

Strictly Confidential



This document is strictly confidential to its recipients and should not be copied, distributed or reproduced in whole or in part, nor passed to any third party

Panbet Curacao N.V.

AML/CFT/CFP Policy

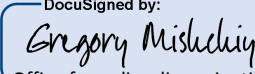
Strictly Confidential



This document is strictly confidential to its recipients and should not be copied, distributed or reproduced in whole or in part, nor passed to any third party

Key Information

Approving Official: Gregory Mishchiy

Signature: 

DocuSigned by: 

Responsible Office for policy dissemination, updates, and reviews: Compliance

Effective Date: 20/04/2026

Next Review Date: 01/04/2027

Contents

Key Information 2

1. Policy Statement 3

2. Purpose 3

3. Audience 3

4. Definitions 3

5. Policy Implementation 4

 5.1 Business Risk Assessment 4

 5.2 Customer Risk Assessment 5

 5.3 Customer Acceptance Policy..... 5

 5.3.1. Risk Categories and Due Diligence:..... 6

 5.4 Customer Due diligence 7

 5.5 Ongoing Monitoring..... 9

 5.6 Reliance on third parties to perform customer due diligence..... 9

 5.7 Reporting of unusual transactions 9

 5.8 Anti-Money Laundering Compliance Program 9

6. Compliance and Consequences of Non-Compliance 10

7. Related Information..... 10

8. Contact Information..... 11

9. Policy History 11

1. Policy Statement

Panbet Curacao N.V. is committed to the highest standards of compliance with anti-money laundering (AML), countering the financing of terrorism (CFT), and preventing the proliferation of weapons of mass destruction (CFP) regulations. We maintain a zero-tolerance approach to financial crime and are dedicated to implementing effective controls to detect, prevent, and report suspicious activities.

This policy applies to all business operations. It is designed to ensure compliance with the "Regulations for the combating of Money Laundering, the Financing of Terrorism and Proliferation of weapons of mass destruction" and all other relevant Curaçao laws and regulations.

2. Purpose

The purpose of this policy is to:

- Establish a comprehensive framework to prevent our services from being used for money laundering, terrorist financing, or proliferation financing
- Implement a risk-based approach to AML/CFT/CFP compliance, focusing resources on areas of highest risk
- Ensure compliance with Curaçao regulations and international standards
- Protect Panbet Curacao N.V.'s reputation and integrity in the global gaming sector

3. Audience

This policy applies to:

- All employees, regardless of position or tenure
- Members of the Board of Directors and Senior Management
- Contractors, agents and third-party service providers
- Any parties involved in the operation or management of licensed casino/gaming services under the Curaçao jurisdiction

4. Definitions

CGA: Curacao Gaming Authority

Money Laundering (ML): The process of making illegally-obtained funds appear legitimate

Financing of Terrorism (FT): The financing of terrorist acts, terrorists, and terrorist organizations. Unlike money laundering, funds may come from legitimate sources but are intended for illegal purposes.

Financing of Proliferation (FP): 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 related materials.

Simplified Due Diligence (SDD): Less intensive due diligence measures that may be applied to demonstrably lower-risk situations.

Strictly Confidential



This document is strictly confidential to its recipients and should not be copied, distributed or reproduced in whole or in part, nor passed to any third party

Customer Due Diligence (CDD): The process of identifying and verifying the identity of customers and understanding the nature of their activities to assess and mitigate risks.

Enhanced Due Diligence (EDD): Additional, more rigorous measures applied to higher-risk customers or transactions.

Politically Exposed Person (PEP): Individuals who are or have been entrusted with prominent public functions, their family members, and close associates.

Business Risk Assessment (BRA): The systematic evaluation of ML/TF/FP risks faced by business.

Customer Risk Assessment (CRA): The evaluation of ML/TF/FP risks associated with a particular customer.

Unusual Transaction Report (UTR): A report submitted to the Financial Intelligence Unit (FIU) regarding transactions that appear unusual or suspicious.

Financial Intelligence Unit (FIU): The government authority in Curaçao responsible for receiving, analysing, and disseminating financial intelligence.

5. Policy Implementation

5.1 Business Risk Assessment

Panbet Curacao N.V. applies a risk-based approach to the management of its' ML/TF/PF risk and has in place an assessment considering key risk factors such as:

- **Operator control risk** – the risks posed by vulnerabilities in controls of operator to ML/TF/PF threats
- **Employee risk** – the risks posed by the employees
- **Customer risk** – specific categories of customers and the resulting business relationships
- **Country or geographic risk** – the risks posed by geographical factors
- **Transaction risk (including means of payment)** – payment methods offered and the degree to which their specific characteristics are vulnerable to ML/TF/PF threats
- **Delivery channel risk** - the way in which services delivered
- **Product risk** – products offered and the degree to which their specific characteristics may be attractive for the purpose of ML/TF/PF

Each category poses varying degrees of risk.

The purpose of ML/TF/PF Risk Assessment is to identify areas where its products and services could be exposed to the risks of ML, TF and PF and taking appropriate steps to ensure that any identified risks are managed and mitigated through the establishment of appropriate and effective policies, procedures and controls. During the Risk Assessment, National Risk Assessment's (NRA) findings and CGA's guidance taken into consideration.

ML/TF/PF risk assessment is updated regularly in the light of any changes of circumstances:

- the introduction of new products or technology
- new methods of payment by customers
- changes in the customer demographic
- any other material changes

Strictly Confidential

This document is strictly confidential to its recipients and should not be copied, distributed or reproduced in whole or in part, nor passed to any third party

In any event, ML/TF/PF risk assessment is reviewed at least annually. As a result of the review, policies, procedures and controls are updated accordingly based on any changes to the ML/TF/PF risk assessment. Risk Assessment is approved by the Board of Directors.

5.2 Customer Risk Assessment

All clients are risk categorised. After the successful registration, the “Medium” risk assigned automatically. Further customer risk assessment is based on a set of measures, checks and investigations that are being performed on certain circumstances and accounts, upon which, according to the characteristics allocated at the end of review, the customer will be assigned with one of the below ML/TF/PF risk (this information is provided as for illustration purposes only and the list is not exhaustive; the risk also decreases or increases with the number of risk factors that are present):

Low Risk

- Low turnover customers (activity with small and/or rare bets on low-risk products)
- Individuals with verified identity and income, with no ML/TF/PF triggers
- Customers with consistent transaction patterns
- Customers with no negative indicators

Medium Risk

- Customers with moderate transaction volumes
- The customer with changing or unusual spending patterns
- The customer with suspicious patterns or ML/TF/PF ‘red-flags’, for example (including, but not limited to): attempts to withdraw their deposits without having placed bets; bets that are not in line with their deposits; bets at low prices etc.

High Risk

- The customers that are associated with higher risk countries
- The customer is a politically exposed person (PEP), or is a family member or close associate of a PEP
- Sanctioned individual
- The customer with negative findings (e.g. published police or criminal records) or customers who are close associates of confirmed criminals
- The customer has engaged in transactions that are complex, unusually large or have no apparent economic or legal purpose
- Panbet Curacao N.V. considers there to be an increased risk of ML/TF/PF associated with any customer account.

5.3 Customer Acceptance Policy

Our Customer Acceptance Policy (CAP) defines the types of customers we will and will not accept, based on risk assessment and our ability to manage those risks effectively. The CAP will be reviewed annually and updated to reflect changes in our risk assessments and regulatory requirements.

Establishing or maintaining business relationships with the following individuals is prohibited:

- 1) Legal entities
- 2) Natural persons, in the following cases:

Strictly Confidential



This document is strictly confidential to its recipients and should not be copied, distributed or reproduced in whole or in part, nor passed to any third party

- Minors
- Individuals who have voluntarily requested to be excluded from gaming activities
- Current or ex-employee who has worked, within the last 5 years, for Panbet Curacao N.V. and/or one of our associated companies and/or a supplier of our gambling equipment and/or services, and/or who is not otherwise acting on their own behalf
- Persons identified through Sanctions Lists
- Persons with history of fraud or ML/TF/PF
- Customers refusing to provide required information
- Customers engaged in prohibited activities under license

5.3.1. Risk Categories and Due Diligence:

Low-Risk Customers

- Low turnover customers (activity with small and/or rare bets on low-risk products)
- Individuals with verified identity and income, with no ML/TF/PF triggers
- Customers with consistent transaction patterns
- Customers with no negative indicators

CDD measures:

- Standard identification and verification
- Standard transaction monitoring
- Ongoing monitoring

Approval Process: Standard approval by onboarding staff

Medium-Risk Customers

- Customers with moderate transaction volumes
- The customer with changing or unusual spending patterns
- The customer with suspicious patterns or ML/TF/PF 'red-flags', for example (including, but not limited to): attempts to withdraw their deposits without having placed bets; bets that are not in line with their deposits; bets at low prices etc.

CDD measures:

- More comprehensive identification and verification might be applied
- Enhanced activity/transactions monitoring
- More frequent reviews, if necessary

Approval Process: Standard approval by onboarding staff with Anti-Fraud Leadership review when required

High-Risk Customers

- The customers that are associated with higher risk countries
- The customer is a politically exposed person (PEP), or is a family member or close associate of a PEP
- Sanctioned individual
- The customer with negative findings (e.g. published police or criminal records) or customers who are close associates of confirmed criminals

Strictly Confidential



This document is strictly confidential to its recipients and should not be copied, distributed or reproduced in whole or in part, nor passed to any third party

- The customer has engaged in transactions that are complex, unusually large or have no apparent economic or legal purpose
- Panbet Curacao N.V. considers there to be an increased risk of ML/TF/PF associated with any customer account.

The following CDD measures might be applied (depending on the risks):

- Additional identification documents or information
- Senior Management approval
- More frequent and intensive monitoring
- Lower thresholds for transaction scrutiny
- More frequent relationship reviews
- Verification of source of wealth and funds

Approval Process: Anti-Fraud Leadership, Compliance Officer, MLRO review. Senior Management approval might be also required.

5.4 Customer Due diligence

Anonymous accounts and accounts in obviously fictitious names are prohibited. The following information collected during the registration:

- full name
- permanent residential address
- date of birth

In high-risk situations, additional personal details can be collected to mitigate the higher risk of ML/FT/PF.

Panbet Curacao N.V. does not apply simplified due diligence due to the increased risk posed by non-face-to-face relationships.

Customer Due Diligence measures undertaken when:

- players engage in financial transactions $\geq$ NAf. 4,000
- carrying out occasional transactions $\geq$ NAf. 4,000
- suspecting money laundering or terrorist financing
- doubting the veracity of previously obtained information

Acceptable documents for identity verification (unexpired government-issued document containing photographic evidence of the customer's identity), for example:

- Travel document or passport
- Driver's license
- Identification card

A photo of the customer holding the Photo ID document next to their face may also be required.

For verification of residential address (if an identity document does not allow to verify it), not to be more than six months:

- Bank statement

Strictly Confidential



This document is strictly confidential to its recipients and should not be copied, distributed or reproduced in whole or in part, nor passed to any third party

- Utility bill (for phone bills, only fixed line telephone bills are accepted as proof of address)
- Correspondence from a central or local government authority, department or agency
- A rental or lease agreement

Documents should be authentic, clear, legible and of good quality.

If CDD cannot be completed satisfactorily, Panbet Curacao N.V. will not enter into a business relationship/terminate relationship with that customer. Panbet Curacao N.V. will consider filing an unusual transaction report and, when possible, return funds through the original payment method.

Sanctions

During the registration process customers are screened against Curaçao designated persons lists, HM Treasury, OFAC, EU and UN sanctions lists using a third-party screening tool. Sanctions screening is also performed:

- due to the changes in the sanctions list(s)
- on monthly basis (an automatically generated report sent out for manual review)
- during enhanced due diligence checks

A potential match creates an alert which must be investigated by an analyst to determine whether the customer is a true match with the person on the sanctions list. Potential positive matches are escalated to the MLRO.

If the individual is determined to be a positive match, the account will be frozen according to the 'Process for freezing resources' and reported to the FIU.

Politically Exposed Persons

A Politically Exposed Person (PEP) is an individual who is or has been entrusted with a prominent public function. The nature of the position and access to public funds may present a higher risk of money laundering, corruption or bribery. An individual who is closely related to such a person is also considered to be high risk.

Foreign PEPs are individuals who are or have been entrusted with prominent public functions by a foreign country. Domestic PEPs are individuals who are or have been entrusted domestically with prominent public functions.

Foreign PEPs are 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.

Domestic PEPs are individuals who are or have been entrusted domestically with prominent public functions, for example Heads of State or of government, senior politicians, senior government, judicial or military officials, senior executives of state owned corporations, important political party officials.

Persons who are or have been entrusted with a prominent function by an international organisation refers to members of senior management, i.e. directors, deputy directors and members of the board or equivalent functions.

Strictly Confidential



This document is strictly confidential to its recipients and should not be copied, distributed or reproduced in whole or in part, nor passed to any third party

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

Where screening identifies that a customer may be a potential PEP the customer is subject to EDD and is escalated to the MLRO for further investigation. Confirmed true matches are subject to approval by the Panbet Curacao N.V.'s Senior Management. If business approval is granted, PEP accounts will be subject to enhanced ongoing monitoring. Reasonable measures are also taken to establish the source of wealth and source of funds that are involved in business relationships or transactions with such persons.

5.5 Ongoing Monitoring

Customer betting and transactional activities are subject to manual and system monitoring. When certain conditions are met, further analysis must be undertaken by the Customer Analysis & Anti-Fraud (behaviour and gambling activity), Trading (betting activity), Products (casino and products activity) and Payments teams (transactional activity).

Irrespective of the reason for the alert, the analyst must perform a review of the account and activities to determine whether there are suspicious patterns or 'red-flags' present. If the reviewed activity is considered suspicious, the analyst must escalate the details to the MLRO.

5.6 Reliance on third parties to perform customer due diligence.

We may rely on qualified third parties to perform sanctions screening and PEP identification, while maintaining ultimate responsibility for compliance.

5.7 Reporting of unusual transactions

If staff knows or suspects, or have reasonable grounds for knowing or suspecting, that a person is engaged in money laundering, terrorist financing or proliferation financing, including criminal spend, or attempting to launder money or finance terrorism, an internal report must be submitted to the Money Laundering Reporting Officer or to the Deputy Money Laundering Reporting Officer immediately.

The Money Laundering Reporting Officer (MLRO) is the designated officer responsible for receiving internal reports of suspicious activity. The MLRO reviews these disclosures and assesses whether there are sufficient grounds to escalate the matter to the Financial Intelligence Unit (FIU). If a report to the FIU Curaçao is warranted, it is submitted via the goAML portal without delay.

Prohibition of Disclosure (Tipping Off):

We strictly prohibit disclosing to any person:

- That an unusual transaction report has been filed
- That an investigation is being conducted
- Any information that could prejudice an investigation

5.8 Anti-Money Laundering Compliance Program

Panbet Curacao N.V. maintains a AML/CFT/CFP program, including:

- Written policies and procedures reflecting current laws/regulations
- Appointment of an independent Compliance Officer
- Comprehensive employee screening, onboarding and regular AML/CFT/CFP training
- Updating controls in response to regulatory or business change
- Procedures for blocking/freezing accounts on suspicion and reporting to authorities

Strictly Confidential



This document is strictly confidential to its recipients and should not be copied, distributed or reproduced in whole or in part, nor passed to any third party

- Independent audit of the AML/CFT/CFP program at least annually
- Data retention of all CDD, transactional and report records for at least five years

6. Compliance and Consequences of Non-Compliance

Regulatory Consequences:

Failure to comply with AML/CFT/CFP regulations may result in:

- Administrative sanctions against the company
- Criminal prosecution
- Substantial monetary penalties
- License suspension or revocation
- Reputational damage

Internal Consequences:

Employees who violate this policy might face:

- Disciplinary action up to and including termination
- Potential personal civil or criminal liability

Particularly Serious Violations:

The following violations are considered especially serious:

- Deliberately failing to report unusual transactions
- Tipping off customers about investigations
- Falsifying records or information
- Assisting customers in evading AML requirements

7. Related Information

This policy should be read in conjunction with:

Laws and Regulations:

- National Ordinance on Offshore Games (NOOGH, PB 1993, no. 63)
- National Ordinance on Games of Chance (NOGC; PB 2024, no. 157, "LOK");
- National Ordinance on Identification when rendering Services (NOIS; N.G. 2017 no. 92)
- National Ordinance on the Reporting Unusual Transactions (NORUT; N.G. 2017 no. 99)
- Sanctions National Ordinance (N.G. 2014, no. 55)
- Kingdom Sanction Act (N.G. 2016, no. 54)
- Regulation Indicators Unusual Transactions (N.G. 2015, no. 73)
- The Code of Criminal Law (Penal Code) (N.G. 2011, no. 48)

External Resources:

- [Curaçao Gaming Authority's AML/CFT/CFP Guidelines](#)

Strictly Confidential



This document is strictly confidential to its recipients and should not be copied, distributed or reproduced in whole or in part, nor passed to any third party

- [FIU Curaçao Reporting Guidelines](#)
- [FATF 40 Recommendations](#)
- [FATF Guidance for a Risk-Based Approach for Casinos](#)
- [FATF Vulnerabilities of Casinos and Gaming Sector](#)

8. Contact Information

For any questions regarding this policy, please contact:

Aleksandr Toptsilin

Panserve Limited, Runway East, Brighton, York And Elder Works, 50 New England Street, Brighton, BN1 4AW

Email: aml@mbet.com

Phone: +44 1273 964700

9. Policy History

Version	Author	Description of Changes	Date	Approved by
1.0	Aleksandr Toptsilin / MLRO	Creation of the new policy, as per the CGA requirements	20/05/2025	Gregory Mishchiy / Director
1.1	Aleksandr Toptsilin / MLRO	Annual review	17/04/2026	Gregory Mishchiy / Director