

KNOW YOUR CUSTOMER (KYC) POLICY
INTERSEAL B.V.

Registration number: 163945



Stanislav Andrieiev, the
MLRO & Compliance
Officer



**Jonathan Marshall Ruwel
Heymans** obo Kurason Trust
Curacao N.V., the Managing
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	11
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 Jonathan Marshall Ruwel Heymans obo Kurason Trust Curacao N.V., the Managing Director
Responsible Office:	Stanislav Andrieiev, the MLRO & compliance officer
Effective Date:	19.05.2025
Next Review Date:	19.05.2026

1. GENERAL PROVISIONS AND POLICY STATEMENT

- 1.1. The company is ensuring that the business is conducted at a high ethical standard and that the laws and regulations pertaining to financial transactions are followed. Our Company requires accurate and complete identification details from all Customers during the registration process.
- 1.2. The Company is entitled to verify the identity of the Customers using reliable and independent sources. The Company shall see to it that the identity data is correct. When it turns out that these data are no longer in accordance with reality, the Company is entitled to adjust these modified identity data.
- 1.3. Our Know Your Customer (KYC) Policy is a critical component of our commitment to ensuring the integrity and security of our operations within the online gambling sector. This policy outlines the procedures and measures implemented to verify the identities of our Customers, maintain compliance with regulatory requirements, and prevent fraudulent activities, including money laundering and terrorism financing.
- 1.4. The head purpose of this Policy is to safeguard our Company from potential legal and regulatory risks by ensuring that all Customers are thoroughly vetted. This process is intended to confirm the identity and legitimacy of each Customer, prevent illicit use of our platform, and enhance overall transparency and trust.
- 1.5. The scope of this policy is to apply to all Customers who wish to register and engage in any gaming activities via our Website. It also covers procedures related to customer identification, verification, and ongoing monitoring of account activities.
- 1.6. This Policy shall be in use with our General AML Policy, General AML Guide, Privacy & Management of Personal Data Policy and any other internal regulation of our Company issued from time to time.
- 1.7. *Subject matter, including the scope and applicability.* 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. Complying with all Anti - Money Laundering Act & Regulations of the jurisdictions.
 - 2.2.2. Requiring all employees to prevent, detect and report to the Responsible person all potential instances in which the Company or its Employees, its facilities or its activities have been or are about to be used for money laundering, terrorist financing and other illegal activity.
 - 2.2.3. Requiring all appropriate employees to attend anti-money laundering training sessions, so that all employees are aware of their responsibilities under FATF, these guidelines and as affected by current developments with respect to anti-money laundering legislations.
 - 2.2.4. Protecting the Company and all its staff as individuals from the risks associated with breaches of the law, regulations and supervisory requirements.
 - 2.2.5. Preserving the good name of the Company against the risk of reputational damage presented by implication in money laundering and terrorist financing activities.
- 2.3. The Company shall monitor this Policy with legal and regulatory requirements and conduct an annual independent KYC policy compliance audit, the findings of which are to be considered and appropriate recommendations for action set out. The Company shall provide the necessary authority and resources for the ongoing implementation of a compliant AML regime.

3. DEFINITIONS AND ABBREVIATIONS

- 3.1. **AML** – Anti-Money Laundering.
- 3.2. **CFT** – Combating the Financing of Terrorism.
- 3.3. **Company** – Interseal B.V., a legal entity validly registered and existing under the laws of Curacao, identification number: 163945, adress: Schottegatweg Oost 10 Unit A1K 10 Unit 1-9, Bon Bini Business Cente, Curasao.
- 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 (Landsverordening 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** – an individual who is entrusted with prominent public functions, other than middle-ranking or more junior officials, including the following individuals:
- heads of state, heads of government, ministers and deputy or assistant ministers; members of parliament or of similar legislative bodies; members of the governing bodies of political parties;
- members of supreme courts, constitutional courts or other high-level judicial bodies whose decisions are not subject to further appeal, except in exceptional circumstances; members of courts of auditors or of the boards of central banks; ambassadors, chargés d'affaires and high-ranking officers in armed forces;
- members of the administrative, management or supervisory bodies of state-owned enterprises; directors, deputy directors and members of the board or equivalent function of an international organization.
- The following individuals are also regarded as PEPs by virtue of their relationship or association with the individuals listed previously:
- family members of the individuals listed previously, including spouse, partner, children and their spouses or partners, and parents;
- known close associates of the individuals listed previously, including individuals with whom joint beneficial ownership of a legal entity or legal arrangement is held, with whom there are close business relations, or who is a sole beneficial owner of a legal entity or arrangement set up for the benefit of the PEP.
- 3.14. **Gambling or Gambling Game** — any online game posted on the Website that means playing a game of chance for a Prize. Game of chance includes (i) a game that involves both an element of chance and an element of skill, (ii) a game that involves an element of chance that can be eliminated by superlative skill, (iii) a game that is presented as involving an element of chance but does not include 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 risks involve assessing the potential threats of money laundering and terrorist financing presented by an individual or group of Customers. This assessment is essential for developing and implementing a comprehensive risk-based framework. According to specified criteria, the Company evaluates whether a specific customer represents a heightened risk and considers how mitigating factors might influence this evaluation. The application of risk variables can either reduce or increase the overall risk assessment.
- 4.2. Customer risk is the risk of ML/TF that arises from maintaining relations with a given Customer. An assessment of the risk posed by a natural person is generally based on the person's economic activity and/or source of wealth. Categories of Customers whose activities may indicate a higher risk include:
 - 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. Our Company sets a value which represents the upper value of a typical transactions. A Customer having a single source of regular income will pose a lesser risk of ML/TF than a Customer who has multiple sources of income or irregular income streams.

5. CUSTOMER ACCEPTANCE POLICY

- 5.1. The Customer Acceptance Policy specifies the criteria used to decide whether a Customer can be approved to open an account or if further scrutiny is needed due to a higher level of risk.
- 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 based on the premise that the Company will accept funds from a new and existing Customer only after the Company has confirmed the Customer's identity and that the Customer is acting as a principal and not for the benefit of any third party unless specific disclosure to that effect is made; or If the Customer is acting on behalf of others, the Company has confirmed the identities of the underlying third parties.
- 6.6. The Customer Identification Procedures should be reviewed in light of the specific characteristics presented by a Customer and in any instance the Responsible person may determine to apply additional KYC measures for any other justifiable reasons.
- 6.7. As a reference tool, an Individual Customer KYC Checklist is used. Staff is encouraged to provide the Responsible person with any revisions they consider appropriate.
- 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. In cases where a Customer cannot produce acceptable documents, the responsible staff will make a risk-based decision on accepting the documents that are available, consulting with the Responsible person if appropriate.
- 6.10. Where the Customer is not the beneficial owner of assets involved, the responsible staff will take the necessary steps to determine who the beneficial owner is, and take reasonable measures to verify their

identity accordingly.

- 6.11. The Responsible person will prepare a format for use by the responsible staff in requesting verification of identity and beneficial ownership information from relevant corporate entities and trustees, and a procedure for following up when requests are not met within the statutory period.
- 6.12. If all possible means of identifying the beneficial owner of a Customer entity have been exhausted without success, and recorded, the responsible staff will seek the approval of the Responsible person, to be given on a risk-sensitive basis, to treat as its beneficial owner the natural person who exercises ultimate effective control over the Customer entity.
- 6.13. In all cases assessed as presenting a higher money laundering risk, where enhanced Customer due diligence is required, the Responsible person will consult with the Management to decide on additional steps 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 should reasonably suspect that the individual is not acting for himself, the Company is entitled to take reasonable measures in order to trace the identity of the Customer for whom he is acting and in the event of representing a Customer by a third party of that representative.
- 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 is entitled to use reliable electronic systems to help with verification. Some of these systems also have the advantage of assisting with the identification of PEPs. The amount of electronic information available about individuals will vary, depending on the extent of their electronic 'footprint'. Electronic data sources can provide a wide range of confirmatory material without necessarily requiring the Customer to produce documents. Electronic sources can be a convenient method of verification. They can be used either as the sole method of verification, or in combination with traditional document checks, on a risk basis. For an electronic check to provide satisfactory evidence of identity on its own it should (i) use data from multiple sources, across time, and (ii) incorporate qualitative checks that assess the strength of the information supplied.
- 6.20. The Company is entitled to obtain or to view the original documents and ensuring that they are valid and genuine, by comparing them to published, authoritative guidance that outlines security features (which

protect against forgeries). In addition, the Company is entitled to compare the person presenting the document, or making the document available, to the document itself (for example, photograph comparison or comparison of information).

- 6.21. If the Company has any doubts on the provided documents, the Company is entitled to conduct electronic verification through a scheme which properly establishes the customer's identity, not just that the customer exists and to obtain information from another person in the regulated sector (for example, from banks), that can be used in conjunction with other documents and information to prove a customer's legitimacy over time, or positive or negative information.
- 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.
- 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. Our Company may use documents to verify Customer identity when appropriate documents are available. In light of the increased instances of identity fraud, we will supplement the use of documentary evidence by using the non-documentary means described below whenever necessary. We may also use non-documentary means, if we are still uncertain about whether we know the true identity of the customer. In verifying the information, we will consider whether the identifying information that we receive, such as the customer's name, street address, zip code, telephone number (if provided), date of birth and Social Security number, allow us to determine that we have a reasonable belief that we know the true identity of the customer (e.g., whether the information is logical or contains inconsistencies).
- 6.26. We understand that we are not required to take steps to determine whether the document that the customer has provided to us for identity verification has been validly issued and that we may rely on government-issued identification as verification of a customer's identity. If, however, we note that the document shows some obvious form of fraud, we must consider that factor in determining whether we can form a reasonable belief that we know the Customer's true identity.
- 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. Every member of staff must be alert for the possibility that the Company's services could be used for money laundering purposes, or that in the course of their work they could become aware of criminal or terrorist property.
- 7.2. A member of staff becoming aware of a possible suspicion shall gather relevant information that is routinely available to them and decide whether there are reasonable grounds to suspect money laundering. Any additional information acquired, in particular any explanations for unusual instructions or transactions, should be recorded on the Customer file in the routine manner, but no mention of suspected money laundering is to be recorded in any 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 gathering and considering routinely available information, the member of staff is entirely satisfied that reasonable grounds for suspicion are not present, no further action should be taken otherwise where there are reasonable grounds for suspicion, the staff shall raise the matter with 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 when performing elements of the KYC measures, provided that the criteria mentioned in this Policy are met. The third party should be subject to KYC and record-keeping requirements of the Company. The third party will have an existing business relationship with the Customer, which is independent from the relationship to be formed by the Customer with the relying institution (our Company). Where such reliance is permitted, the ultimate responsibilities for KYC measures remain with the Company relying on the third party. In this case, our Company should have an agreement with the third party being relied upon that copies of identification data or other relevant documentation relating to KYC requirements will be made available upon request and this arrangement must be tested from time to time to

ensure that it actually functions as set out in the agreement. Our Company, however, remains responsible for the carrying out of a Customer-based risk assessment, determining whether the customer is a PEP and conducting on-going 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 is recording each unusual transaction individually on a reporting Form. Individual reporting forms are numbered sequentially. Any Reporting Form that is voided shall be retained by the Company.
- 10.2. The Company is maintaining records, containing the information and documentation necessary to decide whether the objective of the KYC measures referred to in this policy was met, and to establish the background and purpose of transactions, for at least five years after the business relationship is ended, or after the date of the 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 providing information or documentation on money laundering and terrorist financing policies and deterrence and detection procedures to the examiners of the GCB in preparation of or during an examination and upon GCB request during the year.
- 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 with financial institutions or governmental authorities regarding individuals, entities, organizations and countries for purposes of identifying and, where appropriate, reporting activities that we suspect may involve possible terrorist activity or money laundering. Before we share information with financial institutions or governmental authorities, we will take reasonable steps to verify that the financial institutions or governmental authorities are entitled to receive that information according to the legislation.
- 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 not only required to adhere to the stipulations of the National Ordinance for Identification of Services but are also required to detect and report either intended or completed unusual transactions. Our Company has adequate procedures in place that cover the following (i) the recognition of unusual transactions, (ii) the documentation of unusual transactions, and (iii) the reporting of unusual transactions.
- 10.17. An unusual transaction is a transaction inconsistent with the Customer's profile. Therefore, the first key to recognizing that a transaction or series of transactions is unusual is to know enough about the Customer. The purpose of collecting Customer information is to provide the Company with documentation to assess the risk that may be associated with the Customer and to build a Customer profile to assess how the Customer is going to act within the framework of the business relationship. Based on the NORUT legislation, objective and subjective indicators have been established by means of which our Company should assess whether a Customer's transaction qualifies as an unusual transaction.
- 10.18. Our management provides our staff with specific guidance and training in recognizing and adequately documenting unusual transactions. All these unusual transactions must be reported to the Compliance Officer in the format approved by management. All additional documents available, such as copies of identification documents, cash out slips, and other records must be also submitted as supplements. The Compliance Officer must keep an adequate filing system of these records. If internally reported transactions are not reported to the FIU by the Company, the reasons therefore shall be adequately documented and signed off 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 shall cooperate fully with law enforcement and regulatory authorities, providing requested information within 5 business days unless otherwise specified.
- 11.2. The Compliance Officer shall serve as the primary point of contact for such inquiries.

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, please contact: support@pd.games or send a mail on the address: Schottegatweg Oost 10 Unit A1K 10 Unit 1-9, Bon Bini Business Center, Curaçao.

15. POLICY HISTORY

May 19, 2025	KYC policy update (Annual update)
December 02, 2024	KYC policy update (legal changes)
June 12, 2024	KYC policy update (legal changes)
May 24, 2024	KYC policy update update (Annual update)
December 12, 2023	KYC policy update (legal changes)
June 20, 2023	KYC policy update (legal changes)
May 24, 2023	Initial KYC policy