KNOW YOUR CUSTOMER (KYC) POLICY

PlayDOM B.V.

a Company with registered address at KAYA RICHARD J. BEAUJON Z/N, CURACAO, registration number 145097, domain name ***pkrdm.best*** (hereinafter referred to as "**Company**")

Stanislav Andrieiev, the MLRO & Compliance Officer

Gouloud Mercedes Hammoud obo Global Related Services B.V. the Statutory Director

CONTENTS

KEY INFORMATION

Approving Official(s):	Stanislav Andrieiev, the MLRO & Compliance Officer Gouloud Mercedes Hammoud obo Global Related Services B.V. the Statutory Director
Responsible Office:	Stanislav Andrieiev, the MLRO & Compliance Officer
Effective Date:	28.05.2025
Next Review Date:	28.05.2026

1. GENERAL PROVISIONS AND POLICY STATEMENT

1.1. The Company is committed to conducting its business with the highest ethical standards and in full compliance with all applicable laws and regulations governing financial transactions. As part of this commitment, we require all Customers to provide accurate and complete identification information during the registration process.

1.2. The Company reserves the right to verify Customer identities using reliable and independent sources. We are responsible for ensuring that the identification data remains accurate and up to date. If any discrepancies or changes are identified, the Company may update the identity information accordingly.

1.3. Our Know Your Customer (KYC) Policy is a fundamental aspect of our efforts to maintain the integrity and security of our operations in the online gambling industry. This Policy sets forth the procedures and controls used to verify Customer identities, ensure regulatory compliance, and prevent fraudulent activities, including money laundering and terrorist financing.

1.4. The primary objective of this Policy is to protect the Company from potential legal and regulatory exposure by thoroughly vetting all Customers. This process confirms the identity and legitimacy of each Customer, deters illicit use of our platform, and promotes greater transparency and trust.

1.5. This Policy applies to all individuals seeking to register and participate in gaming activities through our Website. It encompasses procedures for Customer identification, verification, and continuous monitoring of account activity.

1.6. This Policy shall be in use with our General AML Policy, General AML Guide, Information Security Policy and any other internal regulation of our Company issued from time to time.

1.7. *Policy Coverage and Who It Applies To*. Our KYC policy, procedures and internal controls are designed to ensure compliance with all applicable FATF, GCB regulations general AML rules and will be reviewed and updated on a regular basis to ensure appropriate policies, procedures and internal controls are in place to account for both changes in regulations and changes in our business.

1.8. The Company developing the training programs and provide training to all personnel who perform transactions as referred to in the NOIS and the NORUT. Training includes setting out rules of conduct governing employees' behavior and their ongoing education to create awareness of the Company's policy against money laundering and terrorist financing.

1.9. The Company is entitled to engage third parties to perform certain functions related to KYC procedures subject to confidentiality.

1.10. No member of staff shall at any time disclose a money laundering suspicion to the person suspected, whether or not a Customer, or to any outside party. If circumstances arise that may cause difficulties with Customer contact, the member of staff must seek and follow the instructions of the Responsible person.

2. AUDIENCE

2.1. This policy affects and regulates:

2.1.1. Casino Management and Staff. Senior management and operations staff are directly involved in implementing and overseeing KYC policies and procedures. This includes understanding the requirements, ensuring compliance, and creating a culture of vigilance and ethical conduct within the Company.

2.1.2. Compliance Officers. Individuals responsible for developing, implementing, and monitoring our compliance program. They ensure that our Company adheres to relevant laws and regulations and often serve as the primary liaison between the casino and regulatory authorities.

2.1.3. Technology and IT Teams. These teams implement and manage technology solutions that support Customers monitoring, customer due diligence, and reporting systems essential for AML and CTM compliance.

2.1.4. Customers. Although not directly involved in policy creation, Customers are a crucial audience as policies impact their interaction with the casino and our Company. These policies ensure customer transactions are safe and legitimate, thus building trust in the casino's operations and our Company.

2.1.5. Investors and Stakeholders**.** Investors and our stakeholders have a vested interest in the compliance with KYC policies. Compliance can impact the casino's financial performance and reputation, directly affecting their investment.

2.1.6. Financial Institutions. Banks and financial partners that facilitate transactions for our online casino and require assurance that our Company follow robust KYC policies. This is crucial for maintaining banking relationships and ensuring smooth financial operations.

2.1.7. Legal Team. Our Legal team Responsible for advising on regulatory requirements and potential legal implications of policy breaches. They ensure that the casino's policies align with the current legal landscape and international standards.

2.1.8. Third-party suppliers, that facilitate any services and products for our Company.

2.2. These Know Your Customer (KYC) standards and procedures means that all members of staff at all levels actively participate in preventing the services of the Company from being exploited by criminals and terrorists for money laundering purposes. This participation has its objectives as:

2.2.1. Ensuring full compliance with all applicable Anti-Money Laundering (AML) laws and regulations in the relevant jurisdictions.

2.2.2. Mandating that all employees take proactive measures to prevent, identify, and report to the designated Responsible Person any actual or suspected use of the Company, its employees, facilities, or operations for money laundering, terrorist financing, or other illicit activities.

2.2.3. Requiring all relevant employees to participate in AML training programs to ensure they understand their obligations under the FATF standards, these guidelines, and any applicable updates to AML legislation.

2.2.4. Safeguarding the Company and its employees from the legal, regulatory, and supervisory risks associated with AML breaches.

2.2.5. Protecting the Company's reputation from damage arising from any association with money laundering or terrorist financing activities.

2.3. The Company shall regularly review this Policy to ensure alignment with current legal and regulatory standards. An independent annual audit of KYC policy compliance will be conducted, and the resulting findings and recommendations will be duly considered. The Company shall allocate adequate authority and resources to maintain and enhance a robust AML compliance framework.

3. DEFINITIONS AND ABBREVIATIONS

3.1. **AML** – Anti-Money Laundering.

3.2. **CFT –** Combating the Financing of Terrorism.

3.3. **Company** – PlayDOM B.V., a legal entity validly registered and existing under the laws of Curacao, identification number: 145097, address: 6248 Kaya Richard J. Beaujon Z/N Landhuis Joonchi II, Curacao.

3.4. **GCB –** Gaming Control Board of Curacao.

3.5. **POCA** – The Proceeds of Crime Act.

3.6. **OFAC** – Office of Foreign Assets Control.

3.7. **SDN** – Specially Designated Nationals and Blocked Persons list ("SDN List").

3.8. **FATF** – Financial Action Task Force. An independent intergovernmental body, established in 1989 and mandated by its Member Jurisdictions to develop and promote policies to protect the global financial system against money laundering, terrorist financing and the financing of proliferation of weapons of mass destruction.

3.9. **NAF** – Netherlands Antillean guilder, the currency of Curaçao.

3.10. **NOIS** – National Ordinance on Identification when rendering Services (Landsverordening identificatie bij dienstverlening, N.G. 2010, no. 40 as last amended by N.G. 2015, no. 69).

3.11. **NORUT** – National Ordinance on the Reporting of Unusual Transactions (Lands- verordening Melding Ongebruikelijke Transacties, N.G. 2010, no. 41 as last amended by N.G. 2015, no. 68).

3.12. **FIU** – The Financial Intelligence Unit Curacao.

3.13. **PEP** – is defined as an individual who is or has been entrusted with prominent public functions, excluding middle-ranking or more junior officials. This includes, but is not limited to, the following categories:

- Heads of State, Heads of Government, Ministers, and Deputy or Assistant Ministers;
- Members of Parliament or equivalent legislative bodies;
- Senior officials of political parties, including members of their governing bodies;
- Members of supreme courts, constitutional courts, or other high-level judicial bodies whose decisions are generally not subject to further appeal, except under exceptional circumstances;
- Members of courts of auditors or boards of central banks;
- Ambassadors, chargés d'affaires, and senior-ranking officers in the armed forces;
- Members of administrative, management, or supervisory boards of state-owned enterprises;
- Directors, deputy directors, and members of the board or persons performing equivalent functions in international organizations.

In addition, the following individuals are also considered PEPs due to their relationship or association with the persons listed above:

- **Family members**, including spouses, partners, children and their spouses or partners, and parents;
- **Close associates**, including individuals with joint beneficial ownership of legal entities or arrangements with a PEP, those with close business relationships with a PEP, or persons who are sole beneficial owners of entities or arrangements established for the benefit of a PEP.

3.14. **Gambling or Gambling Game** —Any online game made available on the Website that involves participation for the opportunity to win a Prize shall be considered a game of chance. A game of chance includes:

(i) a game that contains elements of both chance and skill;
(ii) a game where the element of chance may be overcome or minimized through exceptional skill;
(iii) a game that is marketed or presented as involving an element of chance, excluding any activity classified as a sport.

3.15. **Reporting Form** – the standard form, issued by the FIU for the purpose of recording the information regarding an unusual transaction.

3.16. **Customer** — an individual, who uses the Website and/or familiarizes himself with the provisions of the Website, these Policy and the provisions of other documents, and intends to register on the Website to participate in Gambling (acquire a Player status).

3.17. **Third Parties** — any individuals and/or legal entities other than the User and/or the Player, in particular, but not exclusively: family members, spouses, friends, partners, counterparties, creditors, service providers, agents, etc.

3.18. **Website** — the official websites of the Company, on which Customer may play the Gambling Games.

3.19. In this Policy singular include the plural, and the plural include singular in cases of a need for interpretation.

POLICY IMPLEMENTATION

4. CUSTOMER RISK ASSESSMENT

4.1. Customer risk refers to the evaluation of potential threats posed by individual Customers or groups of

Customers in relation to money laundering and terrorist financing. This assessment is a critical component in establishing a robust risk-based approach. The Company uses defined criteria to determine whether a Customer presents an elevated level of risk and takes into account any mitigating factors that may influence this assessment. The application of risk variables may either raise or lower the overall level of assessed risk.

4.2. Customer risk refers to the risk of money laundering (ML) or terrorist financing (TF) associated with establishing and maintaining a business relationship with a particular Customer. The assessment of this risk, particularly in the case of natural persons, typically considers the individual's economic activity and/or source of wealth. Certain categories of Customers may present a higher risk due to the nature of their activities, including but not limited to:

4.2.1. Customers who have multiple sources of income;

4.2.2. Customers with irregular income streams;

4.2.3. PEPs;

4.2.4. High spenders (money can be derived from illegal activities);

4.2.5. Disproportionate spenders (inconsistent with our Company's information about the source of wealth or income);

4.2.6. Improper use of third parties, criminals use third parties to gamble and break up large amounts of cash, to buy chips or to cash out on behalf of others to avoid KYC measures;

4.2.7. Customers using multiple casino player rating accounts to hinder a casino to track their gambling activities;

4.3. he Company establishes a benchmark value representing the upper limit of typical transaction amounts. Customers with a single, consistent source of income are generally considered to pose a lower risk of money laundering or terrorist financing compared to those with multiple or irregular income streams.

5. CUSTOMER ACCEPTANCE POLICY

5.1. The Customer Acceptance Policy outlines the criteria for determining whether a Customer is eligible to open an account or if additional due diligence is required due to an elevated risk profile.

5.2. Prohibited Customers include:

5.2.1. Individuals who refuse to provide necessary information or documentation, do not supply sufficient information, fail to disclose their identity, or where KYC processes cannot be carried out.

5.2.2. Individuals who provide False Information.

5.2.3. Individuals who use aliases, hide their real names, or give false information to mask their identity.

5.2.4. Individuals who appear on sanction lists issued by the Money Laundering Officer (MLRO) or international organizations.

5.2.5. Individuals suspected of using the Company for money laundering, terrorist financing, or financing the proliferation of weapons of mass destruction.

5.2.6. Individuals under the legal age of 18 (or the age of majority in their jurisdiction). Anyone under eighteen cannot be registered as a Player, and any deposits or winnings from such individuals will be forfeited to the Regulatory Authority.

5.2.7. Politically Exposed Persons (PEPs). These are individuals with prominent political roles or high-profile public functions, presenting a greater risk of involvement in money laundering or terrorist financing due to their positions.

6. CUSTOMER KYC

6.1. The Company is entitled to conduct the Customer "Know Your Customer" measures when:

6.1.1. Establishing business relations.

6.1.2. Withdrawing from business relations.

6.1.3. Carrying out occasional transactions on and/or above the monetary equivalent of EUR 2 200, or the equivalent of Naf. 4 000 in currency available on the Website (Enhanced due diligence shall be performed in this case).

6.1.4. There is a suspicion of money laundering or terrorist financing.

6.1.5. The Company has doubts about the veracity or adequacy of previously obtained Customer identification data.

6.2. The Company conducts the KYC:

6.2.1. To identify the Customer and verify that Customer's identity using reliable, independent source documents, data or information.

6.2.2. To identify the beneficial owner and take reasonable measures to verify the identity of the beneficial owner.

6.2.3. To understand and, as appropriate, to obtain information on the purpose and intended nature of the business relationship.

6.2.4. When identifying the Customer, at a minimum the following information must be collected: full name; permanent residential address; date of birth; place of birth; nationality; identity number.

6.3. To carry out the KYC the Company is entitled to receive from the Customer-individual the following documents: (i) an ID card, or (ii) a passport, or (iii) a driver's license.

6.4. In addition, the Company is entitled to receive from the Customer the following documents (in case of Enhanced Due Diligence): (i) a birth certificate, (ii) residence permit, (iii) tax bills, (iv) utility bills, (v) bank, building society or credit union statement or passbook containing current address.

6.5. These Customer Identification Procedures are founded on the principle that the Company will only accept funds from new or existing Customers after verifying the Customer's identity and confirming that they are acting on their own behalf. If a Customer is acting on behalf of a third party, such a relationship must be clearly disclosed, and the Company must verify the identities of the underlying third parties before proceeding.

6.6. The Customer Identification Procedures should be adapted based on the specific characteristics of each Customer. Additionally, the Responsible Person may decide to implement enhanced KYC measures whenever justified by particular circumstances.

6.7. An Individual Customer KYC Checklist is utilized as a reference tool. Staff are encouraged to submit any suggested revisions to the Responsible Person for consideration.

6.8. The Responsible person shall retain copies of all documents reviewed or checklists completed in connection with its Customer Identification Procedures in accordance with Company's Customer Records Retention policies.

6.9. If a Customer is unable to provide acceptable identification documents, the responsible staff will make a risk-based decision regarding the acceptance of the available documentation, consulting with the Responsible Person as needed.

6.10. When the Customer is not the beneficial owner of the assets involved, the responsible staff must take appropriate steps to identify the beneficial owner and apply reasonable measures to verify their identity.

6.11. The Responsible Person will develop a standardized format for use by responsible staff when requesting identity and beneficial ownership verification from relevant corporate entities and trustees, as well as procedures for follow-up if responses are not received within the required statutory timeframe.

6.12. If all reasonable efforts to identify the beneficial owner of a Customer entity have been exhausted and documented without success, the responsible staff shall seek approval from the Responsible Person. Approval will be granted on a risk-sensitive basis to designate as the beneficial owner the individual who exercises ultimate effective control over the Customer entity.

6.13. In all cases where a higher risk of money laundering is identified and enhanced Customer due diligence is warranted, the Responsible Person will consult with Management to determine any additional measures necessary to verify the Customer's identity.

6.14. All verification of identity processes as well as actions taken to verify the identity of corporate entities will be recorded. This will include keeping photocopies of documents produced, or in exceptional cases with the approval of the Management, recording information about where copies are held and can be obtained.

6.15. The Company is entitled to verify whether the individual is acting for himself or for a third party. If the individual acts for a third party, the Company is entitled to establish the identity of that third party with the help of the documents submitted by the individual. If the third-party acts for another third party, the Company is entitled to establish the identity of that other third party, etc.

6.16. If the Company knows or has reasonable grounds to suspect that an individual is not acting on their own behalf, it is entitled to take appropriate measures to identify the Customer on whose behalf they are acting, as well as, if applicable, the third-party representative of that Customer.

6.17. Verification of an identity refers to actions taken to verify that a person exists and is who he claims to be. This is done by checking reliable, independent (of the person whose identity is being verified) sources.

6.18. The Company is entitled to record the following data in such a manner that they are accessible:

6.18.1. The name, the address, the identification information from an (i) ID card, or (ii) a passport, or (iii) a driver's license, the residence or place of establishment of the Customer and the ultimate interested party, if there is any, and/or the person in whose name a payment or transaction is made, and also of their representatives.

6.18.2. The nature, the number and the date and place of issue of the document with the help of which the identification has taken place.

6.18.3. Current and past addresses, date of birth, place of birth, physical appearance, employment and financial history, family circumstances.

6.18.4. Phone number, Email address, mailing address, other contacts.

6.19. The Company may utilize reliable electronic systems to assist in Customer verification. These systems often offer the additional benefit of identifying Politically Exposed Persons (PEPs). The availability of electronic information about individuals depends on their digital footprint. Electronic data sources can provide extensive verification material without requiring Customers to submit physical documents. Such electronic verification methods can be convenient and may be used either as the sole means of verification or in conjunction with traditional document checks, based on the assessed risk level. To be considered sufficient evidence of identity on their own, electronic checks should (i) draw data from multiple sources over time, and (ii) include qualitative assessments to evaluate the reliability of the information provided.

6.20. The Company has the right to obtain or review original documents and verify their authenticity by referencing authoritative sources that detail security features designed to prevent forgery. Additionally, the Company may compare the individual presenting or providing the document with the document itself—for example, by matching the photograph or verifying other identifying information.

6.21. If the Company has any doubts about the authenticity of the documents provided, it is entitled to perform electronic verification through a system that reliably confirms the Customer's identity—not merely their existence. Additionally, the Company may obtain relevant information from other regulated entities (such as banks) to complement other documents and data, thereby supporting the ongoing verification of the Customer's legitimacy with either positive or negative findings.

6.22. Before opening an account, and on an ongoing basis, the Company will check to ensure that a Customer does not appear on the SDN list or is not engaging in transactions that are prohibited by the economic sanctions and embargoes administered and enforced by OFAC. (See the OFAC website for the SDN list and listings of current sanctions and embargoes). Because the SDN list and listings of economic sanctions and embargoes are updated frequently, we will consult them on a regular basis and subscribe to receive any available updates when they occur. With respect to the SDN list, we may also access that list through various software programs to ensure speed and accuracy. See also OFAC's Sanctions List Search tool, which screens names against the SDN list and other sanctions lists administered by OFAC. The Company will also review existing accounts against the SDN list and listings of current sanctions and embargoes when they are updated and [he or she] will document the review.

6.23. The Company does not permit accounts to be opened by, or to make any deposits nor used from, customers located or domiciled in Afghanistan, American Samoa, Aruba, Cyprus, Curacao, Democratic People's Republic of Korea (North Korea), Ethiopia, Guyana, Guam, Iraq, Iran, Laos, Samoa, Saudi Arabia, Russia, Belarus, Saba, Serbia, Singapore, Statia, St. Maarten St. Eustatius, Syria, Sri Lanka, Uganda, United States of America, Vanuatu, Venezuela, Trinidad and Tobago, Yemen, Curacao or countries that are placed by FATF to the "black list" of countries. It is prohibited to use our services and play Gambling Games from Curacao, therefore, access to our Website from Curacao is prohibited.

6.24. Based on the risk, and to the extent reasonable and practicable, we will ensure that we have a reasonable belief that we know the true identity of our Customers by using risk-based procedures to verify and document the accuracy of the information we get about our customers. The Company will analyze the information we obtain to determine whether the information is sufficient to form a reasonable belief that we know the true identity of the Customer (e.g., whether the information is logical or contains inconsistencies).

6.25. The Company may rely on documents to verify Customer identity when appropriate documentation is available. Given the rising instances of identity fraud, we will enhance documentary verification by applying non-documentary methods as outlined below whenever necessary. Non-documentary methods may also be employed if uncertainty remains regarding the true identity of the Customer. In verifying information, we will assess whether the identifying details provided—such as name, street address, postal code, telephone number (if available), date of birth, and Social Security number—support a reasonable belief that we have accurately established the Customer's true identity, taking into account the consistency and plausibility of the information

6.26. We acknowledge that we are not obligated to verify the validity of documents provided by Customers for identity verification and may rely on government-issued identification as sufficient proof of identity. However, if a document displays clear signs of fraud, we must take this into account when assessing whether we can reasonably believe that we have accurately identified the Customer.

6.27. We will verify the information within a reasonable time before the account is opened. Depending on the nature of the account and requested transactions, we may refuse to complete a transaction before we have verified the information, or in some instances when we need more time, we may, pending verification, restrict the types of transactions or dollar amount of transactions. If we find suspicious information that indicates possible money laundering, terrorist financing activity, or other suspicious activity, we will, after internal consultation with the firm's AML Compliance Person, file a SAR in accordance with applicable laws and regulations.

6.28. The Company is entitled to engage third parties to conduct Customer Due Diligence subject to confidentiality.

6.29. The Customer checks shall be performed till the moment of receiving all needed documents and information according to this Policy or till the moment when the Customer rejects or unable to provide all needed documents and information for more than 2 weeks from the request date. When the Customer rejects or unable to provide all needed documents and information for more than 2 weeks from the request date the AML specialist shall record the suspicious and shall execute the measures that are provided in this Policy.

7. AWARE POLICY

7.1. All staff members must remain vigilant for any indications that the Company's services might be exploited for money laundering or that they may encounter knowledge of criminal or terrorist property during their work.

7.2. When a staff member becomes aware of a potential suspicion, they should collect any relevant information routinely accessible to them and determine whether there are reasonable grounds to suspect money laundering.

Any further information obtained—especially explanations for unusual instructions or transactions—must be documented in the Customer file as usual; however, no reference to suspected money laundering should be made in the Customer file.

7.3. The requirement to gather relevant information does not extend to undertaking research or investigation, beyond using information sources readily available within the Company.

7.4. If, after reviewing the routinely available information, the staff member is fully satisfied that there are no reasonable grounds for suspicion, no further action is required. However, if reasonable grounds for suspicion do exist, the staff member must promptly escalate the matter to the Responsible Person.

7.5. Where a member of staff based on their own observations decides that there are reasonable grounds to suspect money laundering, he or she shall submit a suspicion report to the Responsible person, in the format specified by the Responsible person for that purpose. Such internal suspicion report does not breach Customer confidentiality.

7.6. A member of staff who forms or is aware of a suspicion of money laundering shall not discuss it with any outside party, or any other member of staff unless directly involved in the matter causing suspicion.

7.7. No member of staff shall at any time disclose a money laundering suspicion to the person suspected, whether or not a Customer, or to any outside party. If circumstances arise that may cause difficulties with Customer contact, the member of staff must seek and follow the instructions of the Responsible person.

8. RELIANCE ON THIRD PARTIES TO PERFORM KYC

8.1. Our Company may rely on third parties to perform certain KYC measures, provided that the criteria set forth in this Policy are satisfied. The third party must be subject to comparable KYC and record-keeping obligations and have an existing business relationship with the Customer, independent of the relationship the Customer intends to establish with our Company. While reliance on a third party is permitted, ultimate responsibility for the KYC measures remains with our Company. Accordingly, the Company must have an agreement in place with the third party to ensure that copies of identification data and other relevant KYC documentation are accessible upon request. This arrangement should be periodically tested to confirm it operates as intended. However, our Company retains full responsibility for conducting the Customer risk assessment, determining whether the Customer is a Politically Exposed Person (PEP), and performing ongoing monitoring.

9. REPORTING OF SUSPICIONS

9.1. If the Company suspects or has reasonable grounds to suspect that funds are linked or related to, or are to be used for terrorism, terrorist acts, or terrorist organizations, it shall promptly report its suspicion to the FIU in accordance with art. 11 of the NORUT.

9.2. By virtue of article 11 of the NORUT, the Company shall report any unusual transaction or any intended unusual transaction to the FIU without delay. Unusual transactions shall be reported in compliance with the NORUT.

9.3. The following transactions or intended transactions are deemed unusual:

9.3.1. 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

9.3.2. Transactions which in connection with money laundering or terrorism financing are reported to the police authorities or to the following department of justice.

9.3.3. We may file a voluntary FIU for any suspicious transaction that we believe is relevant to the possible violation of any law or regulation but that is not required to be reported by us under the FIU rule. It is our policy that all FIU will be reported regularly to the Board of Directors and appropriate senior management, with a clear reminder of the need to maintain the confidentiality of the FIU.

9.3.4. We will retain copies of any FIU filed and the original or business record equivalent of any supporting documentation for five years from the date of filing the forms. We will identify and maintain supporting documentation and make such information available to any appropriate law enforcement agencies, state regulators upon request.

10. RECORDING AND REPOTING

10.1. The Company records each unusual transaction separately using a Reporting Form. These forms are numbered consecutively. Any voided Reporting Form will be retained by the Company for record-keeping purposes.

10.2. The Company maintains records containing the information and documentation necessary to verify that the KYC measures outlined in this policy have been fulfilled, as well as to establish the background and purpose of transactions. These records are retained for a minimum of five years following the termination of the business relationship or the date of an occasional transaction.

10.3. Each report about an unusual transaction will include at least the following information:

10.3.1. The identity of the Customer.

10.3.2. Nature and number of the identification document of the Customer.

10.3.3. The nature, date, time and place of transaction.

10.3.4. The amount, destination and origin of the funds, securities, precious metals, or other values involved in the transaction

10.3.5. The circumstances that identified the transaction as unusual.

10.4. The Compliance Officer signs the reporting form if it is submitted manually.

10.5. The senior management (director, executive director, CEO, etc.) is entitled to sign the reporting form with the verbal consent of the Compliance Officer.

10.6. By virtue of article 11 of the NORUT, our Company reports unusual transaction or any intended unusual transaction to the FIU without delay. In order to do this, it should have clear procedures for internal and external reporting of unusual transactions in place. These should be communicated to its personnel. All unusual individual transactions or series of transactions, as mentioned in Policy Indicators Unusual Transactions, must be reported internally, without any delay. Also supporting documents must be submitted as part of the reporting.

10.7. The Company may use an electronic system approved by the FIU for this purpose, or submit a paper copy of the reporting form. Submission of paper forms shall not be done by fax for the purpose of data security. In either case, our Company will retain a copy of the reporting form for its own records, which are available to GCB agents upon request.

10.8. The Company shall provide information and documentation related to its money laundering and terrorist financing policies, as well as deterrence and detection procedures, to the examiners of the GCB both during examinations and upon request throughout the year.

10.9. The Company making the following documents and information readily available:

10.9.1. Its written and approved policy and procedures on money laundering and terrorist financing prevention.

10.9.2. The name of each Compliance Officer responsible for the Company’s overall money laundering and terrorist financing deterrence and detection procedures and her/his designated job description.

10.9.3. Records of reported unusual transactions

10.9.4. Records on unusual transactions which required closer investigations.

10.9.5. The completed source of funds declaration.

10.9.6. Schedule of the training provided to our personnel regarding money laundering and terrorist financing.

10.9.7. The assessment report on the Company’s policies and procedures on money laundering and terrorist financing by the internal audit department or the Company's external auditor.

10.9.8. Required copies of identification documents.

10.10. The listing above is not limitative and does not exclude the Company from providing additional information and documentation if the GCB so requests.

10.11. In addition, the Company maintain a record in writing of its (i) policies, procedures and controls, (ii) any changes to those policies, procedures and controls, (iii) the steps the Company have taken to communicate the policies, procedures and controls or any changes to them, within the Company's business.

10.12. The Company may share information about individuals, entities, organizations, and countries with financial institutions or government authorities to assist in identifying and, where appropriate, reporting suspected terrorist activities or money laundering. Prior to sharing such information, the Company will take reasonable steps to verify that the recipients are authorized to receive it under applicable laws and regulations.

10.13. We will employ strict procedures both to ensure that only relevant information is shared and to protect the security and confidentiality of this information.

10.14. We also will employ procedures to ensure that any information received from another financial institution shall not be used for any purpose other than:

10.14.1. Identifying and, where appropriate, reporting on money laundering or terrorist activities;

10.14.2. Determining whether to establish or maintain an account, or to engage in a transaction; or

10.14.3. Assisting the financial institution or gambling operator in complying with performing such activities.

10.15. If we determine that a customer is on the SDN list or is engaging in transactions that are prohibited by the economic sanctions and embargoes administered and enforced by OFAC, we will reject the transaction and/or block the customer's assets and file a blocked asset and/or rejected transaction form with OFAC within 10 days.

10.16. Our Company is obligated not only to comply with the National Ordinance for Identification of Services but also to detect and report both intended and completed unusual transactions. We have established adequate procedures covering: (i) the identification of unusual transactions, (ii) the documentation of such transactions, and (iii) the reporting process for unusual transactions.

10.17. An unusual transaction is one that deviates from the Customer's established profile. Therefore, the key to identifying such transactions lies in having sufficient knowledge about the Customer. Collecting Customer information enables the Company to document and assess the potential risks associated with that Customer, and to develop a profile that predicts their expected behavior within the business relationship. In accordance with NORUT legislation, both objective and subjective indicators have been defined to guide the Company in determining whether a Customer's transaction should be classified as unusual.

10.18. Our management provides staff with specific guidance and training to recognize and properly document unusual transactions. All such transactions must be reported to the Compliance Officer using the format approved by management. Any supporting documents, such as copies of identification, cash-out slips, and other relevant records, must also be submitted. The Compliance Officer is responsible for maintaining an organized filing system for these records. If any internally reported transactions are not forwarded to the FIU, the reasons must be thoroughly documented and approved by the Compliance Officer and/or management.

10.19. In order to implement FAT recommendation, Our Company pays special attention to all complex, unusually large transactions, and all unusual patterns of transactions, which have no apparent economic or visible lawful purpose. The following transactions or intended transactions are deemed unusual:

10.19.1. Transactions which in connection with money laundering or terrorism financing are reported to the Police or to the Department of Justice;

10.19.2. 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 (N.G. 2014 no. 55);

10.19.3. Transactions in the amount of equivalent of NAf. 5,000 or more, regardless of 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 equivalent of NAf. 5,000 or more. A cashless transaction is a transfer from a bank account of the Company to a local or international bank account, at the request of the Customer. Accepting or releasing a deposit in the amount of equivalent of NAf. 5,000 or more at the request of the Customer.

10.20. 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 NAf. 5,000 or more and is considered per gaming day.

10.21. Our Company registered with the FIU and to obtain access to the goAML reporting portal after validation by the FIU. The FIU allows bulk reporting, therefore our account manager at the FIU should be contacted in order for the FIU to determine if the operator qualifies for this service.

11. COOPERATION WITH AUTHORITIES

11.1. The Company commits to fully cooperate with law enforcement and regulatory authorities by providing requested information within five (5) business days, unless otherwise specified by the requesting authority.

11.2. The Compliance Officer shall act as the primary liaison for all communications and requests from such authorities.

12. NOTIFICATIONS

12.1. The Company is entitled to provide notice to Customers that the Company is requesting information from them to verify their identities, as required by the legislation.

12.2. The Company is entitled to provide any other notices to Customer, for example – termination notice, notice of blocking of the account, warning notice, etc.

12.3. We will use the following method to provide notices to customers – Email notice and/or phone call and/or internal account notice and/or mail notice.

13. UPDATING POLICIES AND PROCEDURES. RELATED INFORMATION

13.1. The Company is required to check for amendments on Sanctions Decrees and Regulations on a regular basis and update the KYC policies and – procedures accordingly to reflect such amendments. Such information contains lists of suspected terrorists, terrorist groups, and associated individuals and entities as mentioned in (in any case):

13.1.1. The Consolidated United Nations Security Council Sanctions List.

13.1.2. The Sanction Decree "Al-Qaida c.s., the Taliban of Afghanistan c.s., ISIL c.s., ANF c.s." (N.G. 2015, no. 29).

13.1.3. The Ministerial Regulation "Libya" (N.G. 2015, 28).

13.1.4. The Sanction Decree "Islamic Republic Iran 2015" (N.G. 2015, 27).

13.1.5. The Sanction Decree "Democratic People's Republic of Korea 2015" (N.G. 2015, 30).

13.1.6. The Ministerial Regulation "Yemen" (N.G. 2015, 65).

13.1.7. Guidance for Financial Institutions in Detecting Terrorist Financing.

13.1.8. The listing13 of the Office of Foreign Assets Control (OFAC).

13.1.9. The National Ordinance on Identification of Customers when Rendering Services (N.G. 2017, no. 92).

13.1.10. The National Ordinance on the Reporting of Unusual Transactions (N.G. 2017, no. 99).

13.1.11. Ministerial Decree with general operation of November 11, 2015, laying down the indicators as mentioned in article 10 of the National Ordinance on the Reporting of Unusual Transactions.

13.1.12. (Regulation Indicators Unusual Transactions) (N.G. 2015, no. 73).

13.1.13. The Code of Criminal Law (Penal Code) (N.G. 2011, no. 48).

13.1.14. National Ordinance extension of validity sanction decrees 2018 (N.G. 2018, no. 34).

13.1.15. National Decree for general measures, of the 10th of July 2015, for the implementation of article 2 of the Sanctions National Ordinance, containing implementation of Resolutions 1695 (2006), 1718 (2006), 2087 (2013) and 2094 (2013) of the United Nations Security Council.

13.1.16. National Decree for general measures, of the 10th of July 2015, for the implementation of article 2 of the Sanctions National Decree containing implementation of the United Nation Council resolutions concerning Libya (Sanctions Ordinance Libya) (N.G. 2015 no. 28).

13.1.17. Kingdom Sanction Act (N.G. 2016, no. 54).

13.1.18. National Decree entering into force of Kingdom Sanction Law (N.G. 2017, no. 2).

13.1.19. The National Ordinance on Identification of Customers when Rendering Services (N.G. 2017, no. 92).

14. CONTACT INFORMATION

14.1. **For any questions regarding this policy,** For questions or further information regarding this policy, please contact:

🖂 Email: support@pkrdm.best

⚲ Address: 6248 Kaya Richard J. Beaujon Z/N Landhuis Joonchi II, Curacao.

15. POLICY HISTORY

May 28, 2025	Policy update (Annual update)
December 01, 2024	Policy update (legal changes)
June 12, 2024	Policy update (legal changes)
May 28, 2023	Policy update (Annual update)
May 12, 2022	Policy update (Annual update)
May 20, 20213	Policy update (Annual update)
May 24, 2020	Initial Policy