

AML/CTF POLICY

Sena Bet B.V.

Approving Official	Compliance Officer
Responsible Office	Compliance
Effective Date	May 27, 2025
Next Review Date	

1. Policy Statement

Sena Bet B.V. recognizes the importance of preventing money laundering (AML) and terrorist financing (CTF), and is committed to following all current rules and regulations in the operation of its lottery games, gambling and sports betting activities.

2. Purpose

The purpose of this Policy is to provide guidance on the company's approach to combating AML/CTF, in order to ensure full compliance with the relevant legislation

3. Audience

This Policy applies to all employees, as well as to all products and services offered by the company.

4. Definitions.-

For the purposes of this Policy, the following definitions shall apply:

- Compliance Officer A officer independent from the games' operations, responsible for the detection and deterrence of money laundering and terrorist financing.
- Financing of Terrorism: Is the financing of terrorist acts, of terrorists and terrorist organizations. A terrorist act is an act to intimidate a population, or to compel a Government or an international organization to do or to abstain from doing any act.
- Money Laundering: All acts done with money of illegal origin to change its identity so that it appears to have originated from a legitimate source, can be considered money laundering.
- Unusual Transactions: These are transactions whose amount, characteristics, or frequency do not match the customer's profile.
- (Ultimate) beneficial ownership (UBO) Refers to the natural person(s) who ultimately own(s) or control(s) a customer and/or the person on whose behalf a transaction is being conducted.
- Red Flags: Behaviors or specific situations that serve as tools for the company, its employees, and the compliance officer to identify and/or prevent suspicious transactions related to AML/CFT.

5. Policy Implementation

5.1. Business Risk Assessment.

For the purposes of this Policy, AML/CTF risk is defined as the potential for loss or damage that the company may incur as a result of being misused through its operations.

The AML/CTF risk materializes through the following associated risk categories:

- Legal Risk
- Reputational Risk
- Contagion Risk
- Operational Risk

The company has adopted a risk management methodology that defines the procedures for the identification, assessment, mitigation, and monitoring of AML/CTF risks to which it may be exposed. This methodology shall be applied whenever structural changes occur within the organization and shall be documented through the Risk Assessment Report.

The initial phase of this methodology involves the formation of a risk assessment team responsible for identifying and evaluating AML/CTF risks. The team shall begin with an analysis of the operational environment of the company, aimed at compiling an inventory of inherent AML/CTF risks.

Subsequently, existing mitigation controls shall be identified and assessed based on two key criteria: the extent of their coverage and their operational effectiveness. The identified risks will then be subject to a qualitative evaluation, considering both the potential impact and the likelihood of occurrence.

Based on the outcome of this evaluation, the level of residual AML/CTF risk shall be classified as Low, Medium, or High. Finally, appropriate risk response measures shall be defined and implemented, with the objective of minimizing the company's exposure to residual AML/CTF risks.

5.2. Customer Risk Assessment.

Every customer involved in an unusual transaction will be assessed based on the following categories:

- Customer: Variables considered include PEP status, address, nationality, and occupation.
- Product or Service Provided: Variables considered include service channels, betting payment methods, and prize payment methods.
- Geographic Zone (if applicable): Variables considered include the sala's location.

This assessment, based on the variables from the listed categories, allows customers to be categorized into a risk level:

- Low
- Middle
- High

5.3. Customer Acceptance Policy

All customers involved in an unusual transaction, regardless of their risk level, will undergo a customer due diligence procedure.

High-risk customers will be subject to an enhanced due diligence procedure, which may include the following measures:

- Sworn declaration regarding the origin of the customer's funds or assets.
- Verification of submitted identity information through public databases.

5.4. Customer Due Diligence

The company implements a customer knowledge process based on the following details provided during registration:

- Name and surname
- Identification document type and number
- Date of Birth
- Domicile
- PEP status

Following this, a due diligence procedure is carried out, taking into account the information previously obtained and whether client meets any of the following conditions:

- Players engage in financial transactions equal to or above Naf. 4,000 or equivalent in dollars.
- Carrying out occasional transactions above the monetary equivalent of NAf. 4,0003 or equivalent in dollars.
- There is a suspicion of money laundering or terrorist financing.
- They have doubts about the veracity or adequacy of previously obtained customer identification data.

The due diligence procedure consists of:

- Identifying the customer using registration information and verifying their identity through official, publicly accessible sources like official verification services. Additionally, the customer is screened against UN and EU sanctions lists and their PEP status is checked via web portals or verification systems (e.g., Inspektor or Dow Jones RiskCenter).
- Identifying the ultimate beneficial owner through the payment method used by the customer for betting or the bank account where winnings are transferred, ensuring it matches the registered customer.
- Maintaining a record of customer operations to verify no unusual activity exists relative to the established profile and conducted data verification.

5.5. Ongoing Monitoring

The company maintains a record of customer transactions. When these transactions exceed the regulatory threshold, they are reported to the Compliance Officer, enabling an examination of whether they align with the previously established risk profile. This process helps determine, through a due diligence procedure, if the operation is unusual

5.6. Reliance on third parties to perform customer due diligence

The company does not rely on third parties to conduct its due diligence process

5.7. Reporting of unusual transactions

The Compliance Officer is responsible for the analysis and evaluation of unusual transactions. This includes those reported by staff or identified through monitoring functions, utilizing, in whole or in part, the following indicators¹:

- Transactions which in connection with money laundering or terrorism financing are reported to the Police or to the Department of Justice.
- Transactions by or on behalf of a natural or legal person, a group or an entity, who is named on a list.
- Transactions in the amount of NAf. 5,000 or more (or equivalent in dollars), regardless whether the transaction is made in cash, by check or other form of payment, or through electronic or other non- physical means.
- Presumed money laundering transactions or terrorist financing: transactions where there is cause to presume that they can be related to money laundering or terrorist financing.

¹ Inclusive but not limiting list

The Compliance Officer will report to the FIU any operations detected during the exercise of their duties that, in their sound judgment, are deemed suspicious. This communication must be made within a maximum period of twenty-four hours from the moment the operation is classified as suspicious.

The Compliance Officer shall maintain documentary evidence of the analyses and evaluations performed to qualify an transaction as unusual. Furthermore, if an operation is not deemed unusual, the justification for the analysis conducted must likewise be documented.

5.8. Anti-Money Laundering Compliance program

The compliance program developed by the company includes the following measures:

- A system of internal policies, procedures and controls: The company maintains AML/CTF policies and procedures to prevent its facilities, products, and services from being misused for money laundering, terrorist financing, and weapons of mass destruction proliferation (AML/CTF/PF). These are developed in adherence to current AML/CTF legislation, covering aspects such as due diligence, unusual transaction reporting, and transaction record management, among other established controls.
- A designated compliance officer with day-to-day oversight over the AML program: The Compliance Officer enjoys absolute autonomy and independence in the exercise of their responsibilities and functions. Their principal duties include:
 - To verify adherence to local laws and regulations regarding the detection and deterrence of money laundering and terrorist financing.
 - To organize training sessions for the staff on various compliance-related issues
 - To keep records of internally and externally reported unusual transactions;
 - To design an internal procedure about when reporting of unusual transactions will lead to blocking/ freezing of user accounts, taking into account the risk of tipping off the customer.
 - To prepare the external report of unusual transactions.
 - To make necessary changes to the AML program.
- An employee screening program and ongoing employee training program: The Compliance Officer will develop a training program for the company's employees. This program aims to raise awareness among senior management, department heads, and all other employees regarding

the importance of combating money laundering and the financing of terrorism, as well as the prevention mechanisms established by the company.

These training sessions will be conducted at least twice a year, and attendance is mandatory. Non-attendance will be considered an offense in accordance with the Internal Labor Regulations. Training may be delivered through physical or electronic means, as deemed appropriate. Furthermore, certificates of completed training will be included in the employee's personnel file

- An independent audit function to test the AML program: The compliance program is supervised and evaluated annually by a department independent of the company's AML compliance unit.

The results are documented and brought to the attention of General Management and the shareholders. Corrective measures, including improvements to controls and procedures, may also be established

6. Compliance and Consequences of Non-Compliance

The company will sanction any non-compliance with this policy, as well as with current applicable regulations. Sanctions will be applied according to the nature of the breaches, which may be classified as very serious, serious, or minor offenses, as stipulated in the current regulations and company policies. This is all without prejudice to any sanctions, fines, and/or restrictive penalties imposed by the competent governmental bodies, if applicable.

7. Related Information

The company shall ensure compliance with all applicable national and international standards relevant to the sector

8. Contact Information

For any questions regarding this policy, please contact:

9. Policy History

First version