ArenaBet Anti-Money Laundering (AML) Policy

Introduction

The ArenaBet website, account interface and any related mobile applications (collectively, the “Website”) are operated by Arenabet N.V. (company registration number 105293), registered in Willemstad, Curaçao, under the ArenaBet brand (hereinafter referred to as “we”, “our” or “the company”). The Website operates under gaming licence number OGL/2026/592/4783, granted on 23/03/2026, and is regulated by the Curaçao Gaming Control Board (GCB). The terms "user", "player", or "you" refer to the person who has registered or plans to register an Account on the Website. We apply risk-based anti-money laundering and counter-terrorist financing controls. We take reasonable steps to control and mitigate the risk of money laundering, including allocating appropriate resources and imposing specific AML standards on management and employees. We adhere to high anti-money laundering standards in accordance with applicable guidelines and regulations, which require us to prevent the use of our services for money laundering purposes. We strive to offer a high level of security to all our users. To this end, we have implemented a multi-tiered Account verification system to verify user identity. This includes data requests, automatic and manual checks of user Accounts. These measures are necessary to confirm the accuracy of the registered individual's data and ensure that the payment methods used are not stolen or used by unauthorized third parties, forming the basis for combating money laundering. Please note that this AML Policy may be updated periodically. The current version of the AML Policy will always be available on the Website, indicating its effective date. We recommend that you regularly review the current version of the AML Policy on the Website. If the changes made to the AML Policy are unacceptable to you, you may discontinue using the Website and close your Account. Continued use of the Website after the updated AML Policy takes effect will be deemed acceptance of the changes. Please note that we operate exclusively online and do not have physical establishments.

Legal References

ArenaBet is operated by Arenabet N.V., registered in Willemstad, Curaçao under company number 105293. The Website operates under gaming licence number OGL/2026/592/4783, granted on 23/03/2026, and is regulated by the Curaçao Gaming Control Board (GCB). The company’s AML/CFT approach takes account of applicable legal requirements and relevant international standards, including:

- Applicable Curaçao anti-money laundering, counter-terrorist financing and gaming regulatory requirements and guidance;
- Relevant sanctions and restrictive-measures requirements, where applicable;
- Financial Action Task Force (FATF) Recommendations and related risk-based AML/CFT standards, as applicable. This list is not exhaustive and may be updated from time to time.

Key Definitions

For the purposes of this policy, the Financial Intelligence Unit (FIU) is the competent authority responsible for receiving reports of suspicious transactions. Terrorist Financing refers to financing terrorist acts, terrorists, and terrorist organizations. A terrorist act is an action aimed at intimidating the population or compelling a government or international organization to take or refrain from taking an action. Money laundering is understood as:

- The conversion or transfer of property, especially money, knowing that such property is derived from criminal activity or participation in such activity, with the purpose of concealing or disguising the illicit origin of the property or helping any person involved in such activity evade the legal consequences of their actions;
- The concealment or disguise of the true nature, source, location, disposition, movement, ownership, or rights to property, knowing that such property was obtained through criminal activity or participation in such activity;
- The acquisition, possession, or use of property knowing, at the time of receipt, that such property was obtained as a result of criminal activity or participation in such activity;
- Participation in, complicity in committing, attempting to commit, aiding, abetting, facilitating, and advising in the commission of any of the above actions.Money laundering is considered as such even when the actions that resulted in the property being laundered were committed in another country. Politically Exposed Persons (PEP) are individuals who hold or have recently held important public or state positions, making them vulnerable to financial corruption. This group includes heads of state, mayors, religious leaders, local government officials, etc. A Sanctioned Person is an individual who has been officially sanctioned or restricted by a government or international body due to their suspected involvement in dangerous or illegal activities.

AML Organization

The Money Laundering Reporting Officer (MLRO) is responsible for implementing and enforcing the company's AML Policy and procedures. The MLRO reports directly to senior management and has the necessary level of independence and resources to fully carry out AML responsibilities. The company may involve external specialists in fulfilling part of its AML compliance obligations (for example, for conducting user due diligence (CDD) procedures). However, the company always remains responsible for making final decisions on any issues related to AML compliance obligations.

Changes to the AML Policy and Implementation

All substantial changes to the AML Policy must be approved by senior management and the MLRO.

Risk-Based Approach

To ensure that the measures for preventing or mitigating the risks of money laundering, terrorist financing, and the proliferation of weapons of mass destruction are effective and appropriate, the company applies a risk-based approach. This approach includes conducting user risk assessments (CRA) and applying enhanced or simplified measures for identifying and verifying users based on the assessed level of risk. CRA may be conducted either before a transaction is initiated on behalf of the player or during the process. CRA includes:

- User Acceptance Policy (CAP)
- User Due Diligence (CDD) Additionally, we adopt risk mitigation and control policies and continuously monitor the effectiveness of their implementation.

CAP. Screening of users

Some users may hold a higher risk of money laundering (ML) than others. A general risk assessment considers all relevant risk factors, including the user profile, country or jurisdiction, delivery channels and services. There are four risk categories for each user: low risk (score 1-2), medium risk (score 3-5), high risk (score 6-8), and very high risk (score 9-10). We will block any user who:

- Does not provide the required documents;
- Provides fake or fraudulent documents;
- Uses technical means to conceal their true location;
- Resides or operates in restricted countries;
- Is subject to applicable sanctions;
- Cannot satisfactorily confirm their source of wealth (SoW). Additionally, we reserve the right to close a user's Account for any other reason if the business relationship with that user is considered to pose an unacceptable risk. For users with:
- Very high and high-risk profiles, enhanced due diligence (ECDD) will be applied;
- Medium-risk profiles, standard due diligence (CDD) will be applied;
- Low-risk profiles, simplified due diligence (CDD) may be applied. Screening will not be conducted and cannot be based on racial or ethnic grounds.

CDD Procedures

The company is not permitted to service anonymous or fictitious Accounts. All users of the Website must be properly identified as described below. CDD will be conducted in the following cases:

- When a user reaches a cumulative deposit amount of 2200 USD or the equivalent in any other currency, regardless of whether this threshold is reached in a single transaction or over multiple transactions, and upon the initial withdrawal of any funds;
- If there is reasonable suspicion that the user or the nature of the transaction may pose a risk of money laundering;
- If there are reasonable doubts about the accuracy or authenticity of the information provided by the user. Please note that CDD will be applied if we suspect that a series of transactions, each below any threshold, may reasonably be connected to a single transaction. CDD may be applied to both new and existing users and be performed in the following form:
- Identifying the user's identity (including verifying that the person registering the Account is the beneficial owner of the Account) using a reliable and independent source of information;
- Understanding and obtaining information about the purpose and intended nature of the business relationship;

- Conducting ongoing monitoring of the user's transactions and business relationships. CDD will be applied at the following stages:
- Account creation: the player's profile, which must be completed by the user. This information includes: name, surname, phone number, email, date of birth, gender, country of permanent residence, and full address. A check against sanction lists will be conducted;
- Reaching the financial transaction threshold: supporting documentation will be requested, and PEP screening will be conducted. Depending on the risk level of the specific user, we may take the above steps earlier. Users are not prohibited from using the Website while we conduct a review of the information and supporting documents provided by the user. However, please note:
- Once the established financial thresholds are reached, the user will not be able to make new deposits or withdraw funds until the Verification is completed;
- If the user does not provide the required documents within 30 days of reaching the financial transaction threshold, we are required to block such an Account and report the transaction to the FIU.

Supporting Documents and Information

When verifying a user's identity, we may request the following documents and information, depending on the specific verification required:

- Government-issued documents: valid documents issued by government authorities that include photographic identification of the user (such as a passport, national identity card, driver's license);
- Proof of residence: a bank statement, utility bill, letter from a government authority. These documents must not be older than 6 (six) months;
- Verification codes: a verification code sent to the user's email address to confirm its validity;
- Communication: contact via letter, email, or phone to confirm the information provided by the user. Additionally, we may cross reference certain information using social media profiles, phone directories, company registries, media outlets, geolocation data, IP addresses, and payment method data. This list is not exhaustive. We may request additional information (such as additional government issued documents, photographs of the user with their ID) or ask the user to perform certain actions (such as making their first deposit through an account in an approved jurisdiction). All documents must be authentic, clear, legible, and of good quality. We do not accept documents that do not meet these requirements.

Enhanced Due Diligence (ECDD) and Source of Wealth (SoW) Checks

We conduct ongoing monitoring of our users to identify any suspicious activities that may indicate potential money laundering or terrorist financing schemes. To achieve this goal, we have implemented a set of "red flag" indicators that help detect such activities and require additional steps to evaluate user information. Whenever one of these indicators is triggered, the user's Account will be restricted, and we will conduct ECDD.

ECDD measures are always applied to PEPs and high-risk individuals.

In accordance with our risk-based approach, the user's SoW verification will be conducted as follows:

Users with low risk:

- A self-declaration provided by the user may be sufficient, which should include details such as the nature of their business or employment and their annual salary;
- Social media and other publicly available information sources may also be used as supplementary sources of information.
- Users with high risk:
- The information provided by the user about their SoW will be verified through independent and reliable sources;
- This verification may include, but is not limited to, obtaining supporting documents such as employment contracts or payslips, tax returns, bank statements or investment portfolios, financial statements, or company records for business owners. We reserve the right to request any other documents and information to conduct ECDD and SoW.

Ongoing Monitoring

Ongoing monitoring of all user transactions, Accounts, and SoW information is conducted to identify and detect unusual or suspicious activity compared to the user's established profile. This includes continuous Verification of the user's identity and the accuracy of the documents provided, as well as regular assessments of the legitimacy of the declared SoW.

If identity documents, SoW documents, or any other verification documents expire, we may request new documents, and the user is required to provide them promptly.

Until updated documents are provided, any transactions related to depositing or withdrawing funds will be placed on hold.

Ongoing monitoring is conducted at three levels:

- First line of control: We work exclusively with trusted payment service providers that have effective AML policies. These providers conduct thorough KYC procedures to prevent suspicious deposits before they reach us;
- Second line of control: We ensure that the entire company network is aware of the need for due diligence during any interaction with users, their authorized representatives, or other parties. This includes, but is not limited to: (1) queries related to financial transactions of an Account; (2) queries related to payment methods or Account services;
- Third line of control: Internal monitoring of unusual transactions is based on various factors, including the user's KYC, financial behavior, SoW information, behavioral changes, etc. These assessments are mostly carried out using automated systems, with cross-checks performed by staff for added security. Transactions that are difficult to link to legitimate activity or a known source of funds are quickly flagged as atypical. All such atypical cases are immediately reported to the MLRO. In addition, we conduct manual checks of all suspicious or high-risk users to fully prevent money laundering activities. If any case of fraud or money laundering is identified, we are obligated to promptly notify the FIU. Regarding PEPs and high-risk users, additional monitoring measures are taken:
- Real-life updates based on media sources and international databases;
- For PEPs, the scope of monitoring will be extended to include family members and associated persons to fully cover any indirect influence. Our risk assessment models are reviewed and updated twice a year or as

necessary to incorporate new information and changes in FATF recommendations or sanctions lists. Furthermore, internal and external audits related to AML compliance and practices are conducted annually.

Additional Monitoring Measures

An AI system, overseen by the MLRO, monitors unusual behavior and promptly reports any suspicious activity.

Based on a risk-oriented approach and previous experience, the company's staff review the data provided by AI and conduct additional checks as necessary.

Enterprise-Wide Risk Assessment

As part of our risk-oriented approach, we conduct regular enterprise-wide risk assessments to identify and understand risks specific to us and our business lines on an annual basis.

Additionally, we conduct regular AML training for our employees so that all staff members have the necessary knowledge and skills to recognize and address potential cases of money laundering and financial crimes.

Suspicious Transaction Reporting and Record Keeping

Our internal procedures provide clear guidance to our employees on when and how to report any suspicious activity. Atypical transactions are reviewed by the AML team, which makes decisions based on analysis and collected information:

- Whether a transaction needs to be reported to the FIU as suspicious;
- Whether it is necessary to terminate the business relationship with the user involved in such transactions. Users will not be notified that the company has submitted information about suspicious transactions to the FIU. Records of data obtained through CDD procedures are kept for at least five years after the termination of the business relationship. These records will be securely encrypted and stored in both offline and online environments.

Data Security

All data provided by any user will be protected and will not be transferred to third parties without the user's consent or unless required by law.

Data may be disclosed if necessary by law or to prevent money laundering, in which case it may be transferred to the relevant AML authority in the applicable jurisdiction.

We apply data protection safeguards in accordance with applicable Curaçao law and, where applicable, the General Data Protection Regulation (EU) 2016/679 (GDPR).

Contact Information

If you have any questions or complaints regarding this AML Policy or related matters, please email our support team at **support@arenabet.si**. For general enquiries, you can also contact us at **contact@arenabet.si**.