

AML policy

(last update 16.04.2025)

Definitions

AML / Compliance Department - The unit which has primary responsibility for the initiation and delivery aspects of the AML program within an Organisation.

Business relationship - Business or commercial relationship between a Customer and the Organisation and which is expected, at the time when the contact is established, to have an element of duration for a certain period (e.g. conclusion of an agreement between the Customer and the Organisation, continuous performance of gambling/betting and monetary operations and transactions).

Close Associate - A natural person who, together with the Politically Exposed Person, is a member of the same legal entity or of a body without legal personality or maintains other business relationship.

Close family member - The spouse, the person with whom partnership has been registered (i.e. the cohabitant), parents, brothers, sisters, children and children's spouses, children's cohabitants.

Customer due diligence (CDD) - Identification of the Customer and verification the Customer's identity on the basis of documents, data or information obtained from a reliable and independent source; assessment and, as appropriate, obtainment of information on the purpose and intended nature of the Business Relationship; the conducting of ongoing monitoring of the Business Relationship including scrutiny of transactions undertaken throughout the course of that relationship to ensure that the transactions being conducted are consistent with the Organisations' knowledge of the Customer.

Customer/Client/Player - a person that uses online gambling and betting services provided by the Organisation.

FATF – The Financial Action Task Force.

FIU – Financial Investigation Unit Curacao.

High-risk third countries - countries identified as having strategic deficiencies in their AML/CFT regime, which pose a significant threat to the Union's financial system (Article 9 of Directive (EU) 2015/849).

Identification - A part of Customer Due Diligence, allowing to ascertain the identity of a person on the basis of the personalised unique information directly related to that person.

Law – applicable Anti-Money laundering legislation.

Money laundering (ML) - the doing of any act which constitutes an offence of money laundering and is defined in the Law on the Prevention of Money Laundering and Terrorist Financing of Curacao. The criminal acts cover all procedures that seek to change the identity

of illegally obtained funds, arising from drug dealing, terrorist activities or any other crime in order to give impression that such money originated from legitimate or legal sources. Money laundering is the participation in any transaction that seeks to conceal or disguise the nature or origin of funds

Organisation – Promotech N.V., an online gambling institution established and authorized under the laws of Curacao (license number OGL/2024/611/0233 issued by CGA) and, therefore, falling within the definition of an institution that falls under the Curacao legislation on the Prevention of Money Laundering and Terrorist Financing, as well as respective regulations issued by CGA. The term "Company / Organisation" when used in these Policies also refers to the management bodies of the Organisation and the members of such bodies as well as the employees of the Organisation.

Policy – AML/CFT and Sanctions Compliance Policy.

Politically Exposed Person (PEP) - Natural persons who are or have been entrusted with Prominent Public Functions and Close Family Members or Close Associates of such persons.

Prominent Public Functions:

1. The head of the state, the head of the government, a minister, a vice minister or a deputy minister,
a secretary of the state, a chancellor of the parliament, government or a ministry;
2. A member of the parliament;
3. A member of the Supreme Court, the Constitutional Court or any other supreme judicial authorities whose decisions are not subject to appeal;
4. A mayor of the municipality, a head of the municipal administration;
5. A member of the management body of the supreme institution of state audit or control, or a chair, deputy chair or a member of the board of the central bank;
6. Ambassadors of foreign states, a charge d'affaires ad interim, commander of the armed forces and units, chief of defence staff or senior officer of foreign armed forces;
A member of the management or supervisory body of a public undertaking, a public limited company or a private limited company, whose shares or part of shares, carrying more than 1/2 of the total votes at the general meeting of shareholders of such companies, are owned by the state;
8. A member of the management or supervisory body of a municipal undertaking, a public limited company or a private limited company whose shares or part of shares, carrying more than 1/2 of the total votes at the general meeting of shareholders of such companies, that are owned by the state, and which are considered as large enterprises
9. A director, a deputy director or a member of the management or supervisory body of an international intergovernmental organisation;

10. A leader, a deputy leader or a member of the management body of a political party.

Source of funds – means the origin of the funds involved in a business relationship or occasional transaction. It includes both the activity that generated the funds used in the business relationship, for example the customer's salary, as well as the means through which the customer's funds were transferred.

Source of wealth – refers to funds that the customer has acquired during a prolonged period of time and that make up the customer's entire body of wealth (total funds). When determining the source of wealth, the main focus is the acquisition of information on customer's activities that indicate how the customer acquired the wealth.

Terrorist financing (TF) - the solicitation, collection or provision of funds with the intention that they may be used to support terrorist acts or organizations. Funds may stem from both legal and illicit sources. More precisely, according to the International Convention for the Suppression of the Financing of Terrorism, a person commits the crime of financing of terrorism "if that person by any means, directly or indirectly, unlawfully and wilfully, provides or collects funds with the intention that they should be used or in the knowledge that they are to be used, in full or in part, in order to carry out" an offense.

CGA – mean Curacao Gaming Authority who issued a respective license for Organisation.

1. Scope Of The Policy

1.1 This Anti-Money Laundering Policy (hereinafter referred to as the "Policy") establishes the framework through which Promotech N.V. addresses the prevention of money laundering, terrorist financing, and any other unlawful or fraudulent activities. It defines the standards, responsibilities, and internal procedures adopted by the Company in line with applicable AML and counter-terrorism financing laws and regulations.

1.2 By accessing or using <http://fortunica.casino/> (hereinafter the "Website"), all users (the "Users") confirm their understanding and acceptance of this Policy, including any future updates. The Company retains the right to revise this Policy at any time, in accordance with changes in legislation, internal risk evaluations, or procedural improvements. Any significant amendments will be communicated to Users, and continued use of the Website following such notification shall be considered as acceptance of the revised Policy.

1.3 Money laundering is defined as the process of concealing the illicit origin of funds obtained through criminal activities. This may involve proceeds from drug trafficking, fraud, corruption, organized crime, terrorism, and other offenses. The money laundering process is generally broken down into three stages:

- **Placement** – the introduction of illicit funds into the financial system, typically through deposits, purchases, or other transactions;

- **Layering** – the separation of those funds from their criminal source by moving them through a series of complex financial transactions, designed to obscure the audit trail and enhance anonymity;
 - **Integration** – the reinsertion of laundered funds into the economy so that they appear legitimate and can be used freely.
- 1.1. Terrorist financing refers to the methods by which terrorist individuals or organizations acquire, move, and use funds to support their activities. These funds can originate from lawful sources, such as personal donations or profits from legitimate businesses, as well as from unlawful sources, including trafficking, extortion, or kidnapping.
 - 1.2. This Policy is developed and regularly reviewed by the appointed Compliance Officer of the Company, in line with the general framework established by the Board of Directors to ensure full adherence to applicable anti-money laundering and counter-terrorism financing laws and regulations.

2. Responsibilities and recipients of the policy

- 2.1. This policy applies to all employees, subcontractors, and third-party service providers of the Company who are involved in initiating, managing, or reviewing business relationships.
- 2.2. Any identified breach of this policy must be reported immediately to the head of the relevant department. If any inconsistencies are discovered between the actual procedures and those outlined in this document, the responsible process owner must be notified without delay.
- 2.3. In order to ensure strict adherence to applicable anti-money laundering and counter-terrorism financing laws, as well as internal procedures:
 - All employees, subcontractors, and third-party vendors working with Promotech N.V. are required to comply with this AML policy and all relevant legislation and regulatory requirements related to AML, CFT, and sanctions.
 - Contracts with external partners must include clear clauses related to AML/CFT compliance, including duties to identify, prevent, and report any suspicious activity.
 - Third parties must undergo appropriate risk assessment and due diligence before any business engagement begins.
 - Where necessary, the Company will provide training or informational resources to third-party personnel to ensure awareness of anti-money laundering responsibilities.
 - Promotech N.V. reserves the right to audit, assess, and monitor the AML compliance practices of third parties and may suspend or terminate any agreement in cases of

non-compliance.

3. AML annual report

- 3.1. The AML/CFT Compliance Officer prepares an annual report to evaluate the Company's compliance with applicable anti-money laundering and counter-terrorist financing laws. This report must be submitted to the Director no later than two months after the end of each calendar year and provided to the regulator upon request.
- 3.2. The report must include:
 - Updates on implemented measures to comply with changes in AML/CFT legislation.
 - Results of internal inspections, including any deficiencies in AML/CFT policies or controls, related risks, and corrective actions taken.
 - Number of internal suspicious activity reports and any relevant observations.
 - Number of reports submitted to authorities and main reasons for suspicion.
 - Information on communication with staff regarding AML/CFT awareness.
 - Data on high-risk clients, including numbers and countries of origin.
 - Overview of transaction and client monitoring practices.
 - Summary of AML/CFT training completed by the Compliance Officer and staff, including types of training, number of participants, and whether training was internal or external.
 - Assessment of training effectiveness and next year's training plan.
 - Recommendations regarding staffing or resources for the AML/CFT function.
- 3.3. Upon request, the Company shall provide:
 - Business Risk Assessment records.
 - Name and job description of the Compliance Officer.
 - Logs of suspicious and unusual transactions.
 - Records of frozen accounts and related actions.
 - Training schedules and materials.
 - Internal/external audit results on AML/CFT controls.
 - Customer files, including risk assessments, due diligence, and transaction data.

4. Mandatory risk procedures and the risk-based approach

- 4.1. The Company applies a risk-based approach (RBA) to ensure that resources are focused on customers and activities that pose the highest risk of money laundering

and terrorist financing (ML/FT). Measures taken must be proportionate to the level of risk identified.

- 4.2. This Policy establishes the framework for applying the RBA. The AML/CFT Compliance Officer is responsible for developing, implementing, and continuously monitoring procedures and controls based on this approach. These measures are updated as risks or regulatory requirements evolve.
- 4.3. The Director is responsible for reviewing, at least annually, the effective implementation of the risk-based approach.
- 4.4. Risk assessments must take into account factors such as:
 - Type of customer
 - Jurisdiction of customer or transaction
 - Type of product or service
 - Nature of transactions
 - Distribution channels used
- 4.5. As part of its risk-based approach, the Company identifies, records, and evaluates potential money laundering and terrorist financing (ML/TF) risks. Since the Company's online gaming and betting services are typically delivered in a standardized manner to a limited and similar client base, enhanced attention is given to customers who fall outside typical patterns.
- 4.6. Key risk factors considered in client ML/TF risk categorization include:
 - Clients identified as politically exposed persons (PEPs);
 - Clients conducting high-value transactions;
 - Clients from high-risk jurisdictions or countries associated with corruption, organized crime, or drug trafficking;
 - Clients unwilling to provide required identification or documentation;
 - Clients using VPNs or proxy servers to mask their IP address;
 - Clients accessing the platform through multiple or unusual devices.
- 4.7. Client Risk Profiling
The Company conducts an initial risk assessment based on identified risk factors. However, a full risk profile often becomes clearer once the client has completed the Customer Due Diligence (CDD) process and begun transacting.
- 4.8. Given the nature of the Company's online gaming services and the non-face-to-face onboarding of most clients, each customer will be assigned a risk category - Low, Medium, or High-based on the following factors:
 - Results of the CDD process
 - Transaction behavior and volume

- Geographic origin
- Client's willingness to provide information
- Use of anonymity tools or unusual access methods

5. Indicators related to the Client

5.1. High ML/TF PEPs Risk:

- Clients from countries that are selectively sanctioned resident or origin in/from non-reputable jurisdiction according to the FATF list as amended from time to time
- High Deposits
- Any other Client determined by the Company itself to be classified as such Or any unverified client
- Any of the above-mentioned indicators will automatically classify the account as High Risk

5.2. Medium ML/TF Risk

Client that holds all of the below indicators:

- Verified client
- Client that does not fall under any of the categories of High Risk or Low Risk
- Any other Client determined by the Company itself to be classified as such

5.3. Low ML/TF Risk

Client that holds all of the below indicators:

- Resident and origin of an EEA jurisdiction
- Very low deposits
- The country of origin and/or destination of Clients' funds are both EEA jurisdiction
- Client using only debit/credit card or wire transfer
- Clients identified Face-To-Face
- Any Client who does not fall under the 'Medium Risk' or 'High Risk' categories

6. Client Acceptance

6.1. The Company classifies Clients into three risk categories based on the Risk-Based Approach.

- Accounts become fully operational only after completing CDD in line with this Policy.
- Opening or maintaining anonymous, fictitious, or numbered accounts, or accounts in names other than those on official ID, is strictly prohibited.

- CDD approval by the AML/CFT Compliance Officer is required before activation.
- 6.2. Acceptance Criteria
- Only Low-Risk Clients who have successfully passed CDD and meet Policy requirements may be accepted.
- 6.3. The Company will not accept Clients who:
- Refuse or fail to provide required identification data without valid reason.
 - Request anonymous, fictitious, or numbered accounts.
 - Request initial deposit transfers in cash.
 - Are legal entities.
 - Open accounts in the name of a third party.
 - Submit suspicious or faulty documents.
 - Originate from non-cooperative jurisdictions
 - The client has negative information/reports on him or is under investigation.
 - The client is on the list of people involved in terrorist financing or known to be involved in activity connected to money-laundering.
 - Sanctioned individuals.

7. Risk management and monitoring

- 7.1. Risk assessment is an ongoing, dynamic process rather than a one-time action. Client behavior and transaction patterns evolve over time, as do methods of money laundering and terrorist financing.
- 7.2. The AML/CFT Compliance Officer must regularly review existing and new client profiles, along with the effectiveness of current measures, procedures, and controls. These reviews must be documented and included in the Annual Money Laundering Report.
- 7.3. When applying the Risk-Based Approach and CDD procedures, the AML/CFT Compliance Officer and Client Support Department should use data and reports from reputable international sources, such as:
- FATF
 - Council of Europe's AML Evaluation Committee
 - EU Common Foreign & Security Policy (CFSP)
 - UN Security Council Sanctions Committees
 - International Money Laundering Information Network (IMOLIN)
 - International Monetary Fund (IMF)
 - Office of Foreign Assets Control (OFAC)

7.4. The Company also maintains a list of countries prohibited from using its services due to gambling and betting regulations.

In addition, industry-specific fraud prevention and monitoring measures are applied, including:

- Access from multiple devices
- Frequency and pattern of deposits
- Choice and sudden changes in payment methods
- Attempts to use cards failing 3D secure verification
- Transactions with insufficient funds
- Use of multiple bank cards
- Withdrawals through unverified payment methods

These indicators may lead to a reassessment of the client's risk level, filing a suspicious activity report, or account closure.

8. Sanctions compliance policy

8.1. Compliance with applicable sanctions regulations is essential to:

- Avoid administrative or regulatory action against the Company
- Protect the Company's reputation

8.2. Authorities issuing sanctions programs

- OFAC (USA)
- European Union
- United Nations

9. Sanctions risk assessment

9.1. The Company conducts and documents sanctions risk assessments to identify, measure, and manage sanctions risks, taking into account:

- Regions where the Company operates and provides services
- Services and products offered
- Customer risk profile
- Country/geographical risk
- Risks linked to provided services and delivery channels

9.2. All sanctions risk assessments are approved by the Director.

9.3. Internal controls: based on the risk assessment, the Company establishes internal controls for sanctions risk management.

9.4. Indicators of elevated sanctions risk

- Customer or transactions linked to sanctioned territories or border areas

- Involvement in military industries or trade in dual-use goods
 - Activities inconsistent with declared purpose
 - Reuse of the same documents for unrelated transactions
 - Documents containing signs of fraud or sanctions evasion
- 9.5. The Company applies KYC and due diligence procedures to screen all new and existing customers against sanctions lists during onboarding and throughout the business relationship. Matches trigger alerts for further review by the AML Compliance Officer.
- 9.6. The Company screens all transaction parties, including customers and payment institutions against sanctions lists. Matches generate alerts for AML Compliance Officer investigation.
- 9.7. Freezing and unfreezing accounts
Where required by law, the Company freezes accounts and assets of parties subject to sanctions or pending review for potential violations.
- 9.8. Freezing applies under:
- Curaçao and EU laws;
 - U.S. laws where U.S. jurisdiction applies.
- 9.9. Accounts may be unfrozen only upon:
- (a) authorisation from the relevant jurisdiction, or
 - (b) official removal of the sanctions.
- 9.10. The Company will not engage in transactions with sanctioned parties unless expressly permitted under the relevant sanctions and confirmed in advance by the AML Compliance Officer.

10. Client Due Diligence, Identification and Verification Procedures

- 10.1. The Company applies Client identification and CDD measures in the following cases:
- When establishing a Business Relationship.
 - When there is suspicion of ML/TF, regardless of transaction amount.
 - When there are doubts about previous Client identification data.
 - When significant amounts are deposited.
 - For transactions equal to or above EUR 2000.
 - In any case deemed necessary by the AML/CFT Compliance Officer.
- 10.2. Responsibilities:
- The AML/CFT Compliance Officer ensures correct application of all CDD procedures and reviews them at least annually.

- Customer Support collects and files Client identification documents per record-keeping rules.
 - The Compliance Officer maintains and updates requirements for Client documentation in line with the Law.
- 10.3. Before starting a Business Relationship, the Company must:
1. Identify and verify the Client within the allowed time limit.
 2. Determine the purpose and intended nature of the Business Relationship.
 3. Assess ML/TF risk and assign the Client to a risk category.
 4. Apply appropriate CDD or EDD measures.
 5. Screen relevant persons against sanctions lists.
- 10.4. If CDD cannot be completed, including inability to:
- Verify identity from reliable and independent sources.
 - Confirm the Client acts on their own behalf.
 - Obtain information on the Business Relationship's purpose.
 - Conduct ongoing monitoring.
- 10.5. The Company will refuse or terminate the Business Relationship and, if required by legislation, report the case to the FIU Curaçao.

11. Customer identification

- 11.1. The initial identification of the Customer is performed through the review of the initial registration of the players' account.
- 11.2. The registration collects the following information:
- Account number (generated automatically)
 - Password
 - Registration Date (generated automatically)
 - Security Question
 - Answer to Security Question (double input required)
 - Phone number (must be verified)
 - Email Address (must be verified)
 - Surname
 - First Name
 - Date of Birth
 - Type of Document
 - Document Number
 - Document Issue Date
 - Country
 - Permanent Registered Address

- Nationality
- Identity number

The following data allows the AML Officer to perform their initial screening on the potential client.

11.3. Verification of documents

When verifying the identity of the natural person the AML responsible employee must:

- review the documents provided for verification of the customer to ensure that no fraud signs have been noticed;
- ensure that document provided for identity verification is valid and contains the person's photograph;
- the Responsible employee must verify the data, documents, and information received from the Customer during the CDD using the documents, data or information obtained from a reliable and independent source.

12. KYC and customer due diligence procedures (CDD)

12.1. Identification of persons

The true identity of a natural person must be verified by collecting and recording the following information:

- **Full legal name** and any other names used, as stated on:
 - o A valid official identity card (front and back) or valid passport
- **Full permanent residential address**, including postal code.
- **Telephone number** (preferably landline, if available).
- **E-mail address**.
- **Date and place of birth**.
- **Specimen signature** (taken from the official identification document).
- **PEP status**: Information on whether the customer currently holds, has held within the last 12 months, or has previously held a public position, or is an immediate family member or close associate of a person in such a position. This should be verified independently through screening databases.

12.2. Verification of residential address

The customer's declared residential address must be verified through one of the following documents, issued within the last three (3) months:

- Utility bill (electricity, water, gas, waste) showing consumption of the service.
- Municipal tax bill.
- Bank statement from a reputable financial institution.

- Telephone bill (landline only) or internet bill (if linked to a landline connection).

Utility bills must be reviewed for evidence of service consumption to confirm that the declared address is the customer's actual residence.

12.3. Documentation Standards

12.3.1 Only original documents or certified true copies should be accepted (no online statements).

12.3.2 Copies of documents must clearly show:

- Document number.
- Issuing and expiry dates.
- Country of issuance.
- Date of birth.
- Clear photograph.
- Signature of the document holder.

All documents and proof of address must be stored in the customer's file in accordance with record-keeping requirements.

13. Enhanced Diligence Measures (EDD)

13.1. The Company must apply additional and enhanced measures in situations that inherently carry a higher risk of money laundering and terrorist financing.

13.2. Besides the player accounts that the Company classifies as High-Risk through its risk assessment, the applicable laws also identify the following customer categories as high-risk, where enhanced due diligence (EDD) is required:

- Complex, unusually large, or atypical transactions
- Accounts held by Politically Exposed Persons (PEPs)
- Transactions involving natural persons or legal entities established in high-risk third countries

13.3. The minimum enhanced due diligence measures that should be applied for all High-Risk customers of the Company are:

- Perform review and update of records of the customer at least once a year or at a shorter interval if necessary
- Taking more enhanced measures and supporting documentation to establish and verify the source of wealth
- Perform systematic and thorough monitoring of the transactional behaviour.
- Obtaining additional information on the customer, like occupation, previous address and information available through public databases, internet, etc.;

- Obtaining additional information on the intended nature of the business relationship;
 - Obtaining information on the source of funds or source of wealth of the player. Examples of source of funds include personal savings, employment, pension releases, share sales and dividends, property sales, gambling winnings, inheritances and gifts and compensation from legal rulings;
 - Obtaining information on the reasons for intended or performed transactions;
 - Obtaining the approval of senior management to commence or continue the business relationship;
 - Conducting enhanced monitoring of the business relationship;
 - Requiring the first payment to be carried out through an account in the customer's name with a bank subject to similar CDD standards.
- 13.4. The Company is required, to the extent reasonably possible, to investigate the background and purpose of all complex, unusually large, or atypical transactions that lack an obvious or legitimate purpose.
- 13.5. To better assess whether such transactions or activities are suspicious, the Company should classify the client(s) involved in these complex or unusual transactions as high-risk. This classification allows for enhanced monitoring and closer scrutiny of the business relationship.
- 13.5.1. Such enhanced due diligence measures include, but are not limited to:
- 1) Applying reasonable and adequate steps to understand the background and purpose of these transactions, for example by verifying the source of funds through bank statements, payslips, or other relevant documents, or by obtaining additional information about the customer to assess the plausibility of the transaction;
 - 2) Intensifying the monitoring of the specific transactions and the customer's overall transactional history;
 - 3) Conducting ongoing monitoring of the business relationship at least annually, or more frequently if required, as outlined for High-Risk customers in this procedure;
 - 4) Evaluating whether the customer should remain classified as High Risk or if further actions are necessary.

The specific enhanced due diligence measures applied to each customer will depend on the individual circumstances and the factors that made the transaction complex or unusual.

14. Politically Exposed Persons (PEPs)

14.1. Additional screening for PEPs

In addition to the information provided by the customer, independent searches must be conducted using dedicated compliance software and open-source internet checks to determine:

- Public positions currently or previously held by the customer (at least for the last 12 months).

14.2. Whether the customer is an immediate family member or close associate of a PEP.

14.3. For the purposes of identifying a PEP, "prominent public function" includes, but is not limited to, the following roles:

- Head of State, Head of Government, Minister, Deputy or Assistant Minister
- Member of Parliament or similar legislative body
- Member of a governing body of a political party
- Member of the Supreme Court, Constitutional Court, or other high-level judicial body whose decisions are generally final
- Member of a court of auditors or board member of Central Banks
- Ambassador, Chargé d'affaires, and senior officers of the armed or security forces
- Member of the administrative, management, or supervisory body of state-owned enterprises
- Director, Deputy Director, Director General of a Ministry, or board member (or equivalent) of an international organization
- Mayor
- Middle-ranking or junior officials are excluded from this definition.

14.4. Family members and close associates

- Family members include the spouse (or equivalent), children and their spouses (or equivalents), and parents of the PEP.
- Close associates refer to natural persons known to share beneficial ownership of a legal entity or arrangement set up for the benefit of a PEP, or who maintain close business relationships with the PEP.

14.5. Post-term PEP status

If a PEP ceases to hold a prominent public function, the Company continues to treat the individual as High-Risk for at least 12 months following their departure. The Company assesses each case individually and may maintain the PEP classification beyond this period if deemed necessary, including for the full duration of the business relationship.

14.6. PEP identification and classification

To determine whether a prospective customer is a PEP, the Company assesses multiple information sources:

- Information provided directly by the individual;
- Screening databases (recognizing that classification by such databases is not definitive);
- Internet searches;
- Other reliable publicly available information.

Evidence from these sources must be documented and kept in the customer's file. The Company periodically reviews and updates the PEP classification as necessary.

14.7. Enhanced Due Diligence for PEPs

Upon identifying a PEP, the following enhanced due diligence measures apply:

- Approval to establish or continue the business relationship with a PEP must be granted by the Board of Directors, supported by a brief report prepared by the responsible employee outlining the customer's and PEP's profiles.
- Before onboarding a PEP, the Company must gather sufficient information to verify the PEP's identity, business reputation, integrity, and professionalism, potentially including third-party references or internet searches.
- The Company must establish and verify the source of wealth and funds of the PEP to ensure no corruption or criminal proceeds are involved. Verification may involve checking publicly available information such as asset disclosures, property and company registers, and internet/social media sources.
- The expected business activity profile of the PEP should guide ongoing monitoring and be regularly reviewed and updated, with particular vigilance applied to sectors vulnerable to corruption.

All documentation and information collected should be maintained in the customer's file.

14.8. Ongoing Monitoring of PEP business relationships

Business relationships with PEPs require enhanced and continuous monitoring:

- Reviews must occur at least annually and require Board approval to continue the relationship. The AML/CFT Compliance Officer must prepare a summary report detailing the customer profile, transactional activity versus expected turnover (based on verified source of funds/wealth), related customers, any suspicions, and a clear recommendation regarding continuation or termination.
- Transactions should be carefully reviewed for unusual or atypical activity, with reassessment and updating of customer information as needed.
- Any suspicion arising during ongoing monitoring must be addressed following the relevant sections of this Policy.

All documentation related to these reviews must be retained in the customer's file.

15. Screening Database

- 15.1. The Screening Database contains the names of natural and legal persons, countries, organizations, vessels, and other entities that may be:
- Subject to sanctions;
 - Suspected of involvement in money laundering or terrorist financing activities;
 - Identified as Politically Exposed Persons (PEPs).
- 15.2. The database provides general information about the listed individuals or entities, including current and past positions held, as well as any potentially negative information such as allegations of tax evasion, ongoing legal disputes, or links to PEPs or criminals.
- 15.3. A check against the Screening Database must be performed for all relevant customers. Any discarded hits (false positives) must be carefully evaluated, explained, and documented in the customer's file. True matches require immediate escalation to the AML Department.
- 15.4. The Screening Database must be used to screen the names of all active customers on a daily basis.

16. Internet search / Media check

- 16.1. Internet and media searches shall be conducted on all new applicants as well as during regular or ad hoc reviews of identification records and annual account reviews, for all clients and their associated persons.
- 16.2. The purpose of such searches is to:
- Identify any adverse media or negative public information;
 - Gather comprehensive information to build the customer profile;
 - Detect whether the customer or relevant persons are PEPs, family members, or close associates of PEPs;
 - Cross-check the accuracy of the information provided by the customer.
- 16.3. The officer responsible for preparing the customer file must include and sign the following confirmation on the reconciliation page: *"Internet search has been made."*
- 16.4. All search results must be assessed, and copies of relevant findings shall be retained in the customer's file.
- 16.5. Where negative information or public allegations concerning the customer or its officials are discovered, such information must be clearly disclosed in the customer's file. An assessment shall be conducted to determine appropriate actions by the Company (e.g., reclassification to High-Risk, enhanced monitoring, or termination of

the relationship). This assessment must be discussed and finalized with the AML/CFT Compliance Officer.

- 16.6. Failure to disclose readily available negative information discovered during the internet search, despite confirming that a search was conducted, constitutes a direct breach of this Policy and may result in the Company's failure to effectively fulfill its AML obligations.

17. Record keeping

- 17.1. In accordance with applicable AML/CFT legislation and regulatory guidance, the Company maintains a comprehensive record-keeping system to ensure accountability and traceability of customer activities.
- 17.2. The Company retains the following records in a secure and accessible format for a minimum period of five (5) years from the date of the last transaction or termination of the business relationship, whichever is later:
- Identification and verification documents collected during the KYC and due diligence process;
 - Information and documents related to enhanced due diligence (EDD) and source of funds/wealth assessments;
 - Complete transaction records, including payment methods used, amounts deposited or withdrawn, and transaction timestamps;
 - Records of internal risk assessments, alerts, investigations, and decisions related to suspicious activity.
- 17.3. These records are maintained in accordance with applicable data protection laws, including provisions for secure access, confidentiality, and integrity of personal and financial information. Please refer to the Privacy Policy for more information on the storage of personal data of Website users.

18. Activity Monitoring

- 18.1 The Company employs a comprehensive transaction and behavior monitoring system designed to detect and prevent potential money laundering, terrorist financing, and other illicit activities.
- 18.2 All user transactions and activities are subject to continuous review to identify inconsistencies, risk indicators, or unusual patterns that deviate from the expected behavior based on the user's profile.
- 18.3 Where applicable, the following rules and principles are enforced:

- For any banking or card transaction, the account or cardholder's name must match the registered name on the user's account. If a name change has occurred, supporting documentation must be submitted.
- If deposits are made using non-withdrawable payment instruments, withdrawals may only be processed to a verifiable payment method owned by the user. In such cases, the Company may request documentation to confirm ownership.
- The Company reserves the right to request additional verification documents (such as proof of payment method ownership or Source of Funds) in cases where discrepancies, unusual activity, or elevated risk are detected.

19. Identification of Unusual Transactions

- 19.1. The Company detects and reports either intended or completed unusual transactions. The Company applies both objective and subjective indicators when identifying transactions subject to reporting.
- 19.2. Transactions or intended transactions are deemed unusual and must be flagged if they meet any of the following objective criteria:
- 19.2.1. Transactions by or on behalf of a natural or legal person, group, or entity named on a list adopted by virtue of the Sanctions National Ordinance.
- 19.2.2. Any single transaction or pattern of transactions totaling NAf. 5,000 (\$2,775 USD) or more within a single gaming day:
- Cashless transfers to local or international bank accounts requested by the client.
 - Accepting or releasing a deposit of the threshold amount.
 - Sale of chips, tokens, or credits.
 - Cash-out transactions.
- 19.3. The Company reports transactions where there is cause to presume they relate to money laundering or terrorist financing, regardless of the amount:
- 19.3.1. All complex, unusually large transactions and all unusual patterns of transactions which have no apparent economic or visible lawful purpose.
- 19.3.2. Any circumstance observed to deviate from the profile of the client or the client's past transactions.
- 19.3.3. Use of anonymity tools, VPNs, or proxy servers to mask identity or geographic origin.

20. Suspicious Activity Prevention

- 20.1. The Company's system and AML team actively screen for behaviors commonly associated with financial crime or misuse of the platform, including but not limited to:

- Use of multiple payment cards across various payment providers;
- Use of cards from different issuers or regions within a short time span;
- Frequent switching between unrelated payment instruments (e.g., e-wallets, cards, bank transfers);
- Refusal or unwillingness to verify payment methods;
- Mismatch in geographic indicators, such as country of registration, IP address, device settings, or mobile provider;
- Repeated use of devices linked to multiple accounts (based on device fingerprinting);
- Avoidance or refusal of identity confirmation procedures, including video verification or selfie with ID.

20.2. When such behaviors are detected, the account may be subject to enhanced review, temporary restrictions, or full account suspension pending resolution.

21. Employee Screening and Ongoing AML Training Program

21.1. The Company implements a comprehensive program to ensure that all personnel meet high ethical standards and remain informed of Money Laundering (ML) and Terrorist Financing (FT) risks.

21.2. Before recruiting a new employee, the Company establishes their integrity through:

21.2.1. All candidates must provide a valid official identity document (passport or official ID), a detailed CV, and proof of residential address.

21.2.2. The Company has in place policies and procedures for screening all employees for criminal records prior to and during their employment.

21.3. The Company developed and provides trainings to all personnel who handle transactions that may be qualified as "unusual", which includes:

21.3.1. Establishing specific rules of conduct governing employee behavior.

21.3.2. Providing continuous education to create and maintain professional behavior and awareness against money laundering and terrorist financing.

21.4. Most areas of the institution shall receive training, with modules specifically tailored to the relevance of each staff segment.

21.5. All new employees handling customers or transactions receive general training on the nature and process of ML/TF and the necessity of reporting unusual transactions to the designated officer.

21.6. Personnel charged with overseeing and testing AML controls are trained on changes in regulation, ML methods, enforcement trends, and the resulting impact on the Company.

- 21.7. The Director receives regular and thorough communications regarding ML issues and dangers, specifically to maintain awareness of the reputational risks money laundering poses to the Company.
- 21.8. The Company organizes mandatory AML/CFT training sessions for all relevant staff at least annually, with additional sessions conducted as needed in response to regulatory updates or internal procedural changes.
- 21.9. New employees must complete initial AML training as part of their onboarding process before accessing any AML-sensitive systems or handling user data.
- 21.10. The Company performs regular staff assessments to evaluate the level of understanding and competence of its employees in relation to AML/CTF and KYC practices. These assessments help identify areas for improvement and ensure that all team members remain fully equipped to perform their functions.
- 21.11. The training program is overseen by Senior Management and is documented in accordance with the Company's internal control framework.
- 21.12. Employee integrity is subject to continuous review throughout the duration of the employment contract: Employees are required to immediately notify the Compliance Officer of any changes in their legal status, including new criminal charges or investigations; For employees in high-risk or key positions, the Company shall conduct a refreshed criminal background check at least every three (3) years; Regular performance evaluations includes a review of the employee's adherence to internal AML/CFT procedures and ethical codes of conduct.

22. Independent Audit

- 22.1. The AML compliance program is monitored and evaluated at least annually by an adequately resourced independent audit.
- 22.2. Independent testing of the AML program shall include, at a minimum, the following assessments:
 - 22.2.1. Evaluation of the AML Compliance Framework;
 - 22.2.2. Assessment of the overall effectiveness of compliance management structures;
 - 22.2.3. Performance of substantive transaction testing to ensure internal controls are functioning as intended;
 - 22.2.4. Assessment of compliance with applicable laws;
 - 22.2.5. Evaluation of the adequacy and effectiveness of staff training programs.
- 22.3. All identified deficiencies must be reported to the Director, and to the designated officers.

23. Examination by the Gaming Control Board

- 23.1. The Company ensures full cooperation with the GCB and any competent regulatory authority by maintaining and providing, upon request, all relevant information and documentation related to its Anti-Money Laundering (AML), Counter-Terrorist Financing (CFT), and Counter-Proliferation Financing (CPF) framework.
- 23.2. All required documentation is made readily available in preparation for, during, and upon request in connection with any regulatory examination, including requests made throughout the year.
- 23.3. Failure to maintain or provide such documentation in a timely manner is considered a breach of this Policy and may result in disciplinary actions and/or regulatory consequences.

24. Reporting of unusual activity or transactions

- 24.1. The Company reserves the right to report any transaction or user behavior that raises suspicion of money laundering, terrorist financing, or other criminal activity.
- 24.2. If the Company identifies activity that cannot be reasonably explained or justified by the user and meets objective or subjective indicators of suspicious behavior, such activity may be reported to the appropriate authority of Curaçao.
- 24.3. All unusual individual transactions or series of transactions are reported internally, without any delay. The Company reports unusual transaction or any intended unusual transaction to the FIU without delay.

25. References

Here you can find the source list (but not limited to) for this Policy. Additional legislation or documents may be applied.

- 1) The Forty Recommendations and Special Recommendations on Terrorism Financing ("FATF Recommendations");
- 2) Risk-based approach guidance for the casinos (RBA for Casinos), issued by FATF;
- 3) Directive 2015/849 of the European Union and Council of 20 May 2015 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing;
- 4) Commission Delegated Regulation (EU) 2016/1675 of 14 July 2016 supplementing Directive (EU) 2015/849 of the European Parliament and of the Council by identifying high-risk third countries with strategic deficiencies;
- 5) Curacao Gaming Control Board, Regulations for the combating of Money Laundering, the Financing of Terrorism and Proliferation of weapons of mass destruction, last update January 2025;

- 6) FATF list of High-risk and other monitored jurisdictions: <http://www.fatf-gafi.org/countries/#high-risk> .

Document type:	Policy
Version:	1.2
Version Date:	16.04.2026
Approved by:	(SMES) Solutions for Management and Employment Support N.V., Vivian Victoria Ersilia, Managing Director
Owner of the Document:	Inga Grope, Compliance Officer



Vivian Ersilia o.b.o.

(SMES) Solutions for Management and Employment Support N.V.

Managing Director

Date: 30.04.2026