

KNOW YOUR CUSTOMER (KYC) POLICY

Rapture B.V.

a Company with registered address at
Kaya Richard J. Beaujon Z/N Landhuis Joonchi II Curacao,
registration number 156074, domain name pldm.best
(hereinafter referred to as “**Company**”)

Stanislav Andrieiev, the
MLRO & Compliance
Officer

**Gouloud Mercedes
Hammoud** obo Guardian
Corporation Curacao B.V.,
Statutory Director

CONTENTS

1. GENERAL PROVISIONS AND POLICY STATEMENT.....	4
2. AUDIENCE.....	4
3. DEFINITIONS AND ABBREVIATIONS.....	5
4. CUSTOMER RISK ASSESSMENT	7
5. CUSTOMER ACCEPTANCE POLICY	7
6. CUSTOMER KYC	8
7. AWARE POLICY	11
8. RELIANCE ON THIRD PARTIES TO PERFORM KYC	12
9. REPORTING OF SUSPICIONS	12
10.RECORDING AND REPOTING.....	12
11.COOPERATION WITH AUTHORITIES	15
12.NOTIFICATIONS	15
13.UPDATING POLICIES AND PROCEDURES. RELATED INFORMATION.....	15
14.CONTACT INFORMATION.....	16
15.POLICY HISTORY	16

KEY INFORMATION

Approving Official(s):	Stanislav Andrieiev, the MLRO & Compliance Officer Gouloud Mercedes Hammoud obo Guardian Corporation Curacao B.V., the Statutory Director
Responsible Office:	Stanislav Andrieiev, the MLRO & compliance officer
Effective Date:	17.06.2025
Next Review Date:	17.06.2026

1. GENERAL PROVISIONS AND POLICY STATEMENT

- 1.1. The Company is committed to conducting its business with the highest standards of integrity and in full compliance with all applicable laws and regulatory requirements governing financial transactions. As part of this commitment, all Customers must provide complete and truthful identification information during the account registration process.
- 1.2. The Company reserves the right to verify Customer identity using reliable, independent data sources. It is also responsible for ensuring that all identification information remains accurate and up to date. If discrepancies or updates arise, the Company may amend or request confirmation of the relevant data accordingly.
- 1.3. The Company's Know Your Customer (KYC) Policy serves as a fundamental element in safeguarding the integrity and security of its online gambling platform. This Policy outlines the control measures, processes, and responsibilities associated with Customer verification, aimed at achieving regulatory compliance and combating fraudulent conduct, including money laundering and terrorist financing.
- 1.4. The core objective of this Policy is to mitigate legal and compliance risks by accurately identifying and assessing every Customer. This process confirms the legitimacy of users, prevents misuse of the platform for unlawful purposes, and enhances accountability, trust, and transparency across all operations.
- 1.5. This Policy is applicable to all individuals registering or engaging in gaming activities via the Company's Website. It covers Customer identification and verification processes, as well as continuous monitoring of account behavior to detect anomalies or risks.
- 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 Scope and Applicability.* This KYC Policy, along with the associated procedures and internal controls, is designed to ensure compliance with all relevant regulations, including those set forth by the Financial Action Task Force (FATF), the Gaming Control Board (GCB), and general Anti-Money Laundering (AML) requirements. The Policy will be regularly reviewed and updated to reflect changes in applicable laws and regulations, as well as any developments within the Company's business operations. This ensures that our compliance framework remains current, effective, and aligned with evolving regulatory expectations.
- 1.8. The Company is responsible for developing and delivering training programs for all personnel involved in conducting transactions as referenced in the NOIS and NORUT. These programs establish clear rules of conduct for employee behavior and provide ongoing education to enhance awareness of the Company's policies against money laundering and terrorist financing. The training is designed to ensure that all relevant staff understand their responsibilities and are equipped to comply with applicable regulations and internal procedures
- 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. Scope of Applicability

2.2. This Policy governs and impacts the following key stakeholders within and around the operations of the Company:

- **Casino Management and Staff:** Senior management and operational personnel are responsible for implementing and enforcing KYC procedures, promoting compliance, and cultivating a culture of ethical conduct and vigilance throughout the organization.

- **Compliance Officers:** These individuals design, maintain, and monitor the Company's compliance program. They ensure adherence to applicable laws and serve as the principal point of contact with regulatory bodies.
- **Technology and IT Teams:** Responsible for deploying and managing digital systems that enable effective customer due diligence (CDD), transaction monitoring, and compliance reporting.
- **Customers:** Although not involved in the development of this Policy, Customers are directly affected by its provisions. KYC processes are designed to safeguard their interactions with the platform, ensuring legitimacy, safety, and compliance.
- **Investors and Stakeholders:** These parties rely on the Company's adherence to KYC regulations as a foundation for reputational strength and financial sustainability.
- **Financial Institutions:** Banks and other financial partners require assurance that the Company follows sound KYC practices. This fosters secure banking relationships and operational stability.
- **Legal Team:** Provides guidance on evolving regulatory obligations and helps ensure Company policies are compliant with legal standards and aligned with international best practices.
- **Third-Party Service Providers:** Vendors and partners delivering services or technology to the Company are also expected to adhere to applicable KYC standards and contractual compliance requirements.

2.3. Employee Responsibilities and Objectives

All staff members—regardless of department or seniority—play an active role in protecting the Company from being misused for money laundering or terrorist financing. This includes:

- Ensuring full compliance with applicable Anti-Money Laundering (AML) laws, regulations, and industry standards across all relevant jurisdictions.
- Proactively detecting, preventing, and immediately reporting any suspected or actual misuse of the Company's services or infrastructure to the appointed Compliance Officer.
- Participating in mandatory AML/CFT training to maintain up-to-date knowledge of internal procedures, FATF recommendations, and legal obligations.
- Supporting the Company's commitment to mitigate legal and regulatory risk exposure stemming from AML compliance failures.
- Preserving the Company's reputation by avoiding any involvement or association with money laundering, terrorist financing, or other illicit conduct.

2.4. Policy Review and Oversight

This Policy is subject to regular review to ensure alignment with current regulatory standards and industry best practices. An independent audit of KYC compliance will be performed annually. Findings and recommendations from the audit will be used to strengthen the AML/CFT framework. The Company will allocate sufficient authority, staffing, and resources to support the ongoing enhancement of its compliance infrastructure.

3. DEFINITIONS AND ABBREVIATIONS

- 3.1. **AML** – Anti-Money Laundering.
- 3.2. **CFT** – Combating the Financing of Terrorism.
- 3.3. **Company** –Rapture B.V., a legally registered entity under the laws of Curaçao (registration no. 156074),

located at Kaya Richard J. Beaujon Z/N Landhuis Joonchi II, Curaçao

- 3.4. **CPF – Combating the Proliferation Financing**
- 3.5. **GCB**– Gaming Control Board of Curacao.
- 3.6. **POCA** – The Proceeds of Crime Act.
- 3.7. **OFAC** – Office of Foreign Assets Control.
- 3.8. **SDN** – Specially Designated Nationals and Blocked Persons list ("SDN List").
- 3.9. **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.
- 3.10. **XCG** – Netherlands Antillean guilder, the currency of Curaçao.
- 3.11. **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).
- 3.12. **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).
- 3.13. **FIU** – The Financial Intelligence Unit Curacao.
- 3.14. **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.

- 3.15. **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.
- 3.16. **Reporting Form** – the standard form, issued by the FIU for the purpose of recording the information regarding an unusual transaction.
- 3.17. **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).

3.18. . XCG – Caribbean Guilder

3.19. **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.

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

3.21. 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. **Definition of Customer Risk** Customer risk refers to the potential for money laundering (ML) or terrorist financing (TF) arising from the establishment and maintenance of a business relationship with an individual customer or group of customers. Evaluating this risk is a critical component of the Company's risk-based compliance framework.

4.2. **Assessment Criteria** The Company applies a set of structured criteria to determine whether a customer poses an elevated risk. This evaluation also considers mitigating factors that could influence the overall risk profile. Key variables include the customer's economic activity, source of funds or wealth, geographic location, and transaction behavior. Certain customer types inherently carry higher risk due to the nature of their financial behavior or profile, including but not limited to:

- Customers with multiple sources of income
- Customers with irregular or unpredictable income patterns
- Politically Exposed Persons (PEPs)
- High-spending customers, particularly where the source of funds may be questionable
- Customers whose spending is disproportionate to known income or wealth
- Use of third parties to obscure the origin or ownership of funds (e.g., cashing out chips on behalf of others to evade KYC requirements)
- Customers using multiple player accounts to conceal or manipulate their gambling behavior

4.3. Risk Benchmarking

The Company establishes a benchmark value to define the expected upper limit of transaction amounts. This benchmark is used to detect deviations that may indicate unusual activity. Customers with a single, verified source of income and stable financial behavior are generally considered lower risk. Conversely, those exhibiting multiple, inconsistent, or unexplained income streams may be flagged as higher risk and subject to Enhanced Due Diligence (EDD).

5. CUSTOMER ACCEPTANCE POLICY

5.1. The Customer Acceptance Policy establishes the criteria for determining a customer's eligibility to open and maintain an account with the Company. It also defines the conditions under which Enhanced Due Diligence (EDD) is required—particularly when a customer presents an elevated risk profile based on their behavior, profile, or other indicators.

5.2. Prohibited Customers

The following categories of individuals are strictly prohibited from establishing or maintaining an account with the Company:

5.2.1. Individuals who refuse or fail to provide required identification documents, do not submit sufficient information for verification, or cannot be properly identified through the KYC process.

5.2.2. Individuals who knowingly provide false or misleading information during the registration or verification process.

5.2.3. Individuals who use pseudonyms, aliases, or other deceptive means to conceal their true identity.

5.2.4. Individuals listed on sanctions registers maintained by the Money Laundering Reporting Officer (MLRO), or by international regulatory and enforcement bodies.

5.2.5. Individuals reasonably suspected of attempting to use the Company's services for the purposes of money laundering, terrorist financing, or the financing of weapons of mass destruction.

5.2.6. Individuals below the legal age of 18—or below the age of majority as prescribed by local laws. Any player found to be underage will have their account closed, and any deposits or winnings forfeited and reported to the relevant regulatory authority.

5.2.7. Politically Exposed Persons (PEPs), including individuals holding senior political or governmental positions, or those with significant public functions, due to their increased risk of involvement in financial crimes.

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 XCG 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.** In cases where Enhanced Due Diligence (EDD) is required, the Company reserves the right to request additional documentation from the Customer. Such documents may include, but are not limited to:

- Birth certificate
- Residence permit
- Tax statements or bills
- Utility bills
- Bank, building society, or credit union statements or passbooks that display the current residential address.

6.5. The Company's Customer Identification Procedures are guided by the fundamental principle that no funds shall be accepted from new or existing Customers until their identity has been successfully verified and it is confirmed that they are acting on their own behalf. Where a Customer is acting for or on behalf of a third party, full disclosure of this relationship is mandatory, and the identity of the third party must also be independently verified prior to any transactional activity.

6.6. Identification procedures are adapted to reflect each Customer's specific risk profile and circumstances. Where appropriate, the designated Responsible Person may apply enhanced KYC measures based on the level of assessed risk.

6.7. To assist with consistent implementation, an Individual Customer KYC Checklist is utilized as a practical tool during the identification process. Employees are encouraged to provide feedback or suggestions for improvements

to the checklist, which will be reviewed by the Responsible Person for potential adoption.

- 6.8. The Responsible Person is responsible for securely retaining all documentation and checklists reviewed or completed during the Customer Identification Process. This is done in accordance with the Company's Customer Records Retention Policy and applicable regulatory requirements.
- 6.9. In situations where a Customer cannot provide standard forms of identification, the responsible staff must conduct a risk-based assessment of the alternative documentation submitted. Final acceptance shall be made in consultation with the designated Responsible Person, ensuring that any deviation from standard procedures is appropriately justified and documented.
- 6.10. When a Customer is not the beneficial owner of the funds or assets involved, the responsible staff is required to take reasonable and proportionate steps to identify the beneficial owner and verify their identity, in line with applicable due diligence standards.
- 6.11. The Responsible Person shall develop and maintain a standardized request format for obtaining beneficial ownership and identity verification from legal entities, trusts, and similar arrangements. This format will include clear instructions for follow-up procedures in cases where no response is received within the required statutory or regulatory timeframe.
- 6.12. Where all reasonable and documented efforts to identify a Customer entity's beneficial owner have been unsuccessful, responsible staff must escalate the matter to the Responsible Person. A risk-based decision may be made to designate the individual who ultimately exercises effective control over the entity as the beneficial owner, provided that this determination is supported by a thorough risk-sensitive assessment.
- 6.13. In instances where the risk of money laundering or terrorist financing is elevated and Enhanced Due Diligence (EDD) is warranted, the Responsible Person shall consult with senior management to identify and implement any additional verification procedures necessary to confirm the Customer's identity and mitigate the identified risks.
- 6.14. All steps taken during the identity verification process—whether for individual customers or corporate entities—must be fully documented. This includes retaining copies of identification documents. In exceptional cases, and subject to Management approval, it is acceptable to record the specific location where such documents are securely stored and can be accessed if needed.
- 6.15. The Company reserves the right to verify whether a customer is acting on their own behalf or representing another party. Where a customer is acting on behalf of a third party, the Company is entitled to verify the identity of that third party. If it is established that the third party is also acting in a representative capacity, the Company may pursue identification and verification of any further parties involved.
- 6.16. If the Company has knowledge or reasonable grounds to suspect that a customer is not acting independently, it is authorized to take necessary steps to identify the true customer as well as any representatives acting on their behalf.
- 6.17. Identity verification entails confirming that a person exists and that their identity corresponds to the information provided. This process must rely on reliable, independent sources that are not affiliated with the individual being verified.
- 6.18. The Company shall maintain accessible records of the following data for all identified individuals and entities:
 - 6.18.1. The full name, residential or business address, and identification details from an official document (such as an ID card, passport, or driver's license), including those of any ultimate beneficial owners, the person in whose name a transaction is conducted, and their representatives if applicable.

- 6.18.2. The type, number, date of issue, and issuing authority of the identification document used during the verification process.
- 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 reputable electronic verification systems to assist in the identification and authentication of Customer identities. These systems often provide enhanced capabilities, such as the identification of Politically Exposed Persons (PEPs), and can perform identity checks without requiring Customers to submit physical documents. Depending on the Customer's risk profile, electronic verification may serve as a primary method or be used alongside traditional documentation. To be accepted as a standalone method, the electronic system must:
- (i) Aggregate data from multiple independent sources across time, and
 - (ii) Provide qualitative analysis that assesses the reliability and validity of the information gathered.
- 6.20. The Company reserves the right to request and examine original documents and verify their authenticity against official sources that list security features intended to prevent forgery. Furthermore, the Company may verify that the person presenting or submitting the document corresponds to the information therein—such as by matching a photograph or confirming other biometric or identifying details.
- 6.21. If there is any uncertainty or suspicion regarding the authenticity of submitted documents, the Company may employ electronic systems capable of verifying not only the Customer's identity but also their legitimacy. Additionally, the Company may consult external regulated entities, such as financial institutions, to cross-reference and validate Customer information. This multi-source verification process helps confirm or disprove the Customer's identity and strengthens the integrity of the onboarding process.
- 6.22. Prior to account opening and on an ongoing basis, the Company will conduct checks to confirm that a Customer is not listed on the U.S. Department of the Treasury's Office of Foreign Assets Control (OFAC) Specially Designated Nationals (SDN) List and is not involved in any transactions prohibited under applicable economic sanctions or embargoes administered by OFAC. The SDN List and related sanctions programs are subject to frequent updates; therefore, the Company will monitor these changes regularly and subscribe to automatic updates where available. To ensure timely and accurate screening, the Company may use dedicated compliance software tools that integrate with the SDN List and other OFAC-administered sanctions databases, including the OFAC Sanctions List Search tool. All new and existing accounts will be screened against updated sanctions data, and each review will be documented in accordance with internal compliance procedures. If a Customer is found to be listed or associated with any restricted entity or transaction, the Company will take appropriate action, which may include blocking or rejecting the transaction and filing the necessary reports with OFAC or other relevant authorities.
- 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, Algeria, Angola, American Samoa, Aruba, Australia, Antigua and Barbuda, Bahamas, Barbados, Belize, Bermuda, Belgium, Bonaire, Bosnia and Herzegovina, Bolivia, Burma/Myanmar, Burundi, Burkina Faso, Bulgaria, Cameroon, Central African Republic, Curaçao, Côte d'Ivoire, China, Denmark, Democratic Republic of the Congo, Egypt, Eritrea, Estonia, France, French Guyana, Greenland, Guadeloupe, Guam, Guatemala, Haiti, Holy See (Vatican City), Jamaica, Italy, Iran, Iraq, ISIL and Al-Qaida, Ivory Coast, Kenya, Lao People's Democratic Republic, Lebanon, Libya, Lithuania, Kuwait, Malaysia, Marshall Islands, Martinique, Maldives, Mali, Monaco, Mozambique, Namibia, Nepal, Netherlands, North Korea (Democratic People's Republic of Korea), Occupied Palestinian Territory, Poland, Puerto Rico, Qatar, Reunion, Republic of Guinea, Saba, Saint Barthelemy, Saint Martin, Saint Pierre and Miquelon, Singapore, Spain, South Africa, Somalia, South Sudan, St. Eustatius, Sudan, Syria, Tunisia, Trinidad & Tobago, USA, US Minor Outlying Islands, Virgin Islands (UK), Venezuela, Vietnam, Yemen, Zimbabwe, or countries that are placed by FATF to the "black list" of countries.
- 6.24. It is prohibited to use our services and play Gambling Games from Curacao, therefore, access to our Website is prohibited from Curacao.
- 6.25. 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).

- 6.26. The Company may rely on official documents to verify a Customer's identity when such documentation is available and appropriate. However, in light of the increasing prevalence of identity fraud, documentary verification will be strengthened with non-documentary methods whenever necessary. These alternative methods may also be applied if there is any residual uncertainty regarding the Customer's true identity. In conducting identity verification, the Company will evaluate whether the identifying information provided—such as full name, street address, postal code, telephone number (if available), date of birth, and Social Security number—forms a consistent and credible basis for a reasonable belief that the Customer's identity has been accurately established.
- 6.27. 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.
- 6.28. The Company will verify Customer information within a reasonable timeframe prior to account activation. Depending on the nature of the account and the type or value of requested transactions, the Company may, at its discretion, decline to process a transaction until verification is complete. In certain cases, if additional time is required, the Company may impose temporary restrictions on transaction types or monetary limits pending verification. If, during the verification process, any information raises suspicion of potential money laundering, terrorist financing, or other illicit activity, the matter will be escalated internally to the AML Compliance Officer. Following this review, and in accordance with applicable laws and regulations, a Unusual Transaction Report (UTR) will be filed as appropriate.
- 6.29. The Company is entitled to engage third parties to conduct Customer Due Diligence subject to confidentiality.
- 6.30. 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 unusual and shall execute the measures that are provided in this Policy.

7. AWARE POLICY

- 7.1. All employees of the Company play a crucial role in the detection and prevention of money laundering and terrorist financing. The following responsibilities and procedures apply:
- 7.2. **Vigilance and Awareness.** All staff members must exercise constant vigilance for any indicators that the Company's services are being exploited for money laundering or that they may be exposed to criminal or terrorist property during the course of their duties.
- 7.3. **Assessment of Potential Suspicion.** If a staff member encounters conduct or transactions that raise concerns, they are required to gather all routinely accessible information to determine whether there are reasonable grounds for suspicion. Explanations provided by the Customer for unusual transactions or behaviors should be recorded in the Customer's profile. However, no explicit reference to suspected money laundering must be included in the Customer's file.
- 7.4. **Scope of Staff Responsibility.** Employees are not expected to conduct in-depth investigations or seek information beyond what is normally available within the Company's systems. Their obligation is to assess existing internal information and escalate concerns when appropriate.
- 7.5. **Determining Reasonable Grounds.** If the staff member concludes, after reviewing the available data, that no reasonable suspicion exists, no further action is required. Conversely, if suspicion is supported by the facts, the staff member must immediately escalate the concern to the designated Responsible Person (e.g., the Compliance Officer or MLRO). 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.

- 7.6. **Internal Suspicion Reporting.** Where reasonable grounds to suspect money laundering or related criminal activity exist, the staff member must submit a formal Internal Suspicion Report using the prescribed format provided by the Responsible Person. Filing this report is a legal obligation and does not violate the Customer's confidentiality under applicable laws.
- 7.7. **Confidentiality and Information Control.** Once a suspicion is formed or known, it must not be discussed with any third party or other members of staff who are not directly involved in the issue. Strict confidentiality must be maintained to avoid compromising any ongoing or future investigation.
- 7.8. **Prohibition of Tipping-Off.** No employee shall inform the Customer or any third party that an unusual activity report has been or may be filed. If an employee anticipates that ongoing communication with the Customer may lead to inadvertent disclosure or complications, they must immediately consult the Responsible Person and follow their guidance.

8. RELIANCE ON THIRD PARTIES TO PERFORM KYC

- 8.1. The Company may, under certain conditions, rely on third parties to carry out specific Know Your Customer (KYC) procedures, provided that the requirements outlined in this Policy are fully met. Any third party engaged for this purpose must be subject to KYC and record-keeping obligations equivalent to those applicable to the Company, and must have an established, independent business relationship with the Customer outside the relationship the Customer seeks to form with the Company. While such reliance is permitted, the Company retains ultimate responsibility for ensuring that all KYC requirements are fulfilled. To that end, a formal agreement must be in place with the third party, ensuring that copies of identification data and other relevant documentation can be provided upon request. This arrangement must be periodically reviewed and tested to confirm its effectiveness.

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 unusual 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. Every unusual transaction identified by the Company must be documented individually using a designated Unusual Transaction Reporting Form. Each form is assigned a unique, sequential reference number for tracking purposes. If a form is canceled or voided for any reason, it shall still be retained and archived to ensure the completeness and integrity of the Company's record-keeping practices..
- 10.2. The Company keeps thorough records of all data and supporting documentation necessary to demonstrate compliance with the Know Your Customer (KYC) measures specified in this Policy. These records also reflect

the context and intended purpose of the transactions in question. All documentation is retained for a minimum of five years following the termination of the business relationship or the date of a one-time transaction, whichever occurs later.

- 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. Pursuant to Article 11 of the National Ordinance on the Reporting of Unusual Transactions (NORUT), the Company is legally obligated to report any unusual transaction or attempted unusual transaction to the Financial Intelligence Unit (FIU) without undue delay. To meet this obligation, the Company shall establish and maintain clear, documented procedures governing both the internal escalation and external reporting of such transactions. These procedures must be communicated to and understood by all relevant personnel. All unusual transactions—whether isolated events or part of a pattern of related activity as described in the Policy’s indicators of unusual transactions—must be reported internally to the designated Responsible Person immediately upon identification. Each report must be accompanied by all relevant supporting documentation to enable a comprehensive assessment and ensure timely submission to the FIU where required.
- 10.7. The Company may submit reports using an electronic system approved by the Financial Intelligence Unit (FIU) or, alternatively, provide a paper copy of the reporting form. For data security reasons, submission of paper forms via fax is prohibited. Regardless of the submission method, the Company will retain a copy of each reporting form in its records. These records must be made available to agents of the Gaming Control Board (GCB) 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 characterized by a departure from the Customer's established profile. Effectively identifying such transactions requires the Company to have comprehensive knowledge of the Customer. By collecting relevant Customer information, the Company can document and evaluate the associated risks and develop a behavioral profile that anticipates expected transaction patterns within the business relationship. In line with NORUT legislation, the Company utilizes both objective and subjective indicators to assist in determining whether a Customer's transaction should be classified as unusual.
- 10.18. Management ensures that all staff receive specific guidance and training to identify and accurately document unusual transactions. Every such transaction must be reported to the Compliance Officer using the management-approved reporting format. Supporting documents—such as copies of identification, cash-out slips, and other pertinent records—must accompany the report. The Compliance Officer is responsible for maintaining a well-organized filing system for all related records. In cases where internally reported transactions are not escalated to the Financial Intelligence Unit (FIU), the reasons for withholding must be fully 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 XCG 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 XCG 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 XCG 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 XCG 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 cooperating 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 questions or further information regarding this policy, please contact:



Email: support@pldm.best



Address: Kaya Richard J. Beaujon Z/N Landhuis Joonchi II, Willemstad, P.O. Box 6248, Curacao

15. POLICY HISTORY

June 17, 2025	Policy update (Annual update)
December 01, 2024	Policy update (legal changes)
June 12, 2024	Policy update (legal changes)
May 28, 2024	Policy update (Annual update)
December 12, 2023	Policy update (legal changes)
May 20, 2023	Policy update (Annual update)
May 24, 2022	Initial Policy