

**Pegasus 19 B.V. Anti-Money Laundering (AML),
Combating of Terrorist Financing (CFT) & Combating of
Financing Proliferation (CFP) Policy**

Contents

<u>1. Introduction and Purpose</u>	3
<u>1.1 Introduction</u>	3
<u>1.2 Purpose</u>	3
<u>1.3 Definitions</u>	3
<u>2. Legal and Regulatory Framework</u>	4
<u>2.1 Compliance Requirements</u>	4
<u>2.2 International Framework</u>	4
<u>2.3 National Framework in Curacao</u>	4
<u>3. Risk Assessment</u>	5
<u>3.1 Risk-Based Approach</u>	5
<u>3.2 Ongoing Risk Assessment</u>	5
<u>4. Customer Due Diligence (CDD)</u>	5
<u>4.1 Identification and Verification</u>	7
<u>4.2. Obtaining Information on the Purpose and intended nature of the business relationship</u>	8
<u>4.3. Ongoing monitoring</u>	8
<u>4.4. Enhanced Due Diligence</u>	8
<u>4.5 Simplified Due Diligence</u>	9
<u>4.4. Politically Exposed persons PEP-s</u>	9
<u>4.5. Termination</u>	10
<u>5. Account Monitoring and Transaction Reporting</u>	10
<u>5.1 The recognition of unusual transactions</u>	10
<u>5.2 Reporting of unusual transactions</u>	11
<u>5.3. Tipping Off/Confidentiality</u>	12
<u>5.4. Prohibition of disclosure</u>	12
<u>5.5 Record Keeping</u>	12
<u>6. Internal Controls and Procedures</u>	12
<u>6.1 Internal Policies</u>	12
<u>6.2 Employee Screening and Training Programs</u>	12
<u>6.3 Audit and Review</u>	13
<u>7. Responsibilities and Governance</u>	13
<u>7.1 AML Compliance Officer</u>	13
<u>7.2 Board and Management Oversight</u>	13
<u>8. Reporting and Record Keeping</u>	13
<u>8.1 Report Submission</u>	13
<u>8.2 Documentation</u>	13

1. Introduction and Purpose

1.1 Introduction

As a leading provider of online gambling services, we are committed to maintaining the highest standards of integrity and regulatory compliance. This policy outlines our commitment to preventing and detecting money laundering and terrorist financing activities within our operations.

1.2 Purpose

The purpose of this AML Policy is to ensure that Pegasus 19 B.V. ("the Company") operates in accordance with all applicable laws and regulations related to anti-money laundering and counter-terrorist financing. The objectives of this policy are to:

- Protect the integrity and reputation of the Company by implementing robust AML measures.
- Establish a comprehensive framework for identifying, assessing, and managing money laundering and terrorist financing risks.
- Define the responsibilities and procedures for preventing, detecting, and reporting suspicious activities.
- Ensure all employees, partners, and stakeholders understand and adhere to their obligations under this policy.
- Foster a culture of compliance and ethical behavior within our organization.

This policy applies to all employees, agents, and third-party service providers of the Company. Adherence to this policy is mandatory, and any non-compliance will be subject to disciplinary action, up to and including termination of employment or business relationships.

By implementing this AML Policy, Pegasus 19 B.V. demonstrate its commitment to combating financial crimes and contributing to a safer and more secure gambling environment for everyone.

1.3 Definitions

Money laundering is the process by which criminals attempt to hide and disguise the true origin and ownership of the proceeds or any other benefit of their criminal activities, thereby avoiding prosecution, conviction, and confiscation of the criminal funds. There are three stages in the process:

- **Placement:** Cash first enters the financial system at the "placement" stage, where the cash generated from criminal activities is converted into monetary instrument,
- **Layering:** How the link between the funds and the criminal is concealed,
- **Integration:** Investing and/or recovering the funds in a way that looks legitimate.

As a Company policy we do not to accept cash as means of payment, the Company's AML Policy is focused to prevent the use of the Company's activities and resources in the 2nd and in the 3rd stage.

2. Legal and Regulatory Framework

2.1 Compliance Requirements

We are committed to complying with all applicable anti-money laundering (AML) and counter-terrorist financing (CTF) laws and regulations. Our AML Policy is designed also to meet the requirements set forth by international and national regulatory bodies.

2.2 International Framework

Our AML practices are aligned with international standards and guidelines, including:

- **Financial Action Task Force (FATF) Recommendations:** We adhere to the 40 Recommendations established by FATF, which provide a comprehensive framework for AML and CTF efforts globally.
- **Caribbean Financial Action Taskforce (CFATF).**

2.3 National Framework in Curacao

In Curacao, our AML efforts are governed by specific laws and regulations, including

The Regulations for Combating Money Laundering, the Financing of Terrorism and Proliferation of weapons of Mass Destruction are an integral part of the land-based and the online gambling license requirements for the Curaçao jurisdiction.

These Regulations are issued in implementation of article 2 paragraph 8 and article 11, paragraph 3, of the National Ordinance on Identification when rendering Services (NOIS) (N.G. 2024 no.41) and;

- Article 22mm, paragraph 3, of the National Ordinance on the Reporting Unusual Transactions (NORUT) (N.G. 2024 no.41);
- Sanctions National Ordinance (N.G. 2014, no. 55);
- Kingdom Sanction Act (N.G. 2016, no. 54).

2.4 Regulatory Bodies.

Our compliance with AML regulations is overseen by the *Curaçao Gaming Control Board (GCB)* which is the financial intelligence unit in Curacao responsible for monitoring and enforcing AML laws. The GCB provides guidelines and oversight to ensure that offline and online gaming

operators operate in full compliance with national and international standards. EU sanctions are binding for Curaçao on the basis of the Kingdom Sanctions Act.

By adhering to these legal and regulatory frameworks, we ensure that we implement effective measures to prevent money laundering and terrorist financing, thereby safeguarding our business and contributing to the global fight against financial crime.

3. Risk Assessment

3.1 Risk-Based Approach

We adopt a risk-based approach to AML and CTF, allowing us to efficiently allocate resources to areas where they are most needed and to implement appropriate measures to mitigate identified risks. This assessment enables us to develop a risk profile for the customer and to categorize the ML\TF risk posed by such a player as low, medium or high. Our risk assessment process considers various factors, including the nature of our services, customer behavior, and geographic risk.

3.2 Ongoing Risk Assessment

We conduct both business risk assessment and customer risk assessment. Business risk assessment serves to identify the ML/TF risks to which we are exposed to and ensure that the policies, controls and procedures adopted are adequate to prevent and mitigate those risks. The customer specific risk assessment shall be carried out either prior to the carrying out of an occasional transaction, or during establishing a business relationship.

Our risk assessment procedures are continuously reviewed and updated to ensure their effectiveness. This includes:

- Regularly assessing and categorizing risks related to customers, product, service and transaction., and geographical regions.
- Updating risk profiles based on new information and changes in the regulatory environment.
- Conducting periodic audits and reviews of our AML program.

We categorize customers based on their risk profile, considering factors such as transaction size, frequency, and customer background. This allows us to apply appropriate levels of monitoring and due diligence.

4. Customer Due Diligence (CDD)

As an online casino, we do not keep anonymous accounts or accounts in obviously fictitious names. We identify the player and ask for the player's name and other relevant information to determine the purpose and nature of the business relationship.

The purpose of collecting information is to have enough documentation to assess the risk that may be associated with the player and to build a customer profile to assess how the player is going to act within the framework of the business relationship. Such an assessment is necessary in order to detect deviations from the expected behavior. Any unusual behavior shall be reported to the FIU.

- **Minimum requirements for every player who opens an account.** Simultaneously with the opening of an account, we need to identify the customer by collecting the minimum personal details, (this includes: name and surname, permanent residential address and date of birth). This is the minimum applicable in case of low-risk business relationships, and conducting the sanctions screening. Moreover, all players shall be screened against sanctions lists of the UN, EU United States of America (USA, OFAC-lists), Curacao National Lists (currently not in place), local lists of all jurisdictions where online gaming and gambling activities are provided and/or clients accepted, and if they have PEP status.
- **Additional requirements apply in the following cases:**
 - a) when players engage in financial transactions equal to or above XCG. 4,000 (USD 2,198) across any combination of deposits, withdrawals, or transfers;
 - b) when carrying out occasional transactions above the monetary equivalent of XCG. 4,000 (USD 2,198) either in a single transaction or through linked transactions within the same session, game, or time period;
 - c) when there is a suspicion of money laundering or terrorist financing; or
 - d) when the online casino has doubts about the veracity or adequacy of previously obtained.

Once the threshold is reached, we shall proceed with additional due diligence to carry out a customer risk assessment.

In that regard, a player's transaction may be a single transaction, but may also be a series, combination or pattern of transactions involving a total amount in excess of the monetary equivalent of XCG. 4,000 (USD 2,198).

During the time of applying additional measures, customers may be allowed to continue using their gaming account while we obtain any necessary information from the customer concerned. However, If the XCG. 4,000 threshold is reached, the player cannot deposit funds into the account or withdraw funds from the account.

Besides that, if the requested information and documentation is not received within 30 days from the moment the XCG. 4,000 threshold was met to complete CDD, we shall terminate the relationship with the player and report the transaction to the FIU.

Customer Due Diligence measures that should be taken in the mentioned situations when the threshold is reached are explained in the following subtitles.

4.1 Identification and Verification

In a high-risk situation, besides minimum information that we require when opening the account, we also collect the following:

- a) full name;
- b) permanent residential address;
- c) date of birth;
- d) place of birth;
- e) nationality; and
- f) identity number

Afterwards, risk assessment mentioned in 3.2. is done to have sufficient information available to detect unusual activity in the course of the business relationship. Risk rating will be assigned based on initially collected information. This is revised once information is received. On the basis of this assessment proper level of due diligence can be applied.

Furthermore, verification of identity serves for confirming personal details collected for identification (person exists and is who he claims to be) by using independent source documents, data or information. Verification of identity has to be carried out by making reference to an unexpired government-issued document containing photographic evidence of the customer's identity (e.g. high-quality scanned color copies passport, identity card).

Finally, all players should be screened against sanctions lists of the UN and EU. If Curaçao publishes a local list with designated persons and organizations, the casino shall also take that local list into account. We do not conduct business with customers that are subject to international sanctions

4.2. Obtaining Information on the Purpose and intended nature of the business relationship

In case of higher risk, besides sufficient information we obtain documentation to establish a customer's source of wealth as well as the expected level of activity. Source of wealth consists of determining the activities which generate the customer's net worth and whether this justifies the projected and actual level of account activity. As to the extent of the information that casinos are

to collect, it is essential that this reflects the level of money laundering risk identified through the customer risk assessment.

4.3. Ongoing monitoring

It is also needed to conduct ongoing due diligence on the business relationship and scrutinize the transactions undertaken throughout the course of that relationship to ensure that they are consistent with our knowledge of the customer, the customer's business and risk profile. We should also consider to obtain evidence of identity periodically to detect any changes, refresh the data on key events.

In case we realize that a customer's transactions are not consistent with what it knows or expects from the customer, the casino has to question this unusual activity and, where necessary, establish the source of the funds used for that transaction.

4.4. Enhanced Due Diligence (EDD)

For high-risk customers, including those from high-risk jurisdictions, we conduct enhanced due diligence (EDD). This involves additional verification steps and closer scrutiny of transactions to ensure compliance with AML regulations.

Due Diligence **has to** be conducted where the risks of money laundering or terrorist financing are higher. This concerns for example: residents of higher risk geographic areas, political exposed Persons (PEP's), products or transactions that might favor anonymity, new products and new business practices, including new delivery mechanism, and the use of new or developing technologies for both new and pre-existing products.

The applied measures must be consistent with the risks identified. In particular, they should increase the degree and nature of monitoring of the business relationship, in order to determine whether those transactions or activities appear unusual or suspicious.

4.5. Simplified Due Diligence

Where the risks of money laundering or terrorist financing are lower, we conduct simplified CDD measures, which should take into account the nature of the lower risk. Examples of possible measures:

- Not collecting specific information. If the risk assessment undertaken indicates a low risk of money laundering or terrorist financing then it is only necessary to obtain the player's identity (high quality scanned color). Verifying the identity of the customer and the beneficial owner after the establishment of the business relationship;
- The extent of verification may also vary depending on the risk posed by the particular business relationship. In a low-risk situation, the casino can also use alternative reputable information sources, even where these do not contain photographic evidence of the player's identity (e.g. birth certificates, bank statements etc.);
- The extent of personal details verified can also vary. In low-risk situations, we shall verify the basic identification details, as long as we know who its customer is;
- Reducing the frequency of customer identification updates.

4.6. Politically Exposed persons PEP-s

In relation to foreign politically exposed persons (PEPs), (whether as customer or beneficial owner) in addition to performing normal customer due diligence measures, we shall:

- a. has an appropriate risk-management systems to determine whether the customer or the beneficial owner is a politically exposed person;
- b. has the player who was identified as a PEP signed a PEP declaration form;
- c. obtains senior management approval to service the PEP (for establishing the business relationship for new customers, continuing the business relationship for existing customers or for conducting the occasional transaction);
- d. takes reasonable measures to establish the source of wealth and the source of funds. The investigation must then determine whether the player's spending pattern matches their legal source of funds. We shall request a statement from the player about the source of funds and verify them by consulting independent and reliable sources. Depending on the risk in specific cases, this can in the first place be public sources or request the customer to provide documents;

e. conduct enhanced ongoing monitoring of the business relationship.

4.7. Termination

In case the obligations arising from the customer due diligence cannot be met, or when we cannot establish the business relation or perform the transaction, we shall be obliged to terminate the business relationship with the customer. The casino must also keep a record of all the attempts made to get the necessary information and documentation. We shall either close the account or to keep it blocked and suspended in its entirety.

All factors and information at our disposal shall be considered to decide whether there are grounds to suspect ML/FT/FP. If, however the presumption of ML/FT/FP exist we shall submit an unusual transaction report to the FIU with regard to this player.

5. Account Monitoring and Transaction Reporting

5.1 The recognition of unusual transactions

An unusual transaction is a transaction inconsistent with the player's profile. The first key to recognizing that a transaction or series of transactions is unusual is to know enough about the player. This is how collected information about the player shall serves to provide us with documentation to assess the risk that may be associated with the player and to build a customer profile to assess how the player is going to act within the framework of the business relationship.

All these unusual transactions must be reported to the compliance officer in the format approved by management. The compliance officer will keep an adequate filing system of these records.

The following transactions or intended transactions are deemed unusual:

- a. Transactions which in connection with money laundering or terrorism financing are reported to the Police or to the Department of Justice;
- b. Transactions by or on behalf of a natural or legal person, a group or an entity, who is named on a list, adopted by virtue of the Sanctions National Ordinance;

c. Transactions in the amount of XCG. 5,000 or more, regardless whether the transaction is made in cash, by check or other form of payment, or through electronic or other non- physical means. This includes but is not limited to:

- A cashless transaction in the amount of XCG. 5,000 or more. A cashless transaction is a transfer from a bank account of the casino to a local or international bank account, at the request of the client.
- Accepting or releasing a deposit in the amount of XCG. 5,000 or more at the request of the client;
- Sale to a customer of chips in the amount of XCG. 5,000 or more. "Chips" include but is not limited to tokens and credits.
- A cash out in the amount of XCG. 5,000 or more; (A transaction may be a single transaction, but may also be a series, combination or pattern of transactions involving a total amount of the monetary equivalent of XCG. 5,000)
- 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.

5.2. Reporting of unusual transactions

We shall report unusual transaction or any intended unusual transaction to the FIU without delay with all supporting documents. All unusual individual transactions or series of transactions, shall first be reported internally, without any delay.

The compliance officer shall prepare a report of all unusual transactions for external reporting to the FIU.

5.3. Tipping Off/Confidentiality

Any person must treat any information where that person knows or suspects that an unusual transaction report has been made or that an investigation is under way or proposed as strictly confidential.

No staff member may disclose to any person s/he has formed a suspicious that a person may be involved in suspicion that a person may be involved in suspicious matters or transactions or that a report has been lodged about that person with the FIU or any other authority.

Clear lines of reporting where matter or transactions are referred to the MLRO need to be maintained. All matters or transactions are to remain confidential between the reporting staff member and the MLRO.

It is an offense to disclose that an unusual transaction report or related information on a specific transaction has been reported to the FIU or that an investigation into money laundering, terrorist financing or the proceeds of crime is impending/pending, and to divulge that fact or other information to another whereby the investigation is likely to be prejudiced.

5.4. Prohibition of disclosure

Our senior management and our employees shall not disclose any details or information in connection with a report filed to the FIU or a request for information made by the FIU, nor to third parties. Caution is also applied when a casino takes action to terminate a relationship or otherwise block additional transactions following reporting to the FIU.

5.5. Record Keeping

We shall maintain, for at least five years, all necessary records on transactions (both domestic and international). Such records shall be sufficient to permit reconstruction of individual transactions (including the amounts and types of currency involved, if any) so as to provide, if necessary, evidence for prosecution of criminal activity.

All records obtained through CDD measures (e.g. copies or records of official identification documents like passports, identity cards, driving licenses or similar documents), account files and business correspondence shall be kept for at least five years after the business relationship is ended, or after the date of the occasional transaction.

6. Internal Controls and Procedures

6.1 Internal Policies

We implement robust internal controls to detect and prevent money laundering activities. These controls include transaction monitoring systems, customer due diligence procedures, and regular compliance audits.

6.2 Employee Screening and Training Programs

All employees receive regular training on AML regulations, recognizing suspicious activities, and proper reporting procedures. This ensures that our staff are well-equipped to detect and respond to potential money laundering activities. Training programs are applied to new employees, department personnel, audit staff, AML compliance staff, supervisors and managers, senior management and board of directors.

6.3 Audit and Review

Our AML program undergoes regular audits and reviews to ensure its effectiveness and compliance with regulations. This includes both internal and external audits to identify and address any weaknesses in our AML controls.

7. Responsibilities and Governance

7.1 AML Compliance Officer

We appoint a designated AML Compliance Officer (MLCO) responsible for overseeing the implementation and maintenance of our AML program. The AML Compliance Officer reports directly to senior management and the board.

7.2 Board and Management Oversight

Senior management and the board of directors play a critical role in the governance and oversight of our AML policy. They are responsible for ensuring that adequate resources are allocated to the AML program and that it remains effective and compliant with regulations.

8. Reporting and Record Keeping

8.1 Report Submission

We shall provide information or documentation on money laundering and terrorist financing policies and deterrence and detection procedures to the examiners of the GCB in preparation of or during an examination and upon GCB request during the year.

8.2 Documentation

We ensure that all documents related to customer identification, transaction records, and AML reports are retained for the required period of five years. This documentation is securely stored and readily accessible for regulatory review.

By implementing this comprehensive AML Policy, we are committed to maintaining the highest standards of integrity and regulatory compliance, and to contributing to the global effort against money laundering and terrorist financing.

Philip M. Humme

Philip M. Humme, Managing Director o.b.o Allyant Group B.V.



Lydia Obispo, MLRO o.b.o Allyant Group B.V.

Title	AML Policy Pegasus 19
File name	AML_Policy_Pegasus_19.pdf
Document ID	719961457d0e9a86866ebf42e3c6d2922c23b5da
Audit trail date format	MM / DD / YYYY
Status	● Signed

Document History



05 / 27 / 2025
20:23:08 UTC

Sent for signature to Philip Humme (philip.humme@allyant-group.com) and lydia obispo (lydia.obispo@allyant-group.com) from timothy.becker@allyant-group.com
IP: 190.13.122.21



05 / 28 / 2025
10:59:47 UTC

Viewed by lydia obispo (lydia.obispo@allyant-group.com)
IP: 190.13.122.21



05 / 28 / 2025
12:53:29 UTC

Viewed by Philip Humme (philip.humme@allyant-group.com)
IP: 65.208.123.58



05 / 28 / 2025
12:53:52 UTC

Signed by Philip Humme (philip.humme@allyant-group.com)
IP: 65.208.123.58



05 / 28 / 2025
19:04:12 UTC

Signed by lydia obispo (lydia.obispo@allyant-group.com)
IP: 190.13.122.21



COMPLETED

05 / 28 / 2025
19:04:12 UTC

The document has been completed.