

AML Policy

Investan N.V. (Curaçao) (the ‘**Company**’, ‘**We**’) is a company registered and incorporated in Curacao with Company registration: 153108.

The Company is authorised by the Curaçao Gaming Control Board (**OGL/2024/1630/1008**) under a valid Certificate of Operation until the application process is concluded.

The company is further approved to accept and transact with customers in crypto (digital or virtual) currencies.

Table of Contents

Overview

- 1.1. Introduction
- 1.2. Management
- 1.3. Legal framework
- 1.4. Risk-based approach
- 1.5. Data processing system
- 1.6. Staff Training

Customer Acceptance and Registration Policy

- 2.1. Introduction
- 2.2. Customer Acceptance
- 2.3. Restrictions
- 2.4. Information Entered on Registration
- 2.5. Terms of Acceptance
- 2.6. Underage Customers
- 2.7. Customer Due Diligence

Customer Risk Scoring and Profiling

- 3.1. Introduction
- 3.2. Customer Risk Assessment
 - 3.2.1. Individual status
 - 3.2.2. Geographical location
 - 3.2.3. Gambling and transactional behaviour
 - 3.2.4. Payment Methods
 - 3.2.5. Fraud red flags
- 3.3. Risk Score Calculation
- 3.4. Customer Due Diligence Level
- 3.5. Additional Details & Source of Funds/Wealth
- 3.6. On-Going Monitoring
- 3.7. Withdrawals

Customer Due Diligence

- 4.1. Introduction
- 4.2. Standard Customer Due Diligence

- 4.3. Document acceptance
- 4.4. Threshold approach
- 4.5. Ongoing monitoring
- 4.6. Enhanced Due Diligence
- 4.7. Politically Exposed Persons and Sanctions Screening
- 4.8. Procedure for Account Closure

Deposit and Withdrawal Management Procedures

- 5.1. Player Account
- 5.2. Balance Payment Methods
- 5.3. Player Deposits
- 5.4. Player Withdrawals
- 5.5. Withdrawal Payouts

Suspicious Activity Reporting

- 6.1. Introduction
- 6.2. Red Flags Indicators
- 6.3. Inability to Complete CDD Measures
- 6.4. Internal Suspicious Activity Report
- 6.5. External report to FIU
- 6.6. Reporting Procedure
- 6.7. Tipping-off

Internal Control

- 7.1. Introduction
- 7.2. Recordkeeping
- 7.3. Money Laundering Reporting Officer
- 7.4. Training
- 7.5. Employee background check
- 7.6. Technological developments risk assessment
- 7.7. Internal and external revision and staying up-to-date
- 7.8. Version Control

1. Overview

1.1. Introduction

Money laundering refers to the act of hiding, disguising, converting, transferring, or moving illicitly obtained property. Simply put, it is the procedure of transforming the profits from criminal activity into assets that appear to have a lawful origin.

There are three stages of money laundering:

- **Placement** – The introduction of illicit funds into the financial system, either directly or through indirect means such as blending with legitimate funds, committing invoice fraud, or using smurfing techniques;

- **Layering** – This phase focuses on distancing illegal proceeds from their origins by conducting a series of complex financial transactions. These layers are meant to obscure the audit trail and provide anonymity, often through multiple bank transfers or investing in cash-heavy businesses;
- **Integration** – The final stage is when criminally derived money is reintroduced into the economy, appearing legitimate. After successful layering, the funds are integrated into the financial system, for instance, through property purchases, making the illicit money seem legally earned.

Terrorist financing refers to the provision or collection of funds with the intent, or knowledge, that they will be used to support terrorist activities or organizations, or to carry out acts of terrorism.

The main distinctions between money laundering (ML) and terrorist financing (TF) are:

- Money laundering requires that the funds involved come from criminal activities;
- Terrorist financing can involve money from either legal or illegal sources, meaning the origin of the funds is irrelevant.

Despite these differences, both ML and TF involve financial transactions and value movements, such as between individuals, accounts, institutions, countries, or asset classes. Both are focused on concealing the origins and destinations of the funds.

The company has implemented internal security measures to prevent money laundering and terrorist financing. These measures are designed to monitor high-risk customers and identify suspicious behaviours, including those related to predicate offenses of money laundering and terrorist financing.

1.2. Management

Company, a limited liability company incorporated under the laws of Curaçao with company number 168766 and a registered office at Zuikertuintjeweg Z/N, Curaçao (hereinafter referred to as “the Company”), has appointed a Compliance Officer in accordance with Article 5g of the NOIS.

This policy is applicable to all employees and outsourced staff involved in anti-money laundering, responsible gambling, and anti-fraud procedures as they relate to their respective duties, including senior management and the Compliance Officer.

The Compliance Officer, who is primarily responsible for preventing money laundering and the financing of terrorism, is also responsible for ensuring ongoing regulatory compliance and overseeing anti-money laundering procedures.

The Compliance Officer will be actively involved in developing and managing the processes required to combat money laundering and other fraudulent activities based on the following key principles:

- The Company operates on the assumption that the majority of its customers are not engaged in money laundering. However, in compliance with applicable regulations, it uses a risk-based approach to verify player identities;
- The Company monitors all transactions and activities;
- The Company conducts continuous monitoring of its customers, associated risks, and internal processes.

The Company will ensure that all relevant employees receive training on AML and CTF policies and procedures, emphasising awareness of these risks. All applicable employees must pass competency assessments on these topics.

1.3. Legal framework

The Company's Policy and Procedures have been developed in accordance with the relevant applicable legislation, including but not limited to the following:

- Curaçao - National Ordinance Reporting Unusual Transactions (NORUT) of November 7, 2017;
- National Ordinance Identification when Rendering Services (NOIS) of October 2, 2017;
- National Ordinance Penalization of Money Laundering (NOPML)
- EU-Directive 2015/849 of the European Parliament and of the Council of 20 May 2015;
- EU-Directive 2018/843 of the European Parliament and of the Council of 30 May 2018;
- EU-Directive 2018/1673 Of the European Parliament And Of The Council Of 23 October 2018;
- The FATF Recommendations.

1.4. Risk-based approach

The Company is committed to preventing and combating money laundering and terrorist financing by employing a risk-based approach. This approach is outlined in the following key areas:

- **Risk identification and assessment** – Identifying the money laundering risks the Company faces, considering its customer base, products, and services, as well as relevant available information, and evaluating the potential scale and impact of these risks;
- **Risk mitigation** – Implementing appropriate measures to reduce the significant risks that the Company may encounter;
- **Risk monitoring** – Establishing management information systems (MIS) to continuously track changes in the risk profile, whether from business developments or evolving threats;
- **Documentation** – Recording the risk assessment and strategy, ensuring policies and procedures cover these areas, and securing effective accountability from the board and senior management.

1.5. Data processing system

The Company utilizes an internal data processing system to identify high-risk situations, detect money laundering, and monitor terrorist financing in its daily operations.

The data processing system includes the following components:

- Identification of all users before entering into a business relationship requires them to complete a registration form to confirm their details;
- Politically Exposed Person (PEP) and sanction list checks, performed using specialized software;
- Transaction monitoring, handled by trained staff members;
- Reporting of all suspected money laundering cases to the Compliance Officer and the Financial Intelligence Unit (FIU).

The Company will continue to monitor trends and developments related to ML/TF and will introduce additional internal procedures as necessary to stay current.

1.6. Staff Training

Upon joining the Company, and subsequently, on an annual basis, all staff (including outsourced teams) will receive training on AML/CFT procedures and related policies. This training will be delivered either through online and in-person training providers or by the Company's designated specialist. Employees selected for training will be determined based on individual risk assessments.

2. Customer Acceptance and Registration Policy

2.1. Introduction

Before engaging in gambling, making a deposit, or placing real-money bets, customers are required to register an account. Without account registration, customers will not be permitted to participate in gambling activities.

The Customer Acceptance and Registration Policy outlines the criteria the Company uses to determine whether or not to accept potential customers and details the steps involved in the registration process.

2.2. Customer Acceptance

Customers must first complete the registration process to make a deposit and participate in gameplay on the Company's site.

Registration is restricted to individuals who are at least eighteen years of age.

Customers are permitted to open only one account in their name per site. Additional checks are conducted to prevent the creation of multiple accounts, using factors such as email

address, mobile number, device information, and other customer data combinations. These checks are implemented to prevent customers from circumventing AML thresholds by opening multiple accounts.

2.3. Restrictions

Individuals under the age of 18 are strictly prohibited from registering on the site.

Additionally, individuals identified as Politically Exposed Persons (PEP), subject to sanctions, or listed on any blacklists are also not permitted to register. This includes but is not limited to individuals or entities associated with the restricted list of countries as per the Company's Terms and Conditions.

This also applies to individuals who already have an exclusion on the site or exhibit fraud-related red flags.

Players are allowed to open only one account in their name per site. Additional checks are conducted to prevent the creation of multiple accounts using factors like email address, mobile number, device information, and other data combinations. These checks aim to prevent players from opening multiple accounts to bypass AML thresholds.

2.4. Information Entered on Registration

During the registration process, and potentially at later stages, the Company will request the following personal identification and contact information:

- First Name and Last Name;
- Date of Birth;
- Gender;
- Address and country of Residence;
- Email address and mobile number;
- Username and Password.

2.5. Terms of Acceptance

As part of the registration process, the customer is also required to confirm their acceptance of the website's general terms and conditions and privacy policy.

2.6. Underage Customer

The system prevents the registration of underage customers. To successfully complete the registration process, customers must be at least 18 years old or the legal age in their jurisdiction. The provided Date of Birth will be verified against the customer's ID during the Due Diligence process.

2.7. Customer Due Diligence

To finalize registration, the customer must successfully pass the Customer Due Diligence (CDD) process. If the CDD is not passed, the registration will be denied.

The process cannot take more than 72 hours from the time the client sends the information.

3. Customer Risk Scoring and Profiling

3.1. Introduction

As part of the risk-based framework, the Company will conduct risk profiling of all customers upon registration to assess potential money laundering and terrorism financing risks.

It is essential to highlight that the Company's policies and procedures are built on the following:

- Current regulatory and legal requirements;
- Guidance from the CGA and FIU;
- The Company's internal assessment of overall business risk and its knowledge and experience with customers.

3.2. Customer Risk Assessment

Based on the information provided during registration (e.g., customer home address, location, age, PEP/sanctions status), the Company will conduct an initial risk assessment for each customer. Customers will begin their gambling activities with the Company categorized as Low, Medium, or High risk for money laundering (ML) or terrorist financing (FT), which will guide how they are managed at later stages. Risk assessments are conducted regularly and whenever new information becomes available.

The following factors determine the customer risk assessment:

- Individual status (e.g., PEP, under sanctions, adverse media coverage);
- Geographical location;
- Gambling and transactional behaviour;
- Payment methods used by the customer;
- Fraud red flags that the customer may have triggered.

Customers identified as high-risk will be required to undergo Enhanced Due Diligence (EDD).

3.2.1. Individual status

PEP

A Politically Exposed Person (PEP) is any individual who holds or has held a prominent public position at the international, European, or national level, or someone who has been entrusted with a similarly crucial political role at a subnational level.

Any new or existing customer identified as a PEP or as a relative of such a person will have their account either rejected or closed.

Sanctions list

Governments and international organizations release sanctions lists to target individuals, organizations, or governments engaged in unlawful activities. These lists include sanctioned persons, entities, or governments deemed to pose a high risk.

Individuals or entities appearing on these sanctions lists are subject to financial restrictions aimed at combating counterterrorism and money laundering efforts globally.

Any new or existing customer found on the Sanctions database will have their account rejected or closed.

Adverse media

Adverse media refers to any negative or unfavorable information about a customer or business found across various sources. This information could indicate potential involvement in criminal activity.

Any new or existing customer mentioned in adverse media will be subject to Enhanced Due Diligence (EDD). Depending on the results of the EDD, the Company may either close the account or reject the registration.

3.2.2. Geographical location

If the Company determines that a customer resides in a high-risk country, this may trigger Enhanced Due Diligence (EDD).

High-risk countries are those jurisdictions identified as having significant strategic deficiencies in countering money laundering, terrorist financing, and proliferation financing. The Company identifies high-risk countries in accordance with FATF regulations, which are accessible at the following link:

<https://www.fatf-gafi.org/en/countries/black-and-grey-lists.html>

The Company has implemented a geo-blocking tool to restrict access to its services for players located in specific geographic regions. A list of prohibited countries can be found in the Terms and Conditions.

3.2.3. Gambling and transactional behaviour

The company continuously monitors each player's behavior. The monitoring focuses on identifying both signs that could indicate problem gambling and behaviors that suggest potential money laundering.

When certain behaviors are detected, they are assigned scores, which are combined with other scored red flags related to money laundering or terrorist financing (ML/FT).

Suppose any clear examples of ML/FT behavior are observed. In that case, the customer must undergo Enhanced Due Diligence (EDD) immediately, and if needed, the Suspicious Activity Report (SAR) process will be initiated.

3.2.4. Payment Methods

Payment methods that enable the Company to trace the origin of the funds, such as a bank account, and allow refunds to be sent back to the original source are considered low-risk.

On the other hand, payment methods funded by cash, which do not allow for tracing the source of the funds or returning them to the original source, are classified as high risk.

Payment Method	Risk Rating
Bank transfers (Klarna, Trustly, Rapid, ApplePay), debit cards issued by banks	Low
EEA-licensed e-wallets (Skrill, Neteller, Paysafecard)	Medium
Prepaid cards, Vouchers, and Cryptocurrency	High

The company also regards manipulations involving payment methods, such as making deposits with one method and withdrawing with another, as high-risk behavior.

3.2.5. Fraud red flags

The Company has an anti-fraud risk management system designed to prevent various forms of fraud, including bot attacks, fraudulent traffic, synthetic identities, account takeovers, identity theft, credit card and CNP fraud, proxy users, multi-accounting, and collusion. Some fraud red flags may also be linked to potential money laundering.

If the Company detects that a player has triggered a fraud red flag, the player will automatically be subject to Enhanced Due Diligence (EDD).

3.3. Risk Score Calculation

This procedure aims to identify minor instances of ML/FT behavior that, on their own, may not raise suspicion but, when combined with other behaviors, may warrant further investigation.

The internal CMS system will evaluate a player based on the factors mentioned above and assign a risk score accordingly.

Each factor contributes a score, and the total risk score is the sum of the individual scores. The higher the overall score, the greater the risk.

Please note that these factors, scores, and thresholds are internal and will be adjusted as the Risk Score (RS) Calculation process is improved and updated.

Indicator	Description	Score
	Individual status	
PEP	A customer considered to be PEP	100
Adverse media	A customer was mentioned in negative news or information that the company discovered from various sources	50
Sanctions/blacklist	A customer is under international sanctions/ blacklist	100
	Geographical location	
Not at home	A customer whose IP location is different from their registered address	20
High-risk country resident	A customer resides in a high-risk country	30
	Gambling behaviour	
Large sums no play	A customer deposits large sums, then places minimal stake bets, and withdraws all their funds	50
Large sums, big losses	A customer depositing large amounts and repeatedly losing large amounts, as if the loss is of no consequence (EUR 5000 per week)	50
Low odds betting	A customer repeatedly placing short odds (such as red/black on roulette or repetitive betting on favourites) bets	25
Big changes in money	Dramatic changes in terms	20

	of volume and size of player deposits or staking activity	
Several gaming accounts	A customer is trying to register several gaming accounts	30
	Transactional behaviour	
Smurfing	A customer making multiple deposits or withdrawals of small amounts without any objective reasons	30
Spending above wages	A customer's spending is outside of their affordability	20
No withdrawals	The player has never requested a withdrawal	-20
Withdrawal without playing	Money is deposited by a customer or held over a period and withdrawn by the customer without being used for gambling	30
	Payment methods the player is using	
Card switching	A customer opening an account and registering several different cards, and making transfers between them	20
High-risk payment methods	A customer uses high-risk payment methods	30
	Fraud red flags a customer-triggered	
VPN	The customer used a VPN	30

Once the score is calculated, a risk level is assigned:

CMM Score	Risk Category
0 - 20	Low

21 - 40	Medium
41 - and higher	High

Due to technical or practical limitations, not all factors can be automatically incorporated into the Customer Risk Assessment (CRA) calculation. However, we monitor these risks through other methods. For instance, we check for VPN usage and multi-accounting during the registration process, have a separate alert system for players using cards registered under a different name, and ensure that all withdrawals are reviewed before approval and payment.

3.4. Customer Due Diligence Level

The level of Customer Due Diligence (CDD) performed on a player will be determined by the risk score assigned to the player, as outlined below:

	Low	Med	High
Verify ID and address with documents	X	X	X
Collect additional personal details		X	X
Collect the Source of Funds/Wealth info		X	X (with documentation)
Ongoing monitoring	X	X	X (Enhanced)
Additional measures to address any other risk identified			X
Report suspected cases of ML/FT	X	X	X

3.5. Additional Details & Source of Funds/Wealth

The Compliance Officer will receive a daily report detailing any player newly classified as medium or high risk or any player who has moved from medium to high risk.

The responsible AML manager will then:

1. Review all accounts listed in the report, which include:
 - a. Verifying what information the Company already holds on the player;
 - b. Conducting open-source Internet checks;
 - c. Assessing if there are any signs of suspicious activity.
2. The AML manager will then take the appropriate actions:
 - a. Block the account if necessary;

- b. Apply the appropriate Due Diligence measures;
 - c. Review the responses and information provided by the player;
 - d. Take further action as required.
3. If the player fails to respond within 14 days or if the response is deemed unsatisfactory, the account will be blocked. If documents are provided after the deadline, the AML manager will assess whether the delay itself is suspicious and act accordingly.

Accounts classified as medium or high risk will require AML approval before any withdrawal requests can be processed.

All decisions made by the AML manager must be thoroughly documented.

3.6. On-Going Monitoring

The AML team will carry out ongoing monitoring of accounts on a risk-sensitive basis. This includes:

- Obtaining updated identification documents when the existing ones have expired;
- Investigating any inconsistencies in the data or information provided by a player;
- Periodically reviewing and updating account information based on the assessed risk.

3.7. Withdrawals

When the AML Team reviews a withdrawal request, they will also assess the player's risk level:

- If the player is classified as medium or high risk, the Verification Team will review the player's documentation and confirm that all documents are still valid;
- If any documents have expired, updated documents will be requested.

As a result, any withdrawal request from a player flagged as medium or high risk, or any request flagged as high risk for other reasons, will require AML team approval before it can be processed and completed.

4. Customer Due Diligence

4.1. Introduction

The Company differentiates between Customer Due Diligence (CDD) and Enhanced Customer Due Diligence (EDD).

Customers are required to cooperate in fulfilling the due diligence obligations. If the Company is unable to complete the necessary due diligence, the business relationship will not be initiated or continued, and no transactions will be processed. Furthermore, the Company will assess whether it is necessary to file a Suspicious Activity Report (SAR).

4.2. Standard Customer Due Diligence

The Company applies standard Customer Due Diligence (CDD) measures for all customers during the registration process. The CDD process consists of the following:

- Identification – Establishing the customer's identity by collecting relevant personal information;
- Verification – Confirming the customer's identity by obtaining and validating documents or information from reliable, independent sources.

In accordance with these requirements, the Company gathers the following information for identification and verification to prevent money laundering and terrorist financing:

- First and Last Name;
- Date of birth;
- Permanent residential address;
- Nationality;
- Identity number.

The Company may also gather the following documents for verification purposes:

- Identification document (ID);
- Proof of Address (POA).

4.3. Document acceptance

For identity verification, the Company requires a government-issued document that includes photographic evidence of the customer's identity. The following documents may be accepted for this purpose:

- A current, signed passport;
- Driving license;
- Identity card or travel document;
- Any other document designated by the Minister;
- For Proof of Address (POA) verification, the Company accepts:
 - A utility bill for a service installed at the customer's residence, issued within the last 6 months;
 - Correspondence or any government-issued document from a central or local authority, department, or agency issued within the last 6 months;
 - A lease agreement (does not need to be issued in the last 6 months, but must be currently valid);
- The main requirements for the documents provided by the customer are:
 - The document must be valid and not expired;
 - Documents must be clear, legible, and of good quality;
 - Mobile phone bills will not be accepted.

4.4. Threshold approach

The Company may apply Enhanced Due Diligence (EDD) measures for any transaction totalling EUR 2000 or more, whether conducted as a single transaction or as several transactions that appear to be linked.

A “transaction” includes the following:

- The deposit of funds required to participate in remote gambling
- The collection of winnings, including withdrawals of funds deposited for gambling or

Transactions are considered linked if they form part of a customer's overall activity during a single session of logging into the operator's gambling platform. However, this is not an exhaustive definition, and the Company also assesses other situations where transactions may be linked using a risk-based approach.

Careful consideration is given to situations where customers might intentionally spread their wagering or winnings collection across multiple transactions in an attempt to bypass CDD/EDD requirements.

For EDD measures triggered by this threshold, the Company applies verification procedures based on a risk-based approach.

4.5. Ongoing monitoring

The general due diligence duties include ongoing monitoring of the business relationship.

This involves:

- Obtaining updated identification when existing documents expire (this can be done on a risk-sensitive basis);
- Investigating any data or information inconsistencies noticed by the Company;
- Conducting periodic reviews and updates based on risk sensitivity;
- Ensuring transactions align with the documents and information the Company holds about the customer, including the customer's assets and the origin of funds;
- Updating relevant documents, data, or information at appropriate intervals.

To ensure customer information remains current, the Company conducts the ongoing CDD procedure at its sole discretion and based on a risk-sensitive approach.

4.6. Enhanced Due Diligence

The Company applies enhanced customer due diligence measures (hereinafter - EDD) and enhanced ongoing monitoring, in addition to the required CDD measures, to manage and mitigate the money laundering or terrorist financing risks.

EDD is applied in the following situations:

- In any case, identified by the Company or in the information provided by the authorities to the Company as one where there is a high risk of money laundering or terrorist financing;
- If the Company has doubts as to whether the information collected regarding the identity of the customer is correct or not (or no longer) accurate;
- If the Company has determined that a customer or potential customer is a PEPA or a family member or known close associate of a PEP, in any case where the Company discovers that a customer has provided false or stolen identification documentation or information, and the Company proposes to continue to deal with the customer;
- In any case where a transaction is complex or unusually large, or there is an unusual pattern of transactions, or the transaction or transactions have no apparent economic or legal purpose;
- If the payment of a customer's winnings is made to a different payment account of the customer than to the account from which the customer makes the wagers;
- In any other case, which, by its nature, can present a higher risk of money laundering or terrorist financing.

In cases where there is a higher risk, the business relationship can be established or continued (if the higher risk only arose later or was only recognised later) with the consent of the Compliance Officer.

If a customer has been deemed to be a high-risk or becomes one at any stage, the Company undertakes the EDD, comprising (depending on the case):

- Undertaking re-verification of identity (repeated CDD);
- Establishing how the customer acquired his wealth to be satisfied that it is legitimate:
 - Salary income or company profit (Certified Payslip / Certified employer letter / audited accounts if self-employed);
 - Sale or liquidation of financial instruments (Certified shares/investments sale contracts or statements/ accountant letter);
 - Sale of property (Certified copy of the contract of sale or letter from a solicitor or estate agent);
 - Inheritance (Certified copy of will including the value of the heritage);
 - Sale of the company (Certified contracts, media articles, certified letter from accountant or solicitor);
- Establishing the source of the customer's funds to ensure that they do not constitute the proceeds of crime;
- Ensure that deposits originate from payment methods and do not allow anonymity by requesting copies of bank statements or account statements;
- Undertaking increased continuous monitoring of the business relationship;
- The suspicious transaction must be investigated, and the business relationship underlying the transaction shall be monitored to assess the risk of money laundering and terrorist financing.

Undertaking the EDD on transactions, the Company's fundamental aim is to ensure the transparency of payment flows. Accordingly, the origin and destination of the money used in a transaction shall be traceable back to an account in each case.

Meaning of Source of Funds

The Source of Funds refers to the origin of the particular funds being used to deposit on the Company's website. This is not simply verifying which bank or financial institution the customer may have received the funds from. The information obtained should be substantive and relevant, and the fund's origin and the method/circumstances under which the funds were acquired should be established.

Meaning of Source of Wealth

The Source of Wealth refers to the origin of the customer's entire wealth or total assets. The information that the Company obtains should indicate the volume of wealth the client would reasonably be expected to have and provide a picture of how it was acquired.

4.7. Politically Exposed Persons and Sanctions Screening

The Company uses the KYC software tool to check all new customers at the registration stage against the PEP and Sanctions databases. The Company also checks the whole customer database every six months to ensure existing customers have not changed their status.

Any new or existing customer found on the Sanctions database, or a PEP or relative of such, will have their account rejected or closed.

If a PEP is identified, responsible staff will send a report to the Compliance Officer, who in turn will send a report to senior management.

The Compliance Officer will investigate each case to identify positive or false-positive PEP alerts. The Company has the right to request additional documents from the customer during the investigation.

If the PEP alert is true-positive, the Compliance Officer will reject registration or close the account and inform senior management about the decision.

Politically Exposed Person means any person who has been entrusted with a high-ranking, prominent public function at the international, European, or national level or who is or has been entrusted with a public position of comparable political importance below the national level. In particular, politically exposed persons are:

- Heads of state, heads of government, ministers, members of the European Commission, deputy ministers, and assistant ministers;
- Members of parliament and members of similar legislative organs;
- Members of the governing bodies of political parties;
- Members of supreme courts, constitutional courts, or of other high-level judicial bodies, the decisions of which are usually not subject to further appeal;
- Members of the boards of courts of audit;
- Members of the boards of central banks;

- Ambassadors, chargés d'affaires and defence attaches;
- Members of the administrative, management, or supervisory bodies of state-owned enterprises;
- Directors, deputy directors, members of the board, or other managers with a comparable function in an international or European intergovernmental organization.

A family member of PEP means a close relative, in particular:

- The spouse or civil partner;
- A child and the child's spouse or civil partner;
- Both parents.

FATF-blacklisted/grey-listed countries are blocked on the company's sites, and individuals from these countries are not able to register or log in from these countries. The list of FATF blacklist/grey-listed countries may be found here:

<https://www.fatf-gafi.org/en/publications/High-risk-and-other-monitored-jurisdictions.html>

4.8. Procedure for Account Closure

There are several reasons why the Company may choose to close a customer's account, including:

- Fraud;
- Cheating;
- Bonus Abuse;
- Allowing a third person to use their account;
- Underage gambling;
- Problem gambler;
- Abusive behavior towards staff;
- Commercial concerns;
- Failure in Customer Due Diligence (CDD);
- Breach of Terms and Conditions;

However, this Company Policy focuses specifically on situations where there is suspicion or knowledge that the customer may be involved in money laundering (ML) or terrorist financing (FT).

By law, the Company must end the business relationship with the customer unless we have obtained appropriate consent for it to continue, and even then, it is precautionary to close the account.

Due to the laws on Tipping Off, the Company cannot inform the customer that we have concerns regarding ML/FT. Thus, account closure must be done sensitively.

The Compliance Officer will need to consider whether a SAR was submitted as part of the concern about the player's behaviour and whether appropriate consent should have been requested.

Where the Company is unable to complete or apply the required CDD measures in relation to a particular customer at the point the CDD threshold for transactions is reached, it is accordingly required to cease transactions and terminate the business relationship with the customer.

5. Deposit and Withdrawal Management Procedures

5.1. Player Account Balance

Each player has a wallet containing their funds, from which bets are deducted and winnings are added. All funds deposited by the player, as well as any amounts owed by the Company, are credited to the player's account. Players can add funds to their account by making deposits through the site's cashier and can then use these funds to place bets. Bets are subtracted from the account balance, and any winnings are credited back to the balance.

Players can withdraw the funds in their account balance. The Company does not offer credit to players, and players are not permitted to transfer funds to other players.

5.2. Payment Methods

Payments will only be accepted and processed through accounts held with licensed financial institutions or via licensed payment providers.

No cash deposits or withdrawals will be conducted directly between the Company and its players.

5.3. Player Deposits

After completing registration, a player can deposit funds into their account through the site's cashier.

To facilitate these deposits, the Company has integrated with several payment gateways. All gateways are PCI DSS compliant, and the Company does not store any credit card data.

The Company submits the transaction to the Payment Service Provider (PSP) and waits for approval from the card acquirer or e-wallet. Once approved, the deposit status is updated, and the funds are credited to the player's balance.

5.4. Player Withdrawals

A player with an available balance can request a withdrawal of funds through the site's cashier.

The player will enter the desired withdrawal amount and select their preferred payout method. Once the request is submitted, the withdrawal amount is deducted from the player's balance.

5.5. Withdrawal Payouts

When remitting funds to the player, we will, wherever possible, transfer the funds directly to the account from which the original deposit was made.

Provided that, where this is not possible, we will remit the funds to the player in line with the requirements under AML legislation.

6. Suspicious Activity Reporting

6.1. Introduction

Every employee of the Company is required to report any suspicions or knowledge of money laundering, terrorist financing, or the use of criminally derived funds on the Company's website to the Compliance Officer.

The Compliance Officer will review each report to determine whether there are sufficient grounds for suspicion or knowledge. If so, a Suspicious Activity Report (SAR) must be submitted to the Financial Intelligence Unit – Financiële Inlichtingen Eenheid (FIU or FIU Curaçao).

Knowledge means that the person reporting is sure of the event. At the same time, suspicion indicates that the person has observed something unusual or unexpected, and after making inquiries, the facts do not appear normal or commercially or financially reasonable.

A transaction or activity may not seem suspicious at first, but if suspicions arise later, there is an obligation to report it at that point. Similarly, if further inquiries deepen the concern, it is reasonable to conclude that the transaction is suspicious and must be reported to the FIU.

The Compliance Officer will assess all relevant circumstances and may ask the customer or others additional questions if necessary. The approach depends on what is already known about the customer, the transaction, and the ease of making further inquiries.

6.2. Red Flags Indicators

Red flags are not intended to automatically trigger the filing of a Suspicious Activity Report (SAR) with the FIU. Still, they are indicators that should prompt the Company to question the customer's behaviour. If no reasonable explanation for the red flags is found, an internal report must be made to the Compliance Officer.

Below is a list of potential red flags that should be considered:

- The customer does not cooperate during the CDD/EDD process;
- The customer attempts to register more than one account on the site;

- The customer makes small wagers despite depositing significant amounts, followed by withdrawal requests far exceeding any winnings;
- The customer frequently deposits and makes withdrawal requests without any reasonable explanation;
- Noticeable changes in the customer's gaming patterns, such as conducting transactions that are significantly larger in volume compared to their usual activity;
- The customer inquires about transferring funds between accounts within the same gaming group;
- The customer conducts transactions that seem disproportionate to what is known about their wealth, income, or financial situation;
- The customer attempts to transfer funds to a bank account in the name of a third party;
- The customer requests a withdrawal to an account they have never deposited with;
- The customer opens an account and registers multiple cards, making transfers between them;
- The customer deposits large sums, places minimal bets, and then withdraws all their funds;
- The customer deposits large amounts and consistently loses large sums, as if the losses are inconsequential.

6.3. Inability to Complete CDD Measures

If a customer refuses to provide CDD/EDD documentation, the Company will not automatically interpret this refusal as suspicion of money laundering or terrorist financing (ML/FT).

The Company will assess all available factors and information, including the payment method used, the types of games played, playing trends and patterns, the customer's jurisdiction of residence, and any open-source information.

If, after evaluating all of these factors, there are grounds to suspect ML/FT, a SAR must be submitted.

6.4. Internal Suspicious Activity Report

All employees must report suspicious transactions. If any employee suspects a customer's behavior or transaction, they must report it immediately to the Compliance Officer. Employees are required to use the approved Internal Suspicious Activity Report (SAR) Form for this purpose.

Employees should submit the report even if their superiors disagree. The Compliance Officer then determines whether the available information is sufficient to warrant submitting an SAR to the FIU.

The following information is included in an Internal SAR:

- The customer's details;
- The staff member's statement explaining the cause of the report;

- All relevant documentation and information;
- The Compliance Officer will:
- Acknowledge receipt of the report and conduct further review and investigation if needed;
- Assess the information and decide whether the matter should be reported to law enforcement;
- If necessary, submit a SAR to the FIU;
- Document the decision and inform senior management of the actions taken.

6.5. External report to FIU

Once the Compliance Officer receives an Internal SAR, they will determine whether a SAR should be submitted to the FIU.

In making this decision, the Compliance Officer should consider that AML legislation aims to combat serious crime, typically involving substantial amounts or situations that indicate an attempt to bypass safeguards designed to prevent misuse of the financial system for criminal purposes.

For instance, identity fraud and chargebacks could lead to money laundering, but a licensee is only obligated to report if these activities result in funds being deposited with or held by the licensee.

The Company will not report isolated instances involving small amounts but will assess whether there is a broader pattern or scheme that warrants attention.

When evaluating an internal report for potential money laundering, the Compliance Officer considers all relevant information, such as identifying standard links between repeated suspicious behaviours, chargebacks, or identity fraud. This could involve familiar persons, related IP addresses, or other shared factors.

In deciding whether to submit a SAR, the Compliance Officer should answer the following questions:

- Who is involved?
- How are they involved?
- What is the criminal/terrorist property?
- What is the value of the criminal/terrorist property (estimated as necessary)?
- Where is the criminal/terrorist property?
- When did the circumstances arise?
- When are the circumstances planned to happen?
- How did the circumstances arise?
- Why are you suspicious or have knowledge?

6.6. Reporting Procedure

The Company is required to submit a Suspicious Activity Report (SAR) to the FIU, either through the user interfaces on the FIU's website or by mail (if permitted), without undue delay if there are indications that:

- The Company knows, suspects, or has reasonable grounds to believe that money laundering and/or terrorist financing is occurring;
- An asset involved in a business relationship or transaction originates from a criminal offense that could constitute a predicate offense to money laundering;
- A business case, transaction, or asset is linked to terrorist financing;
- When deciding whether to submit a SAR, the Company considers several factors, including but not limited to:
 - The purpose and nature of the transaction;
 - Unusual characteristics or behaviors of the customer;
 - The customer's financial and business background;
 - The origin of the assets involved or to be contributed.

The Company will not execute suspicious transactions except in cases where delaying the transaction is impossible or would hinder the prosecution of an alleged criminal offense. In such cases, the Company submits a SAR immediately.

6.7. Tipping-off

It is a criminal offense to inform anyone that a SAR has been submitted or is being considered if doing so could prejudice the investigation. While internal discussions about the customer are permitted, neither the customer nor their associates should be made aware that the customer may be under investigation.

This means that no employee of the Company:

- Can inform a customer that a transaction is being delayed because a report is pending approval (consent) from the FIU;
- Can disclose to the customer that law enforcement is conducting an investigation.

7. Internal Control

7.1. Introduction

The Company has a number of internal controls and general procedures that will be used on a day-to-day basis to manage and run the business's daily operations and prevent money laundering and terrorist financing.

7.2. Recordkeeping

The Company retains all documents and data collected or obtained during the due diligence process, including:

- All data and information used to identify and verify customers (such as document type, number, issuing authority, etc.);
- All records (receipts) relating to transactions, i.e., winnings paid out or refunds to customer accounts;
- All documents and records used in preparing the risk analysis, the risk analysis itself, including results of the risk assessment, and documentation on the appropriateness of the measures taken based on these results;
- Results of internal investigations, and communications with the FIU and regulators;
- Documents collected as part of due diligence on business partners;
- Documents collected from employees as part of due diligence;
- Documents related to AML training, such as training materials and examination results.

Additionally, the Company retains all documents created and processed in connection with suspected money laundering or terrorist financing, including:

- All related internal and external correspondence;
- File and interview notes;
- Results of internal investigations and the actions taken, explaining the reasoning behind the money laundering officer's decisions and subsequent actions.

The retention period for these documents is five years, starting from the end of the calendar year in which the business relationship ends or, in other cases, the year in which the relevant information was obtained. Applicable legislation may extend this retention period.

After the retention period expires, the Company will destroy all collected documents and data unless other recordkeeping or retention obligations apply, but no later than ten years.

7.3. Money Laundering Reporting Officer

The Company has appointed a Compliance Officer whose primary responsibility is to review internal reports of unusual or suspicious transactions and, when necessary, submit a Suspicious Activity Report (SAR) to the FIU. The Compliance Officer also serves as the main point of contact for the FIU.

To ensure the Compliance Officer can effectively fulfil their role, the Company guarantees that:

- The Compliance Officer acts independently, is knowledgeable about the Company's activities, and can independently decide whether to escalate internal reports to the FIU;
- The Compliance Officer has no conflicting responsibilities that could pose a conflict of interest;
- The Compliance Officer is provided with sufficient time, resources, and information to fulfil their duties;
- The Compliance Officer has the authority to assign tasks to relevant employees and make decisions related to ML/TF prevention;

- The Compliance Officer and their deputy are responsible for the following functions, among others:
- Drafting and continually developing the internal risk analysis, covering the full scope of risks related to money laundering and terrorist financing;
- Developing and updating internal policies and procedures aimed at preventing money laundering and terrorist financing;
- Establishing uniform reporting channels;
- Participating in the creation and further development of internal organizational and operational procedures related to implementing anti-money laundering and counter-terrorist financing regulations;
- Ensuring compliance with current AML regulations and other relevant legislation;
- Continuously monitoring the Company's business activities to ensure compliance with money laundering regulations;
- Ensuring that CDD/EDD is carried out;
- Conducting risk assessments related to suspicious activity;
- Submitting SARs when appropriate;
- Contributing to the development of staff AML training content;
- Maintaining records of inquiries from law enforcement agencies and internal/external disclosures;
- Submit reports to management on the Compliance Officer's activities, the Company's risk situation, and the measures taken or planned to meet AML obligations;
- The Compliance Officer and their deputy are authorized, within the scope of their duties, to:
 - Perform their tasks independently and effectively;
 - Submit legally binding declarations on behalf of the Company and represent it externally in relevant matters;
 - Provide Company-specific instructions on all matters relating to the prevention of money laundering and terrorist financing;
 - Conduct random checks without restriction.

7.4. Training

The Company provides training to all staff, either directly or through a service provider, upon joining the Company and annually thereafter.

Training materials will be specifically prepared for each team, aligned with the Company's policies, which are developed according to applicable legislation and guidelines.

Training will be conducted as follows:

- Training materials will be based on the finalized and approved Company policies and presented as documents and presentations;
- Training will be provided to current management and staff, either in a classroom setting or online;
- Training will also be included as part of the onboarding process for all new staff;
- After training, employees will complete a questionnaire to assess their understanding;
- If any issues remain unclear, the Company will repeat the training, focusing on areas that need further clarification;

- Regular refresher training will be provided, covering updates and addressing any shortfalls identified during the previous period;
- Any updates in policy will be communicated via group email and ad-hoc training, and included in periodic training updates and materials;
- Staff training will focus on raising awareness of the following:
 - All applicable legislation;
 - Provisions related to money laundering and terrorist financing requirements;
 - Staff's personal obligations under money laundering and terrorist financing laws;
 - Applicable internal reporting procedures;
 - The Company's policies and procedures for preventing money laundering and the financing of terrorism;
 - Identification and verification procedures, record-keeping, and other relevant processes;
 - Recognition and handling of suspicious transactions;
 - Staff's personal liability for failing to report information or suspicions in accordance with money laundering and terrorist financing requirements and internal procedures;
 - New developments, including current techniques, methods, and trends in money laundering and terrorist financing;
 - Money laundering and terrorist financing risks faced by the Company;
 - The risks and controls related to any new or developing technologies or products;
 - Data protection regulations.

Induction training will be provided for all employees and will include training on fraud prevention, detection, and other relevant areas as required for their role. Refresher training will be regularly conducted, as well as when needed, to keep staff informed of the Company's policies, procedures, and any updates or improvements.

The Money Laundering Officer is responsible for keeping records of all training sessions, documenting what training was provided, when, by whom, and when the next training is scheduled. Should any changes to the Company's policies, procedures, or relevant legislation occur, all staff will receive updated training.

7.5. Employee background check

Before engaging employees, the Company will conduct relevant integrity checks based on the employee's position, responsibilities, and access levels. The Company will not employ individuals who are not considered fit and proper for their role.

For this purpose, the Company may request the following documents (while ensuring compliance with data protection regulations):

- A valid original identity document;
- CV (Curriculum Vitae);
- Any other documents the Company deems necessary.

Once employed, employees will be screened on an ongoing basis as needed. All employees must adhere to applicable legislation, fulfil due diligence obligations, report any information relevant to money laundering, and ensure they do not engage in or facilitate suspicious transactions, either actively or passively.

Senior management will regularly conduct checks on employees or whenever deemed necessary by the Company. These inspections, particularly when suspicion arises regarding an employee's behavior, may be carried out through surprise spot checks or other procedures to verify compliance with the Company's policies and procedures.

The frequency and scope of screening will be proportionate to the employee's risk level, which will be determined on a case-by-case basis, depending on factors such as their position (e.g., department head, senior, mid-level), responsibilities, and obligations.

All employees will be checked at least once per year. The Company will use an employee performance sheet for this purpose.

7.6. Technological developments risk assessment

This section of the AML policy ensures that the Company proactively assesses and mitigates money laundering (ML) and terrorist financing (TF) risks associated with new technologies, products, services, or delivery mechanisms before implementation.

These conditions apply to all departments and personnel involved in the development, approval, or deployment of:

1. New products or services;
2. New business practices;
3. New delivery mechanisms;
4. New or developing technologies.

The assessment must:

1. Identify potential ML/TF risks associated with the innovation;
2. Evaluate existing controls and whether they sufficiently mitigate the identified risks.

Each risk assessment must be reviewed by the Compliance Officer and retained for a minimum of five (5) years.

No new product, practice, delivery mechanism, or technology may be launched without approval of the documented risk assessment by the Compliance Officer.

7.7. Internal and external audit and staying up-to-date

The Company has developed its policies and procedures in accordance with applicable legislation and the guidance of the FATF, CGA, and FIU. However, both regulatory requirements and external fraud trends are subject to change. To ensure the ongoing

relevance of the Company's internal AML documentation, the following measures have been implemented:

- Key personnel have subscribed to mailing lists from the FIU, CGA, and FATF and have joined relevant forums to stay informed.
- The Company periodically consults gambling industry specialists for legal advice on AML best practices;
- In the event of an update, the Company will take the following actions as necessary:
 - Update internal policy documentation and training materials;
 - Notify relevant staff via email of any updates, meet with team managers, and ensure they inform their teams appropriately;
 - Update email communication templates and chat canned response;
 - Update website policies, maintaining version numbers and "last updated" dates;
 - Update the Terms and Conditions, maintaining a version number and 'last updated' date.

Any updates to the Terms and Conditions will trigger a pop-up notification for players upon their next login, requiring them to accept and agree to the new version before proceeding.

The Company may also engage a third-party service provider specialising in AML compliance to conduct independent external reviews of its AML policies and procedures. The results of these reviews will be reported to senior management and used to enhance the Company's AML/CTF measures and documentation as needed. The frequency of these external reviews will be determined by senior management. They may occur annually or more frequently, depending on the need for updated assessments of the AML program's effectiveness.

7.8. Version Control

The Company is continuously enhancing its policies to combat Money Laundering and the Financing of Terrorism. Version control and formal approval by the director for any updates are required to track changes effectively and ensure proper oversight.