Individuals who have or held a high political profile or who have held public office (past or present) pose a higher-risk, as their positions may make them vulnerable to corruption and bribery, therefore increasing the risk of accounts being funded by the proceeds of crime by such individuals. PEPs might attempt to circumvent screening controls by using third party individuals as proxies to gamble on their behalf with their financial instruments.

The fourth Money Laundering Directive defines a 'politically exposed person' as a natural person who is or who has been entrusted with prominent public functions and includes the following:

1. *Heads of state, heads of government, ministers and deputy or assistant ministers;*

2. *Members of parliament or of similar legislative bodies;*
3. *Members of the governing bodies of political parties;*
4. *Members of supreme courts, of constitutional courts or of other high-level judicial bodies, the decisions of which are not subject to further appeal, except in exceptional circumstances;*
5. *Members of courts of auditors or of the board of central banks;*
6. *Ambassadors, charges d' affaires and high-ranking officers in the armed forces;*
7. *Members of the administrative, management or supervisory bodies of state-owned enterprises;*
8. *Directors, deputy directors and members of the board or equivalent functions of an international organisation.*
9. i) *Associated persons close to the PEP, partners, individuals with shared beneficial ownership in the same legal entity or trust fund, individuals known to have a significant business relationship with them, or the owner of a legal entity or trust fund created for the benefit of a PEP.*

5.4.3.1 Domestic PEPs

The FATF Guidance for PEPs also defines Domestic PEPs as high-risk individuals located in the same country as the financial institution of which it is a client and has a domestically located position. These domestic high-risk individuals are defined as officials of a local political party, senior politicians, heads of state companies, or senior military officials. Other factors, such as the PEPs place of residence, are not important in determining the type of PEP, but these factors can be an important factor in determining the risk level of a particular Domestic PEP. Domestic PEPs are generally considered less risky than Foreign PEPs.

5.4.3.2 Foreign PEPs

Foreign PEPs can make it more difficult to evaluate information during the account opening and customer relationship monitoring phases. Therefore, appropriate risk management is required to address these specific risks within these processes. Foreign PEPs are always considered high-risk, and therefore Enhanced Due Diligence (EDD) measures must be applied instead of Customer Due Diligence (CDD) measures, as with all high-risk customers.

5.4.3.3 International Organisation (IO) PEPs

Persons who are or have been entrusted with a prominent function by an international organisation, refers to members of senior management or individuals who have been entrusted with equivalent functions, i.e. directors, deputy directors and members of the board or equivalent functions. Organisations such as WHO, WTO & FIFA are all categorised as International Organisations.

5.4.3.4 Known Associates and RCAs

The following individuals are also regarded as PEPs by virtue of their relationship or association with the individuals listed above:

'Family members' includes the following;

- The spouse, or a person considered to be equivalent to a spouse, of a politically exposed person;
- The children and their spouses, or person considered to be equivalent to a spouse, of a politically exposed person;
- The parents of a politically exposed person

Persons known to be closed associates' means:

- Natural persons who are known to have joint beneficial ownership of legal entities or legal arrangements, or any other close business relations, with a politically exposed person;
- Natural persons who have sole beneficial ownership of a legal entity or legal arrangements which is known to have been set for the de facto benefit of a politically exposed person.

Any PEP identified by our screening activity or open source investigation must be reviewed by the MLRO and future relationship with the player defined. This includes any deposit or gambling arrangements. Prior to any approval EDD must be performed on the player.

The MLRO must be satisfied that the identified PEP does not pose any risk to the company. In assessing the risk, an important factor is the location of the PEP and whether the PEP is from a high-risk jurisdiction. To assist in the assessment and ultimate decision on whether to continue with the relationship, The Company uses available third-party databases that allow it to compare the registration details of the customer with information contained on this database.

5.4.3.5 Screening for PEP status

Customers are screened against PEPs lists using a third-party provider, SEON. This screening is performed initially upon establishing the business relationship, and subsequently on a daily basis to identify any changes in a customer's PEP status.

When a customer is flagged as a PEP, an EDD Report is completed to establish the Source of Funds and to conduct a thorough risk assessment of the customer. The MLRO reviews the outcome of the EDD review and decides whether the business relationship can be continued, based on the risk assessment, and determines appropriate mitigating measures and ongoing monitoring.

5.4.3.6 PEP Log

Any identified PEP is recorded within the [PEP Log](#). This enables the MLRO to ensure enhanced monitoring is undertaken where applicable. The company can also identify any relevant changes which might increase the risk of the relationship and therefore trigger a further review or termination.

5.4.4 Sanctions

Customers are screened against sanctions lists using a third-party provider, SEON. This screening is performed initially upon establishing the business relationship, and subsequently daily to identify any changes.

If a customer is identified as being in a sanction list, the relationship will be terminated immediately. Under no circumstances will Bet Pegasus knowingly, engage in a relationship with a person and /or organisation appearing in a sanctions list.

Sanction checks are performed daily or where there is reason to believe that a customer account requires additional checks. If a customer is on a sanction list a report will be sent to the Financial Intelligence Unit of Curaçao as soon as identified.

Bet Pegasus will assist the FIU if it becomes necessary to freeze, seize or surrender funds under the control of a person or institution on the sanctions list.

5.5 Ongoing Monitoring

All customer activity (deposits, withdrawals, gambling activity, communications, use of gambling management tools, etc.) is recorded.

In line with our legislative and regulatory requirements as well as factoring in the results of our AML/CTF Risk Assessment, we have developed a combination of systems and processes to effectively monitor customer's activity through the use of non-financial triggers.

Monitoring is designed to identify and escalate high-risk factors (Red Flags), as prescribed by relevant legislation and internal policies, which individually or in combination may warrant EDD or further escalation, including but not limited to:

1. Cases identified as presenting a high risk of money laundering or terrorist financing, or where the nature of the business relationship inherently poses higher ML/TF risk.
2. Relationships or transactions involving players connected to high-risk or sanctioned jurisdictions, including those linked to citizenship/residence-by-investment schemes or using

products that favour anonymity.

3. Players determined to be Politically Exposed Persons (PEPs), family members, or close associates of PEPs, or other categories of customers such as beneficiaries of life insurance policies that may pose elevated ML/TF risk.
4. Instances of false, stolen, or otherwise fraudulent identification or account misuse, including counterfeit or AI-generated documents, multiple or duplicate accounts, or accounts linked by shared devices/IPs.
5. Transactions that are complex, unusually large, or without an apparent economic or legal purpose, such as large deposits with minimal play, instances of low risk wagering or sudden behavioural changes.
6. Transactions funded by third parties without a legitimate or verified connection to the player, or attempts to use payment methods belonging to another individual.
7. Unusual or unexplained customer behaviour, such as sudden changes inconsistent with known profile or expected activity.
8. Use of multiple or inconsistent deposit methods, or repeated failed deposit attempts indicative of possible funding manipulation.
9. High-risk occupations or associations with high-risk industries.
10. Adverse information identified through open sources, intelligence databases, or media linking the player to criminal activity, financial crime, or regulatory sanctions.
11. Concerns identified through financial vulnerability checks, particularly where affordability risk may coincide with ML/TF indicators.

When customers trigger any **Safer Gambling, Risk/Fraud**, or **AML/EDD** alerts, their records and associated documentation are reviewed to determine whether additional due diligence, enhanced monitoring, or other mitigating actions are required.

5.6 Reliance on third parties to perform customer due diligence.

The Company does not rely on any external third party to perform Customer Due Diligence (CDD) measures as set out in this Policy. All elements of CDD — including customer identification, verification, risk assessment, determination of PEP status, and ongoing monitoring — are conducted internally and remain the full responsibility of the Company.

The Company uses **Comply Radar**, an independent third-party tool, exclusively as a *technological solution* to support transaction monitoring activities. This use does not constitute

reliance on a third party for CDD within the meaning of the Curaçao AML/CFT Regulations. Comply Radar does not conduct identification or verification of customers, does not establish business relationships on behalf of the Company, and does not perform CDD measures. The Company maintains full responsibility for reviewing alerts, assessing customer risk, identifying unusual transactions, and determining whether reporting or additional actions are required.

Should the Company ever rely on a third party to perform any CDD elements, such reliance would only occur in accordance with Curaçao regulatory requirements and would involve:

- Obtaining required CDD information immediately from the third party;
- Ensuring the third party is subject to adequate CDD and recordkeeping regulations;
- Maintaining contractual arrangements enabling access to underlying documents;
- Performing independent customer risk assessments, PEP screening, and ongoing monitoring; and
- Retaining full responsibility for compliance with all AML/CFT obligations.

At present, the Company does not rely on any such third parties, and all CDD obligations remain under the Company's direct control.

5.7 Reporting of unusual transactions

5.7.1 Reporting of Unusual Transactions

The Company is required under the National Ordinance Reporting of Unusual Transactions (NORUT) to detect and report all unusual transactions, including both completed and intended transactions. Curaçao operates an Unusual Transaction Reporting (UTR) regime, meaning that reporting is based on objective indicators as well as any subjective concerns. Any unusual behaviour or transaction must be reported to the FIU Curaçao without delay. Following its analysis, if the FIU concludes that an unusual transaction gives rise to a suspicion of money laundering and/or terrorist financing, the FIU will forward the case to the Public Prosecutor's Office as a suspicious transaction.

5.7.2 Objective Indicators – Automatic Reporting Requirements

Under the Regulation Indicators Unusual Transactions, the following transactions are **automatically deemed unusual**, regardless of the customer's profile or whether the Company suspects ML/TF:

- **Any single transaction, or series/pattern of transactions, totalling NAf 5,000 (€2,400) or more per gaming day**, whether performed in cash, electronically, or through other non-

physical means.

This includes:

- cashless transfers to bank accounts;
- deposits or withdrawals of NAf 5,000 or more;
- purchases of chips, tokens, or credits of NAf 5,000 or more;
- cash-outs of NAf 5,000 or more.
- Transactions involving a person or entity listed under the Sanctions National Ordinance.
- Transactions reported to the Police or Department of Justice in connection with possible ML/TF.
- Transactions where there is reason to presume involvement in ML/TF (subjective indicator).

All transactions meeting these objective indicators must be escalated to the MLRO and reported to the FIU without delay, even if they appear routine or legitimate. Suspicion is *not* required.

5.7.3 Recognition of Unusual Transactions (Subjective Indicators)

In addition to automatic indicators, employees are able to identify transactions that:

- appear inconsistent with the customer's known profile,
- appear non-recreational;
- involve unusual patterns, complexity, or structuring, or
- otherwise raise concerns of potential ML/TF.

All staff receive annual AML/CFT training to ensure they can recognise such activity.

5.7.4 Internal Reporting (iSARs)

All employees are trained and required to internally report any unusual transaction or suspicious activity without delay. Internal Suspicious Activity Reports ("iSARs") are submitted to the designated **MLRO inbox** via email.

The MLRO team reviews each iSAR to determine whether the transaction or information meets the threshold for reporting to the Financial Intelligence Unit (FIU) Curaçao.

5.7.5 MLRO Review and Decision

The MLRO reviews each iSAR and determines whether it meets the criteria for external reporting under NORUT.

- If the transaction meets an **objective indicator** (e.g., NAf 5,000+), it *must* be reported to the FIU.
- If the transaction meets a **subjective indicator**, it is reported based on the MLRO's assessment.

5.7.6 External Reporting to the FIU

Where reporting is required, the MLRO prepares and submits the SAR through the **goAML portal without delay**, in accordance with FIU Curaçao requirements. All SARs are filed in English with full supporting documentation.

A SAR shall contain, insofar as possible, the following information:

- a. the identity of the client;
- b. the nature and number of the client's identification document;
- c. the nature, time, and place of the transaction;
- d. the value and the destination and origin of the funds, securities, precious metals, or other valuables involved in the transaction;
- e. the circumstances on the basis of which the transaction is considered unusual.

5.7.7 Documentation and Non-Submitted iSARs

All iSARs, regardless of outcome, are retained by the MLRO. Where an internally reported transaction does **not** result in a SAR to the FIU, the MLRO records the decision in a **central log** detailing the rationale for non-submission, along with any supporting evidence. Each non-submitted iSAR entry is reviewed and signed off by the MLRO.

5.7.8 Prohibition on Disclosure ("Tipping Off")

Employees, management, and all relevant personnel are strictly prohibited from disclosing to customers or third parties that an unusual transaction has been internally reported or externally filed with the FIU, or that an investigation may be underway. Any action taken (such as account restrictions) is carefully considered to avoid alerting the customer and compromising an investigation.

5.7.9 Record Keeping

All records relating to CDD, EDD, iSARs, SARs, supporting documentation, and transaction data are retained for at least five years, ensuring that all information is accessible for regulatory review and that transactions can be fully reconstructed if required.

5.8 Anti-Money Laundering Compliance program

The Company's Anti-Money Laundering (AML) Compliance Program forms a core component of its regulatory framework and is designed to protect the business from money laundering, terrorist financing, and related risks. The program is risk-based, aligned with Curaçao's legal and regulatory requirements, and establishes the internal policies, procedures, controls, and minimum standards necessary to ensure full compliance. It incorporates a designated Compliance Officer, robust screening and ongoing training for employees, and an independent audit function to test its effectiveness. The program covers customer due diligence, unusual transaction reporting, record-keeping, data protection, and ongoing monitoring, and is regularly reviewed and adapted to emerging risks. All elements of the AML program are approved by senior management and apply equally to any foreign branches or subsidiaries.

5.8.1 Risk Based Approach

In line with regulatory standards, the Company takes a risk-based approach to managing its money laundering, terrorist financing risks and proliferation financing. The company first identifies and documents the ML, TF & PF risks. This includes assessing the nature and extent of the risks to which it is exposed, considering factors such as customer types, geographic locations, and transaction types. Based on this assessment, the Company establishes and maintains proportionate policies, procedures, and controls to mitigate the identified risks. These measures are designed to allocate resources effectively and ensure that higher-risk areas receive greater attention. The Company continuously monitors the effectiveness of its mitigation measures, using a combination of ongoing oversight, periodic reviews, and risk assessments. Where necessary, the Company updates its policies, procedures, and controls to respond to new or emerging risks, ensuring a dynamic and responsive risk management framework.

5.8.2 Internal policies, procedures and controls.

The Company maintains a comprehensive system of internal policies, procedures and controls designed to prevent the misuse of its products and services for money laundering, terrorist financing, or proliferation financing. These policies reflect the Company's legal obligations under Curaçao AML/CFT/CFP legislation, including the National Ordinance on Identification of Services (NOIS), the National Ordinance on the Reporting of Unusual Transactions (NORUT), the Sanctions National Ordinance, and the Kingdom Sanctions Act.

The Company's AML procedures translate policy into practical operational steps covering customer due diligence, enhanced due diligence, source of funds collection, ongoing monitoring, unusual transaction reporting, record-keeping, and other core obligations. The

Compliance Officer is constantly checking and implementing regulatory changes to ensure the AML framework remains up to date.

Internal controls support these policies and procedures by enabling the employees and the Compliance Officer to identify unusual activity, monitor adherence to required standards, and address deviations promptly.

5.8.3 The AML/CFT Compliance Officer or MLRO

It is required for all licence holders to appoint an AML/CFT Compliance Officer. The holder of this position, in the company is Joaquin Paton.

The AML/CFT Compliance Officer/MLRO is responsible for ensuring this policy and any derived from it and relevant processes are compliant with the regulations. To ensure this the Compliance Officer, supported by the AML team, will conduct regular reviews of the regulations and best industry practices and where relevant, update the Policy and Processes. The Compliance Officer will also rely on Internal/ External Audit and Assurance QA checks to flag any non-compliances.

In addition to the above the Compliance Officer is responsible for:

- Designing and maintaining the AML/CFT program.
- Ensuring compliance with all applicable laws, regulations, and regulatory requirements.
- Monitoring adherence to the casino's internal AML/CFT policies and procedures.
- Organising staff training on compliance-related topics.
- Reviewing transactions to identify those requiring reporting under the Ministerial Decree on Indicators for Unusual Transactions.
- Assessing internally reported unusual transactions for completeness and accuracy.
- Maintaining records of all internally and externally reported unusual transactions.
- Establishing internal procedures on when unusual transaction reporting should lead to account blocking or freezing, while mitigating the risk of tipping off.
- Conducting enhanced reviews or investigations of unusual transactions when required.
- Preparing and submitting external reports of unusual transactions.
- Updating the AML/CFT program as necessary.
- Staying informed about local and international AML/CFT developments and advising management on improvements.
- Preparing periodic reports on the casino's AML/CFT and proliferation-financing prevention efforts.

5.8.4 Independent Audit function

The Company maintains an independent audit function, the Internal Audit team, to periodically test the effectiveness of its AML/CFT/PF Program. This review is conducted at least annually, and the Internal Audit team members are not involved in the Company's AML operations, ensuring full independence and objectivity.

The purpose of the audit function is to assess whether the Company's AML policies, procedures, and internal controls are adequate, effective, and operating as intended. As part of this process, the audit team will review customer files, assess compliance management, review samples of unusual transactions, evaluate the quality of staff training, and confirm that reporting, monitoring and record-keeping obligations are being met. The Internal Audit team may also interview relevant employees to verify that AML processes are understood and applied in practice.

The Compliance Officer also relies on Internal Audit checks to identify any instances of non-compliance. The audit function is responsible for providing recommendations for improvement and monitoring the Company's implementation of those recommendations to ensure they are addressed in a timely manner.

All audit findings are documented, and any deficiencies are reported to senior management (and the CXO where required), together with required corrective actions.

5.8.5 Employee Screening and Ongoing Training Program

The Company maintains a robust employee screening and training program to ensure that all staff conduct business to high ethical standards and comply with Curaçao's AML/CFT/CFP laws and regulations.

All employees are screened in accordance with the Employee Vetting Process to confirm their suitability for roles involving access to customer information, financial transactions, or sensitive systems. Enhanced vetting is conducted for staff appointed to key roles, including senior management, and for employees working within the AML and Enhanced Due Diligence (EDD) teams, given the higher level of risk and responsibility associated with these functions.

The Company provides ongoing AML/CFT training to all employees who interact with customer activity, financial transactions, user accounts, or internal controls. Training ensures that staff understand the Company's policies and procedures, the Ministerial Decree on Indicators for Unusual Transactions (N.G. 2015 no. 73), and their obligation to recognise and escalate unusual behaviour or transactions.

AML/CFT training is provided during onboarding and refresher training is delivered at least annually, and more frequently when required due to regulatory changes or emerging risks. The Company maintains complete records of all training activities, including:

- Training content and materials;
- Employees who received training;
- Dates of delivery;
- Assessment results where applicable;
- The Company's ongoing training plan.

6. COMPLIANCE AND CONSEQUENCES OF NON-COMPLIANCE

Breaches of this policy may result in disciplinary action (up to termination), regulatory sanctions, fines, licence conditions, or criminal liability.

7. RELATED INFORMATION

- Regulations for the combating of Money Laundering, the Financing of Terrorism and Proliferation of Weapons of Mass Destruction – Curaçao Gaming Control Board (January 2025)
- *National Money Laundering and Terrorist Financing Risk Assessment – Curaçao* - Government of Curaçao (2023)
- *AML/CFT/CFP National Strategy & Action Plan – Curaçao* - Government of Curaçao (2024)
- National Ordinance on Offshore Games of Hazard (PB 1993, no. 63, Landsverordening buitengaatsse hazardspelen, or LBH)
- NOIS - National Ordinance on Identification of Clients when rendering Services (Landsverordening identificatie bij dienstverlening (LID), N.G. 2017, no. 92)
- NORUT - National Ordinance on the Reporting of Unusual Transactions (Landsverordening melding ongebruikelijke transacties (LMOT), N.G. 2017, no. 93)
- 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);
- Sanctions National Ordinance (N.G. 2014, no. 55);
- Kingdom Sanction Act (N.G. 2016, no. 54);
- National Decree entering into force of Kingdom Sanction Law (N.G. 2017, no. 2);
- FATF Recommendations

8. CONTACT INFORMATION

For any questions regarding this policy, please contact:

9. POLICY HISTORY

Version	Changes	Updated By	Approved By	Date
0.1	Initial Draft	Joaquin Paton	Joaquin Paton	13/11/2025
1.0	Section 5.1 updated, including the addition of the AML/CFT Compliance Officer's name. The third-party PEP/SAN screening tool name (SEON) has been updated. The go-live date has also been revised.	MLRO	MLRO	07/04/2026
1.1	Section 5 updated to reflect the revised AML governance	MLRO	MLRO	23/06/2026

	reporting lines. Subheadings within Section 5 updated to align with the CGA template.			
--	---	--	--	--