

Evelnex B.V.

**Anti-Money Laundering
(AML) Policy**

Version 2.0

A handwritten signature in blue ink, located in the bottom right corner of the page. The signature is stylized and appears to be a cursive or semi-cursive script.

1. Overview

1.1. Introduction

Money laundering is the act of concealing or disguising the origins of criminally derived property to make it appear legitimate. This process typically involves three stages:

1. **Placement:** Introducing illicit funds into the financial system, for example, by "smurfing" (making many small deposits) or blending them with legitimate revenue.
2. **Layering:** Obscuring the audit trail by executing complex layers of financial transactions (such as multiple bank transfers or investing in cash-based businesses) to distance the money from its criminal source.
3. **Integration:** Re-introducing the laundered funds into the economy as apparently legitimate assets, such as through property or business investments.

Terrorist financing (TF) is the provision or collection of funds—from either legitimate or illegitimate sources—with the intention or knowledge that they will be used to support terrorist acts or organizations.

While the methods of moving funds are similar, the key difference is that money laundering *always* involves funds from criminal proceeds, whereas the funds for terrorist financing can be from any source. Both activities seek to disguise the source and destination of the funds.

Evelnex B.V. has established robust internal controls and security measures to prevent, detect, and report money laundering and terrorist financing. These measures are designed to identify high-risk customers and detect suspicious activities, including the predicate offenses associated with ML/TF.

1.2. Management

Evelnex B.V. is a limited liability company incorporated under the laws of Curaçao (company number 164180), with its registered office at Kaya Richard J. Beaujon Z/N, Curaçao (referred to as "the Company"). In accordance with Art. 5g of the NOIS, the Company has appointed a designated Compliance Officer.

This policy is mandatory for all employees, senior management, and outsourced staff whose responsibilities involve anti-money laundering, responsible gambling, or anti-fraud procedures.

The Compliance Officer is the key individual with overall responsibility for the Company's ongoing regulatory compliance and the effective implementation of its AML/CFT procedures. The Compliance Officer is responsible for defining and managing the processes needed to prevent fraud and financial crime, based on the following principles:

- The Company operates on the assumption that most customers are not money launderers. However, it applies a risk-based approach to identify all players as required by regulation.
- The Company monitors all transactions and customer activity.
- The Company continuously monitors its customer base, as well as its own risks and processes.



The Company ensures that all relevant employees receive comprehensive training on AML and CTF policies, with a strong emphasis on identifying and escalating risks. Competency tests on this subject are mandatory for relevant staff.

1.3. Legal Framework

The Company's AML/CFT policies and procedures are designed to ensure full compliance with all relevant applicable legislation, including but not limited to:

- 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 (The 4th AML Directive)
- EU-Directive 2018/843 (The 5th AML Directive)
- EU-Directive 2018/1673 (On combating money laundering by criminal law)
- The National Ordinance on Games of Chance
- The Curaçao Gaming Authority Guidelines
- The Financial Action Task Force (FATF) Recommendations

1.4. Risk-Based Approach

The Company employs a comprehensive risk-based approach (RBA) to prevent and combat money laundering and terrorist financing. This RBA framework involves four key components:

1. **Risk Identification and Assessment:** Identifying and assessing the specific ML/TF risks the Company faces based on its customer profiles, products, services, and operational jurisdictions.
2. **Risk Mitigation:** Implementing appropriate controls, policies, and procedures to effectively mitigate the identified risks.
3. **Risk Monitoring:** Utilizing management information systems (MIS) to continuously monitor the Company's risk profile and adapt to new or evolving threats.
4. **Documentation and Accountability:** Maintaining comprehensive documentation of all risk assessments, strategies, and procedures, while ensuring effective accountability from senior management.

1.5. Data Processing System

The Company utilizes an internal data processing system designed to detect high-risk scenarios and support its day-to-day AML/CFT operations. This system includes the following mechanisms:

- Manual identification and verification of all users, carried out by the internal KYC (Know Your Customer) team before establishing a business relationship.



- Automated screening of all customers against Politically Exposed Person (PEP) and international sanctions lists using relevant software.
- Transaction monitoring conducted by trained AML staff.
- Clear internal reporting procedures for all suspected ML/TF cases to the Compliance Officer and, where required, the Financial Intelligence Unit (FIU).

The Company is committed to monitoring emerging ML/TF trends and will continuously update its internal procedures to address new and evolving risks.

1.6. Staff Training

All relevant staff and outsourced teams must complete mandatory AML/CFT training upon hiring and on an annual basis thereafter. This training is designed to ensure a thorough understanding of all associated policies and procedures.

Training may be delivered via online modules, in-person sessions conducted by external providers, or by qualified internal specialists. The scope and intensity of the training are tailored to the specific roles and risk-exposure levels of the employees.

A handwritten signature in blue ink, consisting of a stylized 'S' or 'B' shape with a long horizontal stroke extending to the right.

2. Customer Acceptance and Registration Policy

2.1. Introduction

To be eligible to deposit funds, place real-money stakes, or gamble on the Company's platform, an individual must first successfully register a customer account. Access to gambling activities is not permitted for unregistered users.

This policy outlines the criteria for customer acceptance, details the mandatory registration process, and defines the conditions under which the Company may decline a potential customer.

2.2. Customer Acceptance

A customer must complete all registration steps on the Company's site before they can deposit funds or engage in gameplay.

- Eligibility for registration is strictly limited to individuals aged 18 years or older.
- The Company enforces a "one account per person" policy. To prevent individuals from circumventing AML thresholds by operating multiple accounts, we utilize automated checks to detect and block duplicate registrations based on email address, mobile number, device identifiers, and other data combinations.

2.3. Restrictions

The Company will not permit registration, or will close existing accounts, for the following individuals:

- **Underage Persons:** Individuals under 18 years of age are strictly prohibited from registering.
- **Sanctioned or High-Risk Individuals:** This includes:
 - Individuals identified as Politically Exposed Persons (PEPs).
 - Individuals under sanctions or listed on any of the following official blacklists:
 - *Al-Qaida c.s., the Taliban of Afghanistan c.s., ISIL c.s., ANF c.s."*
 - *Australian Sanctions (AU)*
 - *Bureau of Industry and Security - Entity List (US)*
 - *Bureau of Industry and Security - Unverified List (US)*
 - *Bureau of Industry and Security (US)*
 - *Canada, Office of the Superintendent of Financial Institutions, OSFI Consolidated*
 - *CIA Leader list*
 - *Consolidated Canadian Autonomous Sanctions List*
 - *Department of State, AECA Debarred List (US)*
 - *Department of State, Non-proliferation Sanctions (US)*



- *EU Financial Sanctions (EU)*
- *European Union, Consolidated list of persons, groups and entities subject to EU financial sanctions*
- *Foreign Financial Institutions Subject to Part 561 (the Part 561 List)*
- *Foreign Sanctions Evaders List (FSE)*
- *INTERPOL Wanted List*
- *Islamic Republic of Iran*
- *Libya Sanctions*
- *Non-SDN Iranian Sanctions Act List (NS-ISA)*
- *OFAC Consolidated Sanctions List*
- *Office of the Superintendent of Financial Institutions (Canada)*
- *Palestinian Legislative Council (PLC) List*
- *Sectoral Sanctions Identifications (SSI) List*
- *Specially Designated Nationals (OFAC)*
- *Specially Designated Nationals List (SDN)*
- *Switzerland Sanction List (SECO)*
- *U.S. Department of Commerce, Bureau of Industry and*
- *Security - Denied Persons List*
- *U.S. Department of the Treasury, Office of Foreign*
- *Assets Control (OFAC)*
- *UK Financial Sanctions (UK)*
- *UK, Consolidated Financial Sanctions list (HMT)*
- *United Nations Sanctions (UN)*
- *United Nations Security Council (UN), Consolidated Sanctions list*
- *US Consolidated Sanctions (US)*
- *US State Dept. WMD Non-Proliferation List*
- Individuals who are currently under an active self-exclusion or company-issued exclusion on the site.
- Individuals who exhibit significant red flags associated with fraudulent activity.
- **Multi-Account Holders:** As stated in section 2.2, individuals attempting to open or operate more than one account will be blocked.

2.4. Information Collected at Registration

During the registration process, and potentially at later stages, the Company will collect the following mandatory identification and contact details:

- First Name and Last Name
- Date of Birth
- Gender
- Full Address and Country of Residence
- Email Address and Mobile Number
- A unique Username and secure Password

2.5. Acceptance of Terms

As a non-negotiable step in the registration process, all customers must formally confirm their acceptance of the website's general Terms and Conditions and its Privacy Policy.

2.6. Underage Customers

The Company's systems are designed to prevent the registration of underage individuals. A customer must be at least 18 years old or of the legal age for gambling in their territory to register. The Date of Birth provided at registration is cross-checked against official identification documents during the Customer Due Diligence (CDD) process.

2.7. Customer Due Diligence

Successful completion of the Company's Customer Due Diligence (CDD) process is a prerequisite for finalizing registration. If a customer fails the required CDD checks, their registration will be declined.

3. Customer Risk Scoring and Profiling

3.1. Introduction

As part of its comprehensive risk-based framework, the Company conducts risk profiling for all customers, commencing at the point of registration, to assess their potential for money laundering or terrorism financing (ML/TF) risk.

The Company's policies and procedures are formulated based on:

- Current legal and regulatory requirements;
- Official guidance provided by the GCB and FIU;
- The Company's own internal evaluation of its business risk, informed by knowledge and experience with its customer base.

3.2. Customer Risk Assessment

The Company performs an initial risk assessment for every customer based on the information supplied at registration (e.g., home address, location, age, PEP/sanctions status). This assessment categorizes the customer as **Low**, **Medium**, or **High** risk for ML/TF, a categorization that dictates future monitoring and handling.



Customer risk assessments are dynamic and are reviewed regularly, especially when new information becomes available. The assessment is based on:

- Individual status (PEP, sanctions, adverse media)
- Geographical location
- Gambling and transactional behavior
- Payment methods used
- Fraud red flags

Customers who are classified as **High Risk** will automatically be subject to Enhanced Due Diligence (EDD).

3.2.1. Individual Status

- **PEP (Politically Exposed Person):** An individual who has been entrusted with a high-ranking public function (nationally or internationally). Any new or existing customer identified as a PEP, or a known relative of a PEP, will have their account registration rejected or their existing account closed.
- **Sanctions List:** Any new or existing customer found on any government or international sanctions database will have their account registration rejected or their existing account closed.
- **Adverse Media:** This refers to negative public information that may expose a customer's involvement in criminal activity. Any new or existing customer who is the subject of relevant adverse media will be escalated for EDD, which may result in account rejection or closure.

3.2.2. Geographical Location

If a customer is found to reside in a "High-Risk Country," they may be subject to EDD. High-Risk Countries are jurisdictions identified by bodies such as the FATF as having strategic deficiencies in their AML/CFT regimes (<https://www.fatf-gafi.org/en/countries/black-and-grey-lists.html>).

The Company also utilizes a geo-blocking tool to restrict service access from prohibited countries (listed in Appendix 1).

3.2.3. Gambling and Transactional Behaviour

All player activity is constantly monitored for behaviors indicative of both problem gambling and money laundering. Observed behaviors are allocated scores that contribute to the customer's overall ML/TF risk profile.

If any overt ML/TF behaviors are observed, EDD must be initiated immediately, followed by the Suspicious Activity Report (SAR) process if necessary.

3.2.4. Payment Methods

The risk level of a payment method is determined by its transparency:

- **Low Risk:** Methods where the origin of funds is traceable and funds can be returned to the source (e.g., bank transfers, debit cards).



- **High Risk:** Methods that are cash-funded, anonymous, or do not allow funds to be returned to the source.

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

Manipulating payment methods (e.g., depositing via one method and withdrawing via another) is also considered a high-risk indicator.

3.2.5. Fraud Red Flags

The Company's anti-fraud system is designed to prevent fraudulent activities, including bot attacks, account takeovers, identity theft, and multi-accounting. As these fraud indicators often overlap with ML/TF risks, any player triggering a significant fraud red flag will automatically be subject to EDD.

3.3. Risk Score Calculation

This procedure is designed to aggregate minor behavioral incidents that may not be suspicious in isolation but can indicate risk when combined. The internal CMS system assigns a risk score to each player based on the factors above.

The specific factors, scores, and thresholds are internal, confidential, and subject to regular review and adjustment to improve the Risk Score (RS) Calculation model.

Indicator	Description	Score
individual status		
PEP	A customer considered to be PEP	100
Adverse media	A customer was mentioned in negative news or information the company discovered from various sources	50
Sanctions/blacklist	A customer is under international sanctions/blacklists	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 depositing large sums, then places minimal stake bets, then withdrawing 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 of volume and size of player deposits or staking activity	20
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 no objective reasons	30
Spending above wages	A customers spend is outside of their affordability	20
No withdrawals	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	Customer used a VPN	30

Not all risk factors can be automatically included in the calculation for technical reasons. These risks are monitored through other processes. For example, VPN usage and multi-accounting are checked at registration, alerts are set for third-party card usage, and all withdrawals are manually reviewed.

3.4. Customer Due Diligence Level

The level of CDD conducted on a player corresponds directly to their assigned risk category:

	Low	Med	High
Verify ID and address with docs	X	X	X
Collect additional personal details		X	X
Collect 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

A daily report is sent to the Compliance Officer, listing all players newly classified as medium/high risk or those escalated from medium to high.

The designated AML manager will then:

1. **Review** all accounts on the report, which includes:
 - Checking existing customer information.
 - Conducting open-source internet checks.
 - Assessing for any suspicious activity.
2. **Take appropriate action**, such as:
 - Blocking the account if necessary.
 - Applying the required level of Due Diligence.
 - Reviewing the player's responses and provided information.
3. If the player **fails to reply** to requests within 14 days, or if the response is unsatisfactory, the account will be blocked. A delay in providing documents may itself be considered suspicious.

All decisions and actions taken by the AML manager must be clearly documented.

Furthermore, any withdrawal request from an account classified as medium or high risk requires AML approval before it can be processed.

3.6. On-Going Monitoring

The AML team conducts ongoing monitoring of all accounts on a risk-sensitive basis. This includes:

- Obtaining fresh identification documents when existing ones expire.
- Questioning and resolving any inconsistencies identified in a player's data.
- Reviewing and updating customer information periodically, with frequency based on risk level.

3.7. Withdrawals

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

- If a player is classified as medium or high risk, the Verification Team will re-review all documentation to ensure it is still valid.
- If any documents have expired, new documents will be requested before processing the withdrawal.

Therefore, any withdrawal request by a player flagged as medium or high risk, or any request otherwise flagged as high risk, requires explicit approval from the AML team before it is processed and paid.



4. Customer Due Diligence

4.1. Introduction

The Company's due diligence framework is divided into two distinct levels: **Standard Customer Due Diligence (CDD)** and **Enhanced Customer Due Diligence (EDD)**.

Customers are obligated to cooperate fully with all due diligence requests and provide any required information or documentation.

If the Company cannot complete the necessary due diligence measures, a business relationship will not be established. If a relationship already exists, it will be terminated, and no further transactions will be permitted. In such cases, the Company will also assess the necessity of filing a Suspicious Activity Report (SAR).

4.2. Standard Customer Due Diligence (CDD)

Standard CDD measures are applied to all customers at the registration stage. This process involves two key steps:

1. **Identification:** Collecting the customer's personal data.
2. **Verification:** Confirming the customer's identity by validating their data against reliable, independent source documents.

To meet these requirements and prevent money laundering, the Company collects and verifies the following:

- Full Name (First and Last)
- Date of Birth
- Full Residential Address (street, number, ZIP code, city)
- A copy of an official Identification Document (ID)
- A copy of a Proof of Address (POA) document

4.3. Document Acceptance Criteria

To verify a customer's **identity**, the Company requires a valid, government-issued photographic document. Acceptable documents include:

- Current, signed passport
- Valid driving license
- National identity card
- Official travel document

To verify a customer's **address (POA)**, the Company accepts:

- A utility bill (for a service installed at the residence) issued within the last 6 months.
- Correspondence from a central or local government authority (e.g., tax notice) issued within the last 6 months.



- A current, valid lease agreement.

All submitted documents must be **valid (not expired)**, **clear**, and **legible**. Mobile phone bills are not accepted as proof of address.

4.4. Threshold Approach for EDD

The Company is required to apply Enhanced Due Diligence (EDD) measures when a customer's transactions meet or exceed **EUR 2,000**, whether this occurs in a single operation or through several operations that appear to be linked.

A "transaction" in this context includes:

- The deposit of funds for the purpose of gambling.
- The collection of winnings.
- The withdrawal of funds (either deposited funds or winnings).

Transactions are considered "linked" if they occur during a single login session. However, the Company also actively monitors for other linking patterns, such as a customer deliberately splitting transactions (smurfing) to circumvent this CDD threshold. When this EUR 2,000 threshold triggers EDD, the Company will apply verification measures using a risk-based approach.

4.5. Ongoing Monitoring

Due diligence is a continuous process, not a one-time check. The Company conducts ongoing monitoring of all business relationships, which includes:

- Scrutinizing transactions to ensure they are consistent with the Company's knowledge of the customer and their risk profile.
- Periodically reviewing and updating customer data and information.
- Requesting fresh identification documents when existing ones expire.
- Investigating and resolving any inconsistencies in customer data that may arise.

To ensure all customer information is current, the Company re-applies its CDD procedure at a minimum of **every 6 months** for all verified customers, and more frequently on a risk-sensitive basis.

4.6. Enhanced Due Diligence (EDD)

Enhanced Due Diligence (EDD) involves applying additional, more stringent measures to manage and mitigate scenarios that present a higher risk of money laundering or terrorist financing.

EDD is applied in addition to standard CDD measures when specific high-risk triggers are met, including:

- Any situation identified by the Company or by authorities as high-risk.
- Doubts arise regarding the accuracy or authenticity of previously collected customer information.



- A customer is identified as a Politically Exposed Person (PEP), a family member, or a close associate of a PEP.
- A customer is found to have provided false or stolen identification documents.
- A transaction is complex, unusually large, or displays an unusual pattern with no apparent economic or legal purpose.
- A customer requests to withdraw funds to a different payment account than the one used for deposits.
- Any other case which, by its nature, presents a high risk of ML/TF.

Approval from the **Compliance Officer** is mandatory to establish or continue a business relationship with any customer deemed high-risk.

When EDD is triggered, the Company will undertake one or more of the following actions, as appropriate:

- **Re-verification** of the customer's identity (repeating the CDD process).
- **Establishing the Source of Wealth (SoW)** to understand how the customer acquired their total wealth. Evidence may include:
 - Salary (Certified payslips or employer letter)
 - Sale of property (Certified contract of sale or solicitor's letter)
 - Inheritance (Certified copy of a will)
 - Sale of a company (Certified contracts or accountant's letter)
- **Establishing the Source of Funds (SoF)** to verify the origin of the specific funds being used for transactions.
- Requesting **bank or account statements** to ensure deposits do not originate from anonymous sources.
- Applying **increased and more frequent monitoring** of the business relationship.
- Investigating the specific suspicious transaction in detail.

The primary goal of EDD is to ensure the transparency of payment flows, making the origin and destination of funds traceable to a legitimate account.

- **Defining Source of Funds (SoF):** This refers to the origin of the specific funds being deposited on the Company's website. It requires substantive information establishing where the funds came from and how they were acquired.
- **Defining Source of Wealth (SoW):** This refers to the origin of the customer's entire body of wealth (total assets), providing a picture of how it was accumulated and its approximate volume.

4.7. Politically Exposed Persons (PEPs) and Sanctions Screening

The Company utilizes an automated KYC software tool to screen all new customers against PEP and Sanctions databases at the point of registration. Furthermore, the entire existing customer database is re-screened every six months to identify any changes in status.

Any new or existing customer identified on a **Sanctions list**, or identified as a **PEP** (or a known relative of one), will have their registration **rejected** or their existing account **closed**.

Internal PEP Procedure: If a potential PEP is identified, the responsible staff member will report it to the Compliance Officer. The Compliance Officer will investigate the case (requesting additional documents if necessary) to distinguish between a false-positive and a true-positive alert. If the alert is a true-positive, the Compliance Officer will reject the registration or close the account and formally notify senior management of 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, of 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 attachés,
- 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 organisation.

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 and
- both parents.



The Company actively blocks registrations and access from countries identified by the FATF as high-risk ("blacklisted" or "grey-listed"). (<https://www.fatf-gafi.org/en/countries/black-and-grey-lists.html>)

4.8. Procedure for Account Closure

While an account may be closed for numerous reasons (e.g., Fraud, Cheating, Bonus Abuse, Underage Gambling, Problem Gambling, or Terms & Conditions breaches), this policy is specifically concerned with closures related to ML/TF.

ML/FT-Related Closures: If the Company knows or suspects a customer is involved in money laundering or terrorist financing, the law requires the business relationship to be terminated, unless specific consent to continue has been obtained from authorities (which is rare).

Tipping-Off Restriction: Due to strict anti-tipping-off laws, the Company **cannot** inform a customer that their account is being closed or investigated due to ML/TF concerns. This process must be handled sensitively to avoid alerting the individual. The Compliance Officer will manage this, considering any SAR (Suspicious Activity Report) submissions.

Closure Due to CDD Failure: If the Company is unable to complete its required CDD measures for a customer (either at the outset or during ongoing monitoring), the Company **must** cease all transactions, terminate the business relationship, and block the account.



5. Deposit and Withdrawal Management Procedures

5.1. Player Account Balance

Each registered player is assigned a secure personal account (or "wallet"). This account is credited with all funds deposited by the player and all winnings owed to them by the Company.

A player may deposit additional funds into their account at any time via the site's cashier, and these funds are then available for placing bets. All stakes are deducted from this balance, and all winnings are added to it.

A player may request a withdrawal of any available, cleared funds from their balance.

The following rules are strictly enforced:

- The Company **does not offer credit** to any player.
- Player-to-player account transfers are **strictly prohibited**.

5.2. Payment Methods

The Company will only accept payments from and make payments to accounts held with licensed financial institutions or through licensed payment providers.

The Company **strictly prohibits all cash transactions**. No cash deposits or cash withdrawals will be processed.

5.3. Player Deposits

Once registered, a player can deposit funds into their account using the integrated cashier on the site.

To facilitate this, the Company utilizes several third-party payment gateways. All integrated gateways are fully **PCI DSS compliant**, and the Company **does not store any credit card data** on its own systems.

The deposit process is as follows: the Company securely submits the transaction to the Payment Service Provider (PSP) and awaits approval from the acquirer or e-wallet. Upon receiving approval, the transaction status is updated, and the funds are credited to the player's account balance.

5.4. Player Withdrawals

A player may request a withdrawal of any available funds in their balance by accessing the site's cashier.

The player must enter the desired withdrawal amount and select an available payout method. The requested amount is then deducted from the player's active balance pending review and approval.

5.5. Withdrawal Payouts (Closed-Loop Policy)

As a key AML control, the Company's primary policy is to remit funds back to the original source from which the deposits were made.



In cases where it is not technically possible to return funds to the originating account, the payout will be processed in an alternative manner, in strict compliance with all applicable AML legislation.

A handwritten signature in blue ink, consisting of a stylized, cursive 'S' or 'B' shape with a long, sweeping tail.

6. Suspicious Activity Reporting

6.1. Introduction

All Company employees, regardless of their role, are mandated to immediately report to the Compliance Officer any activity they know or suspect to be related to money laundering, terrorist financing, or the use of criminal proceeds on the Company's platform.

The Compliance Officer is responsible for evaluating every internal report. If this review confirms that the activity provides reasonable grounds for knowledge or suspicion, the Compliance Officer must then submit a formal Suspicious Activity Report (SAR) to the Financial Intelligence Unit (FIU Curaçao).

- **Knowledge** implies a direct, factual awareness that an event is occurring.
- **Suspicion** implies a concern based on observed facts that are unusual, unexpected, or lack a clear commercial or financial rationale, even after initial inquiries.

The obligation to report is not limited to the time of the transaction. If suspicions arise at a later date, or if an initial concern escalates into a clear suspicion following further investigation, the duty to report to the FIU is triggered at that point. The Compliance Officer will assess all circumstances and may pose further questions to the customer to make a determination.

6.2. Red Flag Indicators

A "red flag" is an indicator of potential risk; it does not automatically equate to suspicion or mandate a SAR. Instead, red flags are warning signs that require the Company to question the customer's behavior. If the customer's activity lacks a reasonable, legitimate explanation, an internal report to the Compliance Officer is mandatory.

Common red flags include, but are not limited to:

- Refusal or failure to cooperate with CDD/EDD information requests.
- Attempts to register or operate multiple accounts on the same site.
- Depositing significant funds, followed by minimal or no wagering, and then requesting a large withdrawal.
- A pattern of frequent deposits and withdrawals that lacks a logical explanation.
- Sudden, significant changes in gaming patterns, such as a large increase in transaction volume.
- Inquiring about the possibility of transferring funds between accounts.
- Conducting transactions that appear disproportionate to the customer's known financial profile, wealth, or income.
- Requesting a fund transfer to a bank account held in a third party's name.
- Requesting a withdrawal to a new account that was not the source of any deposits.
- Registering multiple different payment cards and making transfers between them.
- Depositing and losing large amounts repeatedly, demonstrating an apparent indifference to significant financial loss.



6.3. Inability to Complete CDD Measures

A customer's refusal to provide CDD/EDD documentation is not, in isolation, automatically considered grounds for suspicion of ML/TF.

The Company will evaluate the refusal in the full context of the customer's profile, including their payment methods, gaming activity, jurisdiction, and any available open-source information. A SAR must be submitted only if the *totality* of these factors, including the refusal, gives rise to a valid suspicion.

6.4. Internal Suspicious Activity Report

All employees must report suspicions immediately to the Compliance Officer using the approved **Internal Suspicious Activity Report Form**.

This duty to report is absolute. An employee must submit the report even if their direct supervisor disagrees with their suspicion. The Compliance Officer is the sole individual responsible for determining if the information warrants an external SAR.

The Internal SAR must include:

- The customer's full details.
- A clear statement from the staff member explaining the grounds for their suspicion.
- All relevant supporting documentation and information.

Upon receiving an internal report, the Compliance Officer will:

1. Acknowledge receipt and investigate the matter further.
2. Assess all available information to decide if an external report to law enforcement is warranted.
3. If warranted, submit the SAR to the FIU.
4. Record the decision and inform senior management.

6.5. External Report to FIU

After receiving an internal report, the Compliance Officer conducts a final assessment to determine if an external SAR is required. This decision considers that AML legislation targets serious crime, which typically involves significant amounts or a clear intent to circumvent financial safeguards.

For example, while identity fraud or chargebacks are criminal acts, they may only become a reportable ML event if the *proceeds* of that fraud are deposited with or held by the Company. The Company does not typically report isolated, small-value incidents, but rather looks for larger patterns or schemes (e.g., related persons, common IP addresses).

To finalize the decision, the Compliance Officer should seek to answer: Who is involved? What is the value and nature of the criminal property? Where is it? When did/will this happen? How did it arise? and Why is it suspicious?

6.6. Reporting Procedure



The Company is legally obligated to submit a SAR to the FIU (via its online portal) "without due delay" if there are indications of:

- Known or suspected money laundering and/or terrorist financing.
- Assets originating from a predicate criminal offense.
- Any transaction or asset related to terrorist financing.

The decision to report considers all factors, including the transaction's purpose, the customer's background, and the origin of the assets.

The Company's policy is to **halt** suspicious transactions. An exception is made only if halting the transaction is impossible or would obstruct a criminal prosecution, in which case the SAR is filed *immediately* after the transaction.

6.7. Tipping-Off

It is a serious criminal offense to "tip-off" any person by disclosing that a SAR has been filed, is being considered, or that an investigation is underway. Such a disclosure is prohibited as it is likely to prejudice an investigation.

While internal discussion among relevant staff (e.g., with the Compliance Officer) is necessary, no one at the Company may, under any circumstances, give a customer or their associates any indication that they are under scrutiny.

This means no employee can:

- Tell a customer a transaction is being delayed because a report is awaiting clearance from the FIU.
- Tell a customer that law enforcement is conducting an investigation.



7. Internal Control

7.1. Introduction

To effectively prevent money laundering and terrorist financing, the Company has integrated a comprehensive suite of internal controls and general procedures into its daily business operations and management.

7.2. Recordkeeping

The Company is obligated to maintain comprehensive records of all data and documentation obtained through its due diligence, compliance, and operational activities. These records include:

- **Customer Identification:** All data used to identify and verify customers (e.g., document type, number, issuing authority).
- **Transaction Records:** Complete records of all customer transactions, including deposits, wagers, winnings paid out, and refunds.
- **Risk Analysis:** All documentation related to the creation and execution of the risk analysis, including assessment results and the justification for measures taken.
- **Investigations:** Records of internal investigations, communications with the FIU, and all regulatory correspondence.
- **Third-Party Due Diligence:** Due diligence documentation for business partners.
- **Employee Records:** Due diligence and background check documentation for all employees.
- **Training Logs:** All AML training materials, attendance records, and examination results.

Specific, confidential records must also be maintained for any case involving a suspicion of ML/TF, including:

- All related internal and external correspondence.
- File notes, interview notes, and internal investigation results.
- Documentation explaining the measures taken and the Compliance Officer's decisions.

Retention Period: The standard retention period for all documents is **five years**, which begins at the end of the calendar year in which the business relationship is terminated (or, for other cases, the year the information was created). This period may be extended if required by applicable legislation.

The Company will securely destroy all documents and data after the retention period expires, but no later than 10 years, unless other legal obligations apply.

7.3. Money Laundering Reporting Officer



The Company has designated a **Compliance Officer** (also referred to as the Money Laundering Reporting Officer) who acts as the central point of contact for the FIU. The Compliance Officer's primary function is to receive, review, and investigate all internal reports of unusual or suspicious transactions and, where necessary, submit a formal Suspicious Activity Report (SAR) to the FIU.

To ensure the effectiveness of this role, the Company guarantees that the Compliance Officer:

- Acts with full independence and autonomy in all AML-related decisions.
- Has no conflicting responsibilities that could create a conflict of interest.
- Is provided with sufficient time, resources, and access to all necessary information to fulfill their responsibilities.
- Is authorized to delegate tasks and make binding decisions regarding ML/TF prevention.

The Compliance Officer's functions include, but are not limited to:

- Developing, documenting, and continuously updating the Company's internal ML/TF risk analysis.
- Authoring and maintaining all internal AML/CFT policies, procedures, and controls.
- Establishing and managing clear and confidential internal reporting channels.
- Ensuring all business operations comply with current AML regulations.
- Overseeing the implementation and effectiveness of all CDD and EDD processes.
- Personally assessing all internal suspicious activity reports.
- Filing SARs with the FIU as required by law.
- Overseeing the content, delivery, and tracking of the staff AML training program.
- Acting as the official liaison for, and logging all inquiries from, law enforcement agencies.
- Providing regular (at least annual) reports to senior management on the Company's risk status, compliance measures, and overall AML program health.

To execute these duties, the Compliance Officer is fully authorized to:

- Operate independently and effectively.
- Represent the Company externally in all relevant AML/CFT matters.
- Issue binding, undertaking-specific instructions regarding ML/TF prevention.
- Conduct unrestricted, random checks to ensure compliance.

7.4. Training

The Company mandates comprehensive AML/CFT training for all staff at the time of hiring and provides a **mandatory annual refresher course** for all employees.



This training program is structured as follows:

- All training materials are based on the Company's approved policies, applicable legislation, and regulatory guidelines.
- Training is delivered to all existing and new staff through online or in-person sessions.
- All training modules conclude with a competency test or questionnaire to ensure full understanding.
- Any areas of misunderstanding identified by the tests will be addressed with focused, repeated training.
- Refresher training incorporates all recent policy updates, new legislation, and emerging ML/TF risk trends.
- Any critical policy updates are communicated immediately to all staff via email or ad-hoc training sessions.

Staff training is designed to ensure full awareness and competence in:

- Current AML/CFT legislation and regulatory requirements.
- Personal legal obligations and liabilities under the law.
- The Company's internal procedure for reporting suspicious activity.
- All internal policies (CDD, EDD, record-keeping, etc.).
- How to recognize and handle suspicious transactions and red flags.
- New developments, techniques, and trends in money laundering.
- The specific ML/TF risks faced by the Company.
- Data protection regulations and responsibilities.

The Compliance Officer maintains detailed records of all training delivered, including the content, dates, provider, and attendee lists.

7.5. Employee Background Checks

The Company conducts mandatory integrity and background checks on all prospective employees prior to engagement. The depth of this check is proportionate to the employee's proposed role, responsibilities, and access levels. The Company will not employ any individual who is not deemed "fit and proper."

- As part of this due diligence, the Company may request a valid original ID, a curriculum vitae (CV), and other necessary documents, in full compliance with data protection laws.
- Screening is an ongoing process. All employees must contractually agree to observe all AML provisions and report relevant facts.



- Management will conduct regular checks, including unannounced spot checks, to ensure employees are complying with all policies. These inspections may be triggered if an employee's behavior raises suspicion.
- The frequency and extent of ongoing screening are risk-based. However, all employees will be subject to a formal review at least once per year.

7.6. Internal and External Revision and Staying Up to Date

The Company recognizes that AML/CFT legislation, guidance, and external threats are constantly evolving. To ensure the Company's policies remain relevant, effective, and compliant, the following measures are in place:

- Key personnel are subscribed to official mailing lists and forums from the FIU, GCB, and FATF.
- The Company periodically retains legal counsel to review and advise on AML best practices.
- When an update is required, the Company will:
 - Update all internal policy documentation and training materials.
 - Formally inform all relevant staff and managers of the changes.
 - Update all communication templates (email, chat).
 - Update all public-facing website policies (Privacy Policy, T&Cs), ensuring a new version number and "last updated" date are present.

Any material change to the Terms and Conditions will trigger a pop-up notification to all players on their next login, requiring their formal acceptance before they can proceed.

Furthermore, the Company may engage independent, third-party service providers to conduct external reviews and audits of its AML policies. The results of these reviews will be reported directly to senior management and used to enhance the AML/CTF program. The frequency of these external audits is determined by senior management on a risk-based basis.

7.7. Version Control

The Company is committed to the continuous improvement of its policies to actively combat Money Laundering and the Financing of Terrorism. All revisions to this policy are tracked, and the Director must approve all changes.

Version	Date	Approved By
2.0	November 5, 2025	 Gouloud Hammoud f/obo Guardian Corporation Curacao BV

Appendix 1

- Afghanistan
- Aland Islands
- American Samoa
- Angola
- Anguilla
- Antarctica
- Antigua and Barbuda
- Barbados
- Belize
- Benin
- Bhutan
- Bonaire (including Sint Eustatius and Saba)
- Bouvet Island
- British Indian Ocean Territory
- Burundi
- Cape Verde
- Central African Republic
- Chad
- Cocos (Keeling) Islands
- Cook Islands
- Comoros
- Congo, Democratic Republic of
- Congo, Republic of
- Crimea
- Cuba
- Curacao
- Djibouti
- Donbas
- Equatorial Guinea
- Eritrea
- Fiji
- French Guyana
- French Polynesia
- French Southern Territories
- Gabon
- Gambia
- Grenada
- Guadeloupe



- Guam
- Guinea
- Guinea-Bissau
- Guyana
- Haiti
- Heard Island and McDonald Islands
- Holy See (Vatican City State)
- Iran
- Iraq
- Ivory Coast (Côte d'Ivoire)
- Kherson
- Kiribati
- Kosovo
- Kyrgyzstan
- Lao People's Democratic Republic
- Lebanon
- Liberia
- Libya
- Macao
- Malawi
- Mali
- Marshall Islands
- Martinique
- Mauritania
- Mayotte
- Micronesia, Federated States of
- Montserrat
- Myanmar
- Nauru
- Netherlands
- New Caledonia
- Niger
- Niue
- Norfolk Island
- North Korea
- Northern Mariana Islands
- Palau
- Palestinian Territory
- Papua New Guinea
- Pitcairn
- Puerto Rico
- Rwanda
- Saint Barthelemy
- Saint Helena
- Saint Kitts and Nevis
- Saint Lucia



- Saint Martin
- Saint Pierre and Miquelon
- Saint Vincent and the Grenadines
- Sao Tome E Principe
- Seychelles
- Sint Maarten
- Sierra Leone
- Solomon Islands
- Somalia
- South Georgia and the South Sandwich Islands
- Sudan (North and South)
- Suriname
- Svalbard and Jan Mayen
- Syria
- Tajikistan
- Timor-Leste
- Togo
- Tokelau
- Tonga
- Turkmenistan
- Turks and Caicos Islands
- Tuvalu
- United States of America
- United States Minor Outlying Islands
- US Virgin Islands
- Uzbekistan
- Vanuatu
- Venezuela
- Wallis and Futuna
- Western Sahara
- Western Samoa
- Yemen
- Zaporizhzhia
- Zimbabwe

A handwritten signature or mark in blue ink, located in the bottom right corner of the page. It appears to be a stylized, cursive signature.