

Mr. Cedric Pietersz
Curaçao Gaming Authority
Scharlooweg 172-174
Willemstad-Curaçao

30 May 2025

Re: Uploading AML/CFT Policy

Dear Mr. Pietersz,

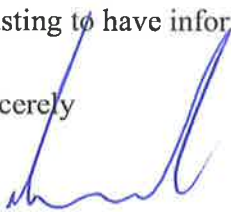
In order to comply with the due date for submission of the AML/CFT Policy, the applicant hereby uploads the draft version of the AML/CFT policy.

Note that this policy is not yet final as it is under review by management for approval and sign off.

Once approved, the final and official version will be signed off by management and uploaded to the portal. We expect this to take place in the course of the coming week.

Trusting to have informed you accordingly.

Sincerely



Raoul Behr
Managing Director

ISLAND LUKKLY B.V.

AML/CFT policy

2025

Document properties

Document	Details
Document title	AML/ CFT policy
Document version	V 1.4.
Document usage	Internal
Status	Released
Issued date	30.05.2025
Document approved by	Head of Legal / Compliance officer Antonis Tsiattalos

Change log

Date	Version	Name, position	Description of change
13.11.2024	V 1.2.	Head of Legal / Compliance officer Antonis Tsiattalos	Yearly update, take into consideration the risk based approach
15.05.2025	V 1.3	Head of Legal / Compliance officer Antonis Tsiattalos	Yearly update, take into consideration the risk based approach
30.05.2025	V 1.4		

Distribution list

Name	Position
All employees	
All employees	

1. INTRODUCTION

1.1. These rules establish internal controls to ensure Island Lukkly B.V., registered in March 2024 under registration number 166711 with the legal address at “Don” Martins 31, Curaçao, complies with international sanctions, Anti-Money Laundering (AML), and Counter-Terrorist Financing (CFT) regulations. Operating within Curaçao's gambling framework, Island Lukkly B.V. has developed this comprehensive policy to meet regulatory obligations while ensuring adherence to international best practices in preventing illicit financial activities.

1.2. The objectives of this Company Policy are to:

1.2.1. Strengthen the reputation and operational transparency of Island Lukkly B.V.

1.2.2. Prevent criminal elements from exploiting the services of Island Lukkly B.V. for laundering illicit funds or financing terrorism.

1.3. The Company comply with the following legislations including:

1.3.1. The following laws and regulations, as well as any additional regulations issued pursuant to the NOIS, NORUT, the Sanction National Ordinance and the Kingdom Sanction Law, are applicable to the Company:

- Code of Criminal Law (Penal Code) (N.G. 2011, no. 48);
- National Ordinance on Identification of Customers when Rendering Services (NOIS) (N.G. 2017, no. 92), last update June 2024;
- National Ordinance on the Reporting of Unusual Transactions (NORUT) (N.G. 2017, no. 99), last update June 2024;
- National Decree penalties and fines reporting unusual transactions (N.G. 2021, no. 69) as amended by PB 2023, no. 6.;
- 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 (Regulation Indicators Unusual Transactions) (N.G. 2015, no. 73);
- Sanctions National Ordinance (N.G. 2014, no. 55);
- Kingdom Sanction Act (N.G. 2016, no. 54);
- National Decree entering into force of Kingdom Sanction Law (N.G. 2017, no. 2);
- National Ordinance extension of validity sanction decrees 2018 (N.G. 2018, no. 34);
- National Decree for general measures, of the 10 July 2015, for the implementation of article 2 of the Sanctions National Decree containing implementation of the United Nations' Security Council resolutions concerning Libya (Sanctions Ordinance Libya) (N.G. 2015 no. 28);
- National Decree for general measures, of the 10 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 (Sanctions Decree People's Democratic Republic of Korea 2015) (N.G. 2015 no. 30);
- 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 United Nations' Security Council Resolutions concerning Al-Qaeda c.s., the Taliban of Afghanistan c.s., ISIL c.s. ANF c.s. and persons and organizations to be designated locally (N.G. 2015, no. 29);
- National Ordinance of the 20th of December 2024 Containing Rules concerning

Games of Chance (National Ordinance on Games of Chance) (PB 2024, no. 157);

Hereafter mentioned as the AML/CFT Act.

- 1.3.2. Curaçao Gaming Control Board Regulations for the combating of Money Laundering, the Financing of Terrorism and Proliferation of weapons of mass destruction, last update January 2025.
- 1.3.3. Any other relevant measures or/and guidelines which may be issued from time to time by the Curacao gaming Board “GCB”, the Financial Action Task Force (FATF) and/or any relevant authority of agency.
- 1.3.4. Any other subsidiary or related legislation, including any amendments to such laws or subsequent legislation.

1.4. The key aims of this policy are to:

- 1.4.1. Risk Management: Identify, evaluate, and mitigate the risks associated with money laundering and terrorism financing
- 1.4.2. Customer Due Diligence (CDD): Implement a robust framework for verifying client identities and assessing their risks, incorporating both simplified and enhanced measures based on risk levels
- 1.4.3. Data Management: Define clear responsibilities for collecting, managing, and securing data related to client due diligence activities.
- 1.4.4. High-Risk Identification: Provide guidance for identifying Politically Exposed Persons (PEPs), sanctioned individuals, and residents of high-risk jurisdictions.
- 1.4.5. Suspicious Activity Reporting: Establish methodologies for recognizing and reporting suspicious transactions to the appropriate authorities.
- 1.4.6. Technological Adaptation: Continuously evaluate and manage risks stemming from new technologies, services, and business models.
- 1.4.7. Account Holder Management: Outline the processes for collecting and maintaining accurate account holder information.

1.5. This Company Policy is applicable to all transactions conducted by customers, including those facilitated through agents and third-party providers, as mandated by the AML/CFT legislation, see paragraph

1.6. Employee Training:

- 1.6.1. Management ensures ongoing employee training on:
 - AML/CFT procedures
 - Emerging methods of money laundering and terrorist financing
 - Recognizing suspicious transactions
 - Data protection and compliance obligations
 - Data protection and Reporting processes for unusual or suspicious activities compliance obligations
- 1.6.2. Training sessions are conducted annually at a minimum.
- 1.6.3. Materials and content for training are developed based on the AML/CFT Act and guidance from the Financial Intelligence Unit (FIU).

1.7. Employee Responsibilities:

- 1.7.1. The compliance team is responsible for compiling, updating and maintaining this policy
- 1.7.2. Employees must be fully familiar with AML/CFT procedures
- 1.7.3. Compliance with the AML/CFT Act and FIU guidelines is mandatory for all staff
- 1.7.4. Employees are required to independently review relevant laws and updates annually
- 1.7.5. Cooperation with government authorities in combatting money laundering and

terrorism financing is an integral part of their responsibilities

1.8. Island Lukkly B.V. is resolute in its commitment to preventing the misuse of its systems for illicit financial activities, including money laundering (ML) and the financing of terrorism (TF). To achieve this, the company ensures full compliance with its legal and regulatory obligations by promptly identifying and addressing suspicious activities. Any such activities will be thoroughly investigated and, if necessary, escalated to the relevant authorities in accordance with Curaçao regulations.

1.9. The AML Policy establishes comprehensive standards for internal controls aimed at preventing and mitigating risks associated with AML/CFT. These standards are designed to be fully integrated into the daily operations of Island Lukkly B.V., requiring strict adherence from both management and employees. This policy serves as a cornerstone of the company's risk management strategy, ensuring a consistent approach to combating ML and TF threats.

1.10. Through the implementation of this policy, Island Lukkly B.V. underscores its steadfast commitment to ethical business practices and rigorous regulatory compliance. By fostering a culture of transparency and accountability, the company protects the safety and integrity of its operations while contributing to the global fight against financial crimes. This approach not only ensures legal compliance but also reinforces the trust of stakeholders and customers.

2. DEFINITIONS

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

2.1.1. Placement: Cash first enters the financial system at the "placement"; stage, where the cash generated from criminal activities is converted into monetary instruments.

2.1.2. Layering: How the link between funds and the criminal is concealed.

2.1.3. Integration: Investing and/or recovering the funds in a way that looks legitimate.

2.1.4. As it is strictly a Company policy not to accept cash as means of payment, the Company's AML Policy is focused to prevent the use of the Company's activities and resources.

2.2. Counter Proliferation Financing (CPF) Island Lukkly B.V. is committed to the prevention of financing the proliferation of weapons of mass destruction. In accordance with CGA regulations and FATF Recommendation 7, the company performs screening for CPF risks, maintains relevant policies and procedures, and ensures prompt reporting to the FIU where applicable.

2.3. Money Laundering Reporting Officer - The responsible for receiving and assessing reports of suspected money laundering or terrorism financing activities. The MLRO's duties include: Advising the Company on AML policies and procedures, supervising the Company's compliance with AML regulations, evaluating the content of reports and disclosures in the context of all relevant information available to the Company, ensuring timely reporting of suspicious activities to the appropriate authorities.

2.4. Customer Due Diligence (CDD) - Procedures for identifying and verifying customer identities and assessing risk.

2.5. Politically Exposed Persons (PEPs) - Individuals holding prominent public positions or their associates.

3. INTERNAL CONTROLS

3.1. Island Lukkly B.V. may engage a qualified third party to conduct independent evaluations of its AML Compliance Program. Such reviews are essential to ensuring the program's ongoing effectiveness and alignment with the company's AML/CFT obligations. These evaluations shall be conducted at least once every two years. The purpose of the review shall be to:

3.1.1. Assess the adequacy of the company's AML Compliance Program in mitigating risks associated with money laundering (ML) and terrorism financing (TF).

3.1.2. Determine whether AML/CFT controls have been properly and effectively implemented across the company's operations.

3.1.3. Verify that the company is operating in full adherence to the requirements and obligations outlined in its AML/CFT policy and regulatory standards.

3.2. The results of the review, including any reports prepared, are shared with senior management and, where applicable, the governing body. All findings and reports from the review are documented and, if required, shared with the Curaçao Gaming Control Board.

4. RISK ASSESSMENT

4.1. Island Lukkly B.V. adopts a risk-based approach in the development and operation of its systems and controls to prevent financial crimes such as money laundering (ML) and terrorist financing (TF). The company conducts risk assessments during the onboarding stage (prior to engagement) and continues to monitor risks throughout the business relationship.

4.2. During the onboarding process, the company gathers information about the purpose and intended nature of the business relationship. This enables Island Lukkly B.V. to establish a customer's business and risk profile, allowing it to accept or reject potential clients. Ongoing procedures ensure that customer information remains accurate and up-to-date through internal triggers and periodic due diligence checks.

4.3. The risk-based approach to preventing ML/TF is integrated into the company's operations, including the development and enhancement of its systems, controls, and processes. Risk management is central to the development of new business areas, product functionality, and expansion into new markets. The company's approach ensures that its operations are resilient to financial crime.

4.4. Mitigation Measures include policies, controls, procedure, and other measures adopted by the Company so as to counter the inherent risk it is exposed to. These are aimed at decreasing the specific inherent risk to form the Company's Residual Risk. The Company shall finally determine whether the residual risk falls within its Risk Appetite. If residual risk falls outside the Company's risk appetite the mitigating measures must be revisited and strengthened to reduce the residual risk to acceptable parameters.

4.5. Island Lukkly B.V. evaluates risks based on the following four key pillars:

4.5.1. Customer Risk – the risk of ML/TF that arises from entertaining relations with a given person or entity. This may be due to the business or professional activity carried out by the customer, the customer's reputation, political exposures and similar aspects that are inherent to the customer.

4.5.2. Geographic Risk – different geographic areas are exposed to differing levels of ML/TF risk, and have AML/CFT frameworks of different effectiveness, and therefore the geographies associated with impact the ML/TF risk of the customer. Geographical risk arises from links with one or more geographical areas, usually related to those jurisdictions (a) where the customer is based, has their main place of business or where the activity generating the customer's wealth is carried out, and the jurisdictions with which the customer has especially strong trading or financial connections; and/or (b) with which the customer or its beneficial owner have relevant personal links (for example the individual's residence in a given jurisdiction).

4.5.3. Product, Services and Transactions Risk – is the risk one is exposed to as a result of

providing a given product or services or carrying out a particular transaction. Tshi typically depends of (a) the level of transparency or opaqueness that the product affords; (b) the complexity of the product; and (c) the value or size of the product.

4.5.4. Interface Channel Risk – the delivery channel, or interface risk, is the risk arising from how the subject person interacts with the customer and the channels it uses to provide a given product. Interacting with customers on a non-face-to-face basis need not be considered as automatically presenting a higher risk of ML/FT.

4.6. All players, whether new or existing, will undergo a risk assessment prior to onboarding. The customer's risk profile will be continuously monitored and automatically updated based on their ongoing activities, such as product usage, transaction patterns, payment methods, and geographic connections. This ensures that the company maintains an accurate and up-to-date understanding of its customers' risk levels.

4.7. Any changes in risk identified through customer activities will be subject to review, with priority given to high-risk customers. This review process will remain active throughout the business relationship to ensure that any emerging risks are promptly identified and mitigated.

4.8. The cornerstone of protecting against abuse by money launderers is the principle of "Know Your Customer" (KYC). KYC is implemented through a robust Customer Due Diligence (CDD) framework. CDD encompasses all processes and controls designed to ensure that Island Lukkly B.V. has a clear and comprehensive understanding of its customers at all stages of the business relationship, including their identity, financial behavior, and risk profile. Through the implementation of these measures, Island Lukkly B.V. ensures the integrity of its operations while complying with regulatory requirements.

5. RESPONSIBILITY OF MONEY LAUNDERING REPORTING OFFICER

5.1. The Fraud Manager, as the nominated Money Laundering Reporting Officer (MLRO), shall receive disclosures about any suspected money laundering or financial terrorism activity and shall be responsible for informing the Company of the AML policies and procedures. The responsibilities of the MLRO is to supervise the actions of the Company and consider the contents of any report made to him/her in relation to relevant information that is available to the Company.

5.2. The MLRO is assigned at the following responsibilities:

- 1) To design and implement the AML program; To verify adherence to local laws and regulations regarding the detection and deterrence of money laundering and terrorist financing; To review compliance with the casino's policy and procedures;
- 2) To organize training sessions for the staff on various compliance-related issues;
- 3) To analyze transactions and verify whether any are subject to reporting according to the indicators mentioned in the Ministerial Decree regarding the Indicators for Unusual Transactions;
- 4) To review all internally reported unusual transactions for their completeness and accuracy with other sources;
- 5) To keep records of internally and externally reported unusual transactions;
- 6) To execute closer investigation of unusual transactions if necessary;
- 7) To prepare the external report of unusual transactions;
- 8) To make necessary changes to the AML program;
- 9) To remain informed on the local and international developments on money laundering and terrorist financing and to make suggestions to management for improvements;
- 10) To prepare periodic information on the casino's efforts against money laundering and financing of terrorism and financing of proliferation.

5.3. All responsibilities are included in employee job description.

6. TRAINING PROCESS

- 6.1. The Company maintains and continuously develops a robust training program aimed at fostering and updating AML/CFT awareness among all employees. This ongoing process ensures that staff remain knowledgeable about their roles and responsibilities in identifying and mitigating money laundering (ML) and terrorism financing (TF) risks.
- 6.2. The training program includes a variety of formats to cater to different learning preferences and schedules, including: Briefings, in-class training sessions, online training modules, webinars and interactive sessions, digest-style updates and written instructions.
- 6.3. New employees are required to undergo anti-money laundering training as part of their mandatory introductory training program. The Money Laundering Reporting Officer (MLRO) is responsible for providing clarifications and detailed information to address any questions or concerns raised by new hires.
- 6.4. All employees play a critical role in implementing measures designed to minimize risks and protect the Company from exposure to financial crimes. Every employee is expected to: (a) understand their significance in the Company's AML/CFT compliance framework. (B) actively engage in training sessions and apply the acquired knowledge in their daily activities.
- 6.5. All employees are required to complete the Company's AML training annually. Employees must incorporate the knowledge and recommendations gained from training into their daily responsibilities to ensure compliance with AML/CFT obligations. Upon the request of a department head or manager, the MLRO will organize individual training or briefings for specific employees as needed.
- 6.6. The Company reserves the right to conduct periodic assessments or testing to evaluate employees' understanding of AML/CFT mechanisms, tools, and responsibilities. This ensures that the workforce remains proficient and capable of identifying and managing risks effectively.

7. NATURAL PERSON'S IDENTITY VERIFICATION.

7.1. The obliged entity's employee establishes the customer's identity and, if necessary, the customer's representative identity, and also the following information in respect of the customer's and, if necessary, the customer's representative, must be secured:

- 7.1.1. name and surname
- 7.1.2. personal identification code, in case of its absence, date of birth and place of birth, as well as the place of residence or location
- 7.1.3. date of birth
- 7.1.4. place of birth
- 7.1.5. nationality
- 7.1.6. permanent residential address
- 7.1.7. that the player is over the age of 18+ (inbuilt control in system)
- 7.1.8. the player's valid e-mail address
- 7.1.9. the player's valid phone number
- 7.1.10. currency

7.2. The obliged entity's employee verifies the correctness of the data specified in clauses 14.1. using information from an independent and reliable source

7.3. The user is obliged to provide a scanned copy of the necessary identification documents. If it is necessary employees can ask users to provide a certified copy of such documents

7.4. The following effective documents are allowed to be used as the basis for the natural person's identity verification:

- 7.4.1. identity card
- 7.4.2. digital identity card

- 7.4.3. residence permit card
- 7.4.4. national/foreign passport
- 7.4.5. diplomatic passport
- 7.4.6. the seaman's service book
- 7.4.7. alien's passport
- 7.4.8. temporary travel document
- 7.4.9. refugee travel document
- 7.4.10. a maritime certificate
- 7.4.11. driver's license issued in a foreign country, if the owner's name, a photograph or facial image, signature or facsimile of the signature and date of birth or personal identification code are indicated in the document

7.5. If the original document specified in clause 14.4 of these rules cannot be seen, a notarized copy of the document and also notarized or officially certified copy of the document or information from other independent and reliable sources, including the means of electronic identification and through electronic transactions, using in this case, the data control at least two different sources can be used to verify the identity.

7.6. Verification on the other hand consists in confirming the personal details collected for identification purposes using data, information and documentation obtained from independent and reliable sources. The personal information to be collected, and the extent of verification to be carried out, is to be determined based on the overall customer risk level or regulatory thresholds set by the GCB.

8. CUSTOMER DUE DILIGENCE AND ON-GOING MONITORING

8.1. It is the policy of Island Lukkly B.V. to conduct a thorough risk assessment and ensure that sufficient evidence of each customer's identity is obtained, verified, and retained in compliance with Curaçao's AML/CFT regulations. This includes adherence to Know Your Customer (KYC) and Customer Due Diligence (CDD) requirements.

8.2. Given the inherent risks associated with the online gaming industry, the company applies Enhanced Due Diligence (EDD) measures to all prospective customers. This process aims to ensure that all customers are thoroughly vetted before being granted access to the company's services.

8.3. The company collects and verifies comprehensive KYC documentation and information from customers, including but not limited to full details of Ultimate Beneficial Owners (UBOs); details of directors or controlling parties (if applicable); evidence of gaming licenses (if relevant to the customer's profile); other relevant identification and verification details. Every customer is required to complete a Due Diligence Form, as outlined in Appendix 1 (Customer Form), which is part of the onboarding process.

8.4. Once all requested information and documentation are obtained, the company sends a confirmation email to the customer at the email address provided during registration. This step ensures that the customer's contact details are accurate and that the onboarding process is formally completed.

8.5. In addition to performing thorough due diligence during the initial acceptance stage, Island Lukkly B.V. implements robust ongoing monitoring procedures. Customers' accounts and activities are continuously reviewed to ensure compliance with applicable AML/CFT requirements.

8.6. The company follows the Internal Controls (referenced in Section 3.) for ongoing monitoring of customers. This includes automated and manual processes for flagging unusual or high-risk transactions and conducting periodic reviews to update customer risk profiles as needed.

8.7. By adhering to these processes, Island Lukkly B.V. ensures that its customer verification and monitoring practices meet Curaçao's stringent AML/CFT standards while mitigating the risks associated with money laundering and terrorist financing in the online gaming industry.

8.8. The identity of a customer or the customer's representative may be verified on the basis of information obtained from a credible and independent source also at the time of the establishment of the business relationship, provided that it is necessary for not disturbing the ordinary course of business. In such an event the verification of identity must be carried out as quickly as possible and before the taking of binding measures

8.9. The obliged entity may choose the extent of performance of the duty and the need to verify the information and data used therefore with the help of a credible and independent source.

8.10. Due diligence measures to the business relationship may be applied in a simplified manner by the simplified procedure, provided that a factor characterizing a lower risk has been established and at least the following criteria are met: (a) a long-term contract has been concluded with the customer in writing, electronically, or in a form reproducible in writing; (b) the total value of incoming and outgoing payments in transactions made in the framework of the business relationship does not exceed EUR 15,000.00 a year.

9. ADDITIONAL CUSTOMER DUE DILIGENCE MEASURES

9.1. The obliged entity chooses additional customer due diligence measures to manage and mitigate an established risk of money laundering and terrorist financing that is higher than usual, choosing at own discretion to apply one or several of the following due diligence measures:

9.1.1. verification of information additionally submitted upon identification of the person based on additional documents, data, or information originating from a credible and independent source;

9.1.2. gathering additional information on the purpose and nature of the business relationship, transaction, or operation and verifying the submitted information based on additional documents, data, or information that originates from a reliable and independent source;

9.1.3. gathering additional information and documents regarding the actual execution of transactions made in the business relationship to rule out the sensibility of the transactions;

9.1.4. gathering additional information and documents to identify the source and origin of the funds used in a transaction made in the business relationship to rule out the sensibility of the transactions;

9.1.5. the making of the first payment related to a transaction via an account that has been opened in the name of the person or customer participating in the transaction in a credit institution registered or having its place of business in a contracting state of the European Economic Area or in a country where requirements equal to those of Directive (EU) 2015/849 of the European Parliament and the Council are in force;

9.1.6. the application of due diligence measures regarding the person or their representative while being at the same place as the person or their representative.

9.2. Upon application of enhanced customer due diligence measures, the obliged entity must apply the monitoring of a business relationship more frequently than usual; including reassessing the customer's risk profile not later than six months after the establishment of the business relationship.

10. POLITICALLY EXPOSED PERSON IDENTIFICATION

10.1. A politically exposed person is an individual who performs the duties of public authority or performs significant duties of public authority, including the president of the republic, the head of government, the minister or deputy minister or minister's assistant, a member of parliament or a member of a state body similar to the parliament, a member of the state court or the supreme court, the state controller and a member of the central bank's

management board, the ambassador, the charge affairs and the senior officer of the defense forces, the management board member of the state, a member of the administrative or supervisory authority, the head of an international organization, a deputy's head and a member of the management, or a person who performs the same functions but does not have an official secondary or lower status level.

10.2. A person politically connected with local authorities is the person specified in clause XIII. 1. that performs or performed significant public authority duties in Curacao, in other countries which are the contracting states of the European Economic Area Agreement or in the European Union 'institutions.

10.3. A member of the family of a politically exposed person at the state level or apolitically exposed person at the local level is a spouse of a person or person who is considered to be a spouse of a politically exposed person at the state level or a politically exposed person at the local level, a child of a politically exposed person at the state level or a politically exposed person of the local level or spouse of a child of a politically exposed person at the state level or a politically exposed person at the local level or a person who is considered to be a spouse of a child of a politically exposed person at the state level or a politically exposed person at the local level, and a parent of a politically exposed person at the state level or a politically exposed person at the local level.

10.4. The close associate is an individual concerning whom it is known that he or she is about a legal entity or legal structure and he or she is the actual beneficial owner or co-owner together with a politically exposed person at the state level or with a politically exposed person at the local level or has close business relations with a politically exposed person at the state level or with a politically exposed person at the local level and an individual who is the only actual beneficial owner or of such legal entity's legal framework in respect of which it is known that it is indeed established by a politically exposed person at the national level or in favor of a politically exposed person at the local level.

10.5. In a situation where an economic or professional transaction or a participant in the performance of an official act, the customer or their actual beneficial owner is a politically exposed person of national level, a member of the family of a politically exposed person of national level, or a person who is a close associate of a politically exposed person of national level, then the obliged person applies the following customer due diligence measures: (a) receives approval from senior management to establish a partnership or to continue business relationships with that person; (b) applies methods of customer due diligence measures to establish the origin of the material wealth and the sources of funds that are used in partnerships or that are used for the transaction; (c) monitors these partnerships in an enhanced manner of customer due diligence and conducts regular enhanced monitoring, except cases specified in legal acts.

10.6. If a politically exposed person of state-level no longer fulfills the public duties entrusted to him or her, then the obliged entity, for at least 12 months, must take into account the risks that have been associated with the person in question and apply the necessary and risk-based methods until it is sure that the risks inherent in a politically exposed person of a national level no longer arise.

10.7. The obliged entity may not apply the methods of customer due diligence described in this part to a politically exposed person of national level, to members of his or her family, and to persons who are considered his or her close associates, if no other circumstances are indicating the presence of other, higher than usual risks.

10.8. The obliged entity should establish the internal procedural rules based on which the decision shall be made whether the potential customer or the actual beneficial owner of the customer is a politically exposed person of state level, a politically exposed person of the local level of a county which is the contracting state of the European Economic Area Agreement or a third country or who performs or performed the public duties assigned to him or her in international organizations. The obliged entity should establish the close associates of a politically exposed person of state-level and members of his or her family only if their connection with the executor of important public duties is known to the public or when the obliged entity has reason to believe that such a relationship exists.

10.9. The obliged entity must apply the enhanced customer due diligence measures in addition to the necessary methods of customer due diligence with regard to a politically exposed person of state-level including the following methods:

10.9.1. require the additional information from the customer, as well as to apply all necessary methods to establish sources of wealth and money that are used to establish business relationships or when conducting a transaction

10.9.2. verify data or make inquiries to the relevant databases or open databases or make inquiries or verify data concerning the customer, or to the appropriate supervisory authorities at the customer's location or on official websites of government agencies. The following data should be checked primarily

10.9.3. a politically exposed person of local level can be checked on the proper website of the Financial Intelligence Unit

10.9.4. a foreign politically exposed person of national level can be identified using the Name Scan database which has a free access, or in any paid database (for example, Thomson Reuters, Member Check and others)

10.9.5. while checking a politically exposed person of local level, as well as a politically exposed person of national level, it is necessary to perform an additional check up using Google, and also using local search systems in the country of origin of the customer, by entering the customer's name and date of birth both in Latin letters and using the local language

10.10. The decision to establish a business relationship with a politically exposed person of national level must be taken by the management board of the obliged entity, the responsible member of the management board or the contact person. If a business relationship is established with the customer that will become later on or later it will become known that he or she or actual beneficial owner has become a politically important person of state level in the understanding of this guidance, then it is necessary to inform the management board, the responsible member of the management board or the contact person.

11. DATA RECORDS

11.1. The Company's policy mandates that any knowledge or suspicion of money laundering (ML) or financing of terrorism (FT) activities must be reported immediately to the Money Laundering Reporting Officer (MLRO). Employees are required to use the Internal Reporting Form provided in Appendix 2 to submit their reports:

11.2. Upon receiving an internal report regarding an unusual or suspicious transaction, the MLRO will:

11.2.1. Carefully review the details contained in the internal report.

11.2.2. Request additional information or clarification from relevant personnel when necessary.

11.2.3. Decide on the appropriate action to be taken based on the information provided.

11.3. For every report received, the MLRO is required to document each decision and the rationale behind it. This documentation ensures transparency and compliance and must follow the format outlined in Appendix 2.

11.4. If the MLRO determines there are reasonable grounds to suspect that:

11.4.1. A transaction may be related to money laundering or the funding of terrorism.

11.4.2. A person may be connected to money laundering or terrorist financing.

11.4.3. Money laundering or terrorist financing has been, is being, or may be committed or attempted.

11.5. The MLRO is required to prepare and file a Suspicious Transaction Report (STR)

with the relevant regulatory authority, such as the Financial Intelligence Unit (FIU) Curaçao. The STR must be filed as soon as reasonably practicable, but no later than five working days from the point at which the suspicion first arose.

11.6. The results of any investigation, as well as the fact that an STR has been filed, must not be disclosed or discussed with any person except those who have a legitimate need to know within the organization. Under no circumstances shall any employee, officer, or agent disclose or discuss any AML concern, investigation, or the filing of an STR with the person or persons who are the subject of the suspicion, or with any unauthorized third party. This restriction also extends to the employee's or agent's family members.

11.7. To comply with Curaçao AML/CFT regulations, the Company maintains accurate and complete records of all AML-related activities. These records include:

11.7.1. A copy of, or references to, the evidence of customer identity, including Ultimate Beneficial Owners (UBOs) or directors, as obtained during the due diligence process.

11.7.2. Supporting documentation and records concerning business relationships and occasional transactions subject to due diligence requirements

11.7.3. Internal reports submitted to the MLRO and external STRs filed with the FIU Curaçao.

11.7.4. Records of AML training sessions provided to employees, including attendance logs and training materials.

11.8. These records are preserved for a minimum period of five years, beginning on the date the business relationship with the customer ends. All records must be securely stored and readily accessible for inspection or audit by the Curaçao Gaming Control Board or other relevant authorities, as required by law.

12. DEPOSITS AND WITHDRAWALS OF THE CLIENT'S FUNDS.

12.1. When a client deposits funds into their account, they must act as the sender of the funds. The sender's name must match the name of the registered client associated with the account. The intermediation of third parties in the deposit process is strictly prohibited.

12.2. For withdrawals, the recipient's name must match the registered client's name, who is also the sender of the original funds. The recipient client must be the owner of the account from which the funds were debited.

12.3. Matching Accounts for Transfers: (a) Bank Transfers: The account from which the funds were originally deposited must be the same as the account to which the funds are withdrawn; (b) Online Transfers: For online transactions, the accounts used for deposits and withdrawals must also match to ensure consistency and prevent third-party involvement.

13. TRANSACTION MONITORING

13.1. Island Lukkly B.V. has implemented robust procedures for monitoring and reviewing transactions to identify activities that may be suspicious, high-risk, or otherwise unusual. These procedures ensure compliance with Curaçao's AML/CFT regulations and help detect transactions that may require enhanced scrutiny, special record-keeping, or reporting to the appropriate authorities.

13.2. The company employs automated and manual systems to monitor and analyze all money transfers, with a focus on detecting patterns or behaviors indicative of suspicious activity. This process is designed to flag transactions that fall outside normal or expected behavior, including but not limited to large sums, unusual transaction patterns, or activities linked to high-risk jurisdictions.

13.3. The following types of transactions will initiate an internal review and, if necessary, result in the filing of a Suspicious Transaction Report (STR) with the Financial Intelligence Unit (FIU) Curaçao:

13.3.1. Transactions by Known Suspicious Individuals: Transactions aggregating to over USD 5,000 by individuals previously identified as suspicious.

13.3.2. High-Value Aggregated Transactions: Any individual conducting transactions that aggregate to over USD 25,000, regardless of other risk factors.

13.3.3. Proceeds of Criminal Activity: Transactions involving funds known or suspected to be proceeds of criminal activities.

13.3.4. Unusual Behavior and PEP-Related Activities: Unusual transaction patterns that suggest account takeover, bribery, or corruption. Transactions involving individuals named on Politically Exposed Person (PEP) lists or their relatives/close associates.

13.4. Any individual identified as being from a high-risk jurisdiction (based on FATF and Curaçao-specific risk designations) will be added to a monitoring list. Transactions linked to such individuals or jurisdictions are flagged for additional scrutiny, ensuring early detection of suspicious activities.

13.5. Transactions flagged as suspicious or unusual are escalated to the Money Laundering Reporting Officer (MLRO) for further investigation. Based on the findings, the MLRO will decide whether an STR should be submitted to FIU Curaçao, following the timelines and procedures outlined in this policy.

14. SUSPICIOUS TRANSACTION/ACTIVITY REPORTING (STR/SAR)

14.1. Island Lukkly B.V. fully complies with the National Ordinance on Identification of Services (NOIS), the National Ordinance on the Reporting of Unusual Transactions (NORUT), and all guidance issued by the FIU Curaçao. Objective and subjective indicators issued under the Ministerial Decree are used to detect unusual transactions. Internal reports are filed within 24 hours and external reports with the FIU within 48 hours, as mandated. All employees are trained on reporting obligations, and failure to comply is subject to disciplinary action.

14.2. The primary goal of filing Suspicious Transaction Reports (STRs) and Suspicious Activity Reports (SARs), in the National Ordinance Reporting Unusual Transactions (NORUT), referred as unusual transactions, is to assist government authorities in identifying individuals, groups, and organizations involved in criminal activities such as terrorist financing, money laundering, and other financial crimes.

14.3. Island Lukkly B.V. adheres to the recommendations of the Financial Action Task Force (FATF) in all aspects of its operations and client relationships to maintain international AML/CFT standards.

14.4. The Money Laundering Reporting Officer (MLRO) is responsible for ensuring the company is properly registered with goAML, the online reporting portal of FIU Curaçao. All STRs and SARs are submitted through this system in compliance with local regulations.

14.5. The MLRO must file an STR or SAR with FIU Curaçao whenever there are reasonable grounds to suspect that a transaction is linked to criminal activity (subjective indicator) or based on an objective indicator (all transactions above XCG 4,000).

14.6. To identify unusual or suspicious transactions, the MLRO must refer to the Indicators List published by FIU Curaçao. This list provides specific criteria for determining whether a transaction may be related to money laundering, terrorism financing, or other illicit activities.

14.7. All suspicious transactions, including attempted transactions, must be reported, regardless of the transaction amount.

14.8. The MLRO is required to report suspicious transactions or activities to FIU Curaçao without undue delay, and in any case: (a) Within 48 hours after the transaction has been executed or an intention for a transaction has been identified, for reports based on an objective indicator; (b) Within 24 hours for reports based on a subjective indicator.

14.9. If FIU Curaçao determines, after analyzing an unusual transaction, that there is a reasonable suspicion of money laundering or terrorism financing, the case is escalated to the Public Prosecutor's Office. FIU Curaçao serves as an administrative intermediary, protecting the information submitted by reporting institutions. Only if there is sufficient evidence to

presume money laundering or financing of terrorism will the transaction details be forwarded to the Public Prosecutor's Office for further investigation.

15. LIST OF PROHIBITED PARTIES TO Island Lukkly B.V. TRANSACTIONS

15.1. Island Lukkly B.V. operates in multiple jurisdictions and adheres to the laws of various countries, including those enforcing international sanctions. The company is particularly obligated to comply with regulations issued by the U.S. Office of Foreign Assets Control (OFAC), which administers laws prohibiting business with sanctioned nations and blocked persons. Violations of these laws can result in severe civil and criminal penalties.

15.2. The company strictly prohibits engaging in transactions with individuals, entities, or nations included in any sanctions list maintained by the following authorities:

15.2.1. OFAC (U.S. Office of Foreign Assets Control): Comprehensive lists of blocked persons and entities, including embargoed nations, available at OFAC Website.

15.2.2. UK Sanctions List: Published and updated at UK Sanctions List.

15.2.3. EU Consolidated Sanctions List: Available at EU Sanctions List.

15.2.4. Sanctions National Ordinance (N.G. 2014, no. 55);

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

15.3. In accordance with the Sanctions National Ordinance, the Kingdom Sanction Law, and international standards, Island Lukkly B.V. screens all clients against updated sanctions lists (e.g., UN, EU, OFAC, Kingdom of the Netherlands). Sanctions screening is integrated at onboarding, during transactions, and periodically thereafter. Any potential match is escalated to the MLRO and, if verified, reported immediately to the appropriate regulatory body. Funds subject to sanctions are frozen and reported without delay.

15.4. Island Lukkly B.V. continuously monitors and updates its systems to ensure compliance with these and other applicable sanctions lists maintained by the United Nations, Australia, Canada, the European Union, Curaçao, and additional jurisdictions.

15.5. Each time a client attempts to conduct a transaction, Island Lukkly B.V.'s screening processes automatically compare the client's name against the aforementioned sanctions lists. The same process applies to similar lists maintained by international organizations and governments to identify restricted parties.

15.6. The Money Laundering Reporting Officer (MLRO) reviews all exact and partial matches flagged during the screening process. Obvious false positives are cleared by the MLRO without further action.

15.7. If it is unclear whether a match is true or false, the MLRO will request additional information from the originator or beneficiary of the transaction to clarify the matter.

15.8. Transactions involving true matches are reported to the regulatory authority responsible for maintaining the relevant sanctions list (e.g., OFAC, Curaçao FIU, or the EU regulatory body).

15.9. Depending on the applicable law, the company may be required to: Submit the associated funds to the respective regulatory authority. Hold the funds until further instructions are received.

15.10. Additional client information may be requested to aid in the evaluation process prior to releasing any funds or completing the transaction.

15.11. Island Lukkly B.V. also complies with responsible gaming requirements by screening against self-exclusion lists of individuals who have identified themselves as having a gambling addiction. The company prevents such individuals from creating an account or engaging in gambling activities to uphold responsible gaming practices. This dual-layered approach ensures compliance with both international sanctions and responsible gaming regulations, reflecting Island Lukkly B.V.'s commitment to legal and ethical standards.

CUSTOMER FORM

This form must be completed as part of Island Lukkly B.V.'s Customer Due Diligence (CDD) and Know Your Customer (KYC) procedures. All information provided will be treated as confidential and used solely for compliance with AML/CFT regulations.

Section 1: Personal Information	
Full Name (as per ID):	
Date of Birth:	
Nationality:	
Residential Address:	
Postal Code:	
Phone Number:	
Email Address:	
Government-Issued Identification:	
Type of ID (e.g., Passport, ID Card, Driver's License):	
ID Number:	
Expiration Date:	
Country of Issue:	
Are you a Politically Exposed Person (PEP)?	☐ Yes (If Yes, please specify your position/role) ☐ No
Section 2: Financial Information	
Source of Funds: (Please check all that apply and provide documentation where necessary.)	☐ Employment Income ☐ Business Income ☐ Investments ☐ Other (Please specify):
Purpose of Business Relationship:	☐ Gaming/Betting ☐ Other (Please specify):
Estimated Annual Turnover with Island Lukkly B.V.:	☐ Less than USD 10,000 ☐ USD 10,001 – USD 50,000 ☐ USD 50,001 – USD 100,000 ☐ Above USD 100,000
Section 3: Corporate Information (If Applicable)	
Company Name:	
Registration Number:	
Country of Incorporation:	
Ultimate Beneficial Owners (UBOs):	Full Name: Nationality: Ownership Percentage:
Directors (If Different from UBOs):	Full Name:

	Nationality: Position:
Section 4: Declarations	
Compliance with AML/CFT Regulations: I hereby declare that all funds deposited with Island Lukkly B.V. are lawful and are not derived from any criminal activities.	Signature: _____ Date: _____
Acknowledgment of Terms: I confirm that I have read and understood the terms and conditions of Island Lukkly B.V., including its AML/CFT policies, and agree to comply with them.	Signature: _____ Date: _____
For Internal Use Only	
Risk Assessment Outcome:	☐ Low Risk ☐ Medium Risk ☐ High Risk
Reviewed By (MLRO or Compliance Officer):	Name: _____ Signature: _____ Date: _____

INTERNAL REPORTING FORM

Confidential: For Submission to the Money Laundering Reporting Officer (MLRO)

This form is to be completed by employees of Island Lukkly B.V. when identifying transactions or activities that raise suspicion of money laundering or terrorist financing. Once completed, the form must be submitted directly to the MLRO for review.

Section 1: Reporting Employee Details	
Full Name:	
Position:	
Department:	
Date of Report Submission:	
Section 2: Transaction/Activity Details	
Customer Name:	
Account ID/Customer Reference Number:	
Transaction Date and Time:	
Transaction Type:	☐ Deposit ☐ Withdrawal ☐ Transfer ☐ Other (Specify):
Transaction Amount (USD/EUR):	
Account Details (if applicable):	
Source Account:	
Destination Account:	
Section 3: Description of Suspicious Activity	
Provide a detailed description of the activity or transaction that raised suspicion. Include any observed behavior, irregularities, or circumstances that may indicate potential money laundering or terrorist financing:	
Section 4: Supporting Documents	
Attach any relevant documents or evidence (e.g., transaction records, customer communications, identification documents).	☐ Transaction records ☐ Customer identification documents ☐ Screenshots or communications ☐ Other (Specify):
Section 5: Preliminary Assessment by Reporting Employee	
Briefly explain why this transaction or activity is considered suspicious. Include references to any applicable AML indicators or risk factors:	
Section 6: Employee Declaration	
I hereby declare that the information	Signature:

provided in this report is accurate to the best of my knowledge and has been submitted in good faith for further review by the MLRO.	Date:
For MLRO Use Only	
Date Report Received:	
Report Reference Number:	
Initial Review Outcome:	☐ False Positive (No further action required) ☐ Requires Additional Information/Investigation ☐ Suspicious Transaction Report (STR) to be filed with FIU Curaçao
Action Taken:	
MLRO Name:	
MLRO Signature:	
Date of Action:	

Confidentiality Notice: All information contained in this form is strictly confidential and must not be disclosed to unauthorized individuals, including the subject of the report. Unauthorized disclosure may result in disciplinary action and potential legal consequences.