

AML POLICY

ISLAND LUKKLY B.V.

Registration No: 166711

B2C gambling provider

Approving persons:	e-Management N.V., Director Yevhen Panov, UBO
Responsible Employee	Antonis Tsiattalos, Compliance Officer
Effective Date	October 5 th , 2025
Next review date:	October 6 th , 2026



e-Management N.V.
Managing Director

Table of Contents

INTRODUCTION. POLICY STATEMENT.....	3
Purpose.....	3
Audience.....	4
Non-Compliance and Enforcement.....	4
2. DEFINITIONS.....	5
3. INTERNAL CONTROLS.....	5
4. RISK ASSESSMENT.....	6
5. RESPONSIBILITY OF MONEY LAUNDERING REPORTING OFFICER.....	7
6. STAFF TRAINING.....	9
7. CUSTOMER DUE DILIGENCE.....	10
8. ENHANCED DUE DILIGENCE AND ONGOING MONITORING.....	12
9. POLITICALLY EXPOSED PERSONS.....	13
11. RECORD KEEPING.....	14
12. DEPOSITS AND WITHDRAWALS OF THE CLIENTS FUNDS.....	16
13. TRANSACTION MONITORING.....	16
14. SUSPICIOUS TRANSACTION/ACTIVITY REPORTING (STR/SAR).....	18
15. PROHIBITED PARTIES.....	19
United States: Office of Foreign Assets Control (OFAC)	19
European Union: Consolidated Sanctions List.....	19
United Kingdom: Office of Financial Sanctions Implementation (OFSI)	19
United Nations: Consolidated Sanctions List	20
Curaçao and the Kingdom of the Netherlands.....	20
Other Jurisdictions and Regulatory Bodies	20
Appendix 1.....	21
CUSTOMER FORM.....	21
Appendix 2.....	23
INTERNAL REPORTING FORM.....	23

INTRODUCTION. POLICY STATEMENT.

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.

The AML policy establishes 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.

The present 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.

Through the implementation of this AML 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.

Purpose

Risk Management: Identify, evaluate, and mitigate the risks associated with money laundering and terrorism financing

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

Data Management: Define clear responsibilities for collecting, managing, and securing data related to client due diligence activities.

High-Risk Identification: Provide guidance for identifying Politically Exposed Persons (PEPs), sanctioned individuals, and residents of high-risk jurisdictions.

Suspicious Activity Reporting: Establish methodologies for recognizing and reporting suspicious transactions to the appropriate authorities.

Technological Adaptation: Continuously evaluate and manage risks stemming from new technologies, services, and business models.

Account Holder Management: Outline the processes for collecting and maintaining accurate account holder information.

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

Audience

The present Policy applies to:

- All employees of Island Lukkly B.V.;
- Contractors and consultants engaged by the Company;
- Third-party service providers (e.g. PSPs, KYC/AML verification vendors);
- Any business partners operating under the Company's license framework.

Non-Compliance and Enforcement

Island Lukkly B.V. enforces a strict zero-tolerance policy for breaches of its Anti-Money Laundering and Counter-Terrorist Financing (AML/CFT) obligations. Every employee, contractor, and senior officer is personally responsible for understanding and adhering to this Policy. Failure to comply may result in disciplinary, legal, or regulatory consequences depending on the nature and gravity of the breach.

The Company's management and the Compliance Department maintain a structured internal enforcement framework to ensure accountability and consistency in addressing non-compliance. Any breach or suspected breach of AML/CFT procedures is immediately escalated to the Money Laundering Reporting Officer (MLRO) and, where appropriate, to senior management or the Board of Directors.

Consequences for non-compliance may include, but are not limited to:

- **Internal disciplinary action**, such as formal warnings, reassignment, suspension, or termination of employment or contract;
- **Performance review consequences**, including the removal of access to sensitive systems, the loss of compliance-related responsibilities, or exclusion from incentive programmes;
- **Mandatory retraining or compliance re-certification**, when the breach is due to negligence, lack of knowledge, or procedural misunderstanding;
- **Legal or regulatory action**, including administrative fines, criminal prosecution, or sanctions imposed by the Curaçao Gaming Authority (CGA), FIU Curaçao, or other competent authorities;

- **Business and reputational risks**, including licence suspension or revocation, contractual penalties, loss of banking or payment processing relationships, and reputational damage to the Company and its management.

The Compliance Department maintains detailed logs of all identified breaches, investigations, and disciplinary measures taken. All such actions are documented to demonstrate the Company's consistent enforcement of its compliance obligations.

Where systemic or repeated breaches are detected, the MLRO prepares a root-cause analysis and recommends corrective measures, such as additional training, process redesign, or enhanced oversight. The Board of Directors receives regular updates on the overall compliance performance and any material incidents of non-compliance.

Through this enforcement structure, Island Lukkly B.V. demonstrates a firm commitment to integrity, accountability, and transparency in all AML/CFT-related matters, reinforcing the Company's culture of compliance and ensuring alignment with the Curaçao Gaming Authority's expectations for effective governance.

2. DEFINITIONS

- **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:
- **Placement:** Cash first enters the financial system at the "placement"; stage, where the cash generated from criminal activities is converted into monetary instruments.
- **Layering:** How the link between funds and the criminal is concealed.
- **Integration:** Investing and/or recovering the funds in a way that looks legitimate
- **Money Laundering Reporting Officer:** a person 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.
- **Customer Due Diligence (CDD):** Procedures for identifying and verifying customer identities and assessing risk.
- **Politically Exposed Persons (PEPs):** Individuals holding prominent public positions or their associates.

3. INTERNAL CONTROLS

Island Lukkly B.V. maintains a comprehensive framework of internal controls designed to ensure compliance with Curaçao's Anti-Money Laundering and Counter-Terrorist

Financing (AML/CFT) requirements. These controls form the backbone of the Company's compliance culture, supporting the identification, prevention, and reporting of potential money laundering and terrorist financing activities within all operational processes.

The Company ensures that all internal controls are risk-based, proportionate to its size and business model, and consistent with the Curaçao Gaming Authority's (CGA) AML/CFT guidance and the Financial Intelligence Unit (FIU) requirements. Each department is responsible for integrating these controls into its day-to-day operations to ensure continuous compliance and operational integrity.

The effectiveness of the AML framework is subject to ongoing evaluation. To maintain independence and objectivity, Island Lukkly B.V. appoints an external qualified auditor or compliance consultant to conduct a comprehensive review of the AML Program at least once every two years. The review assesses the adequacy of the AML framework, evaluates the effectiveness of implemented procedures, and ensures alignment with current regulatory expectations and emerging risks.

All findings from such assessments are documented and presented to senior management and the Compliance Committee for consideration and corrective action. If deficiencies or areas for improvement are identified, the Company ensures timely remediation and follows up to verify the effectiveness of corrective measures.

Internal control mechanisms also include clear escalation procedures for suspicious or non-compliant activities, system-based transaction monitoring, dual-control principles for approvals, and restricted access to sensitive data. These mechanisms collectively ensure transparency, accountability, and integrity across all operational levels.

Senior management bears ultimate responsibility for ensuring that internal controls are adequate, effective, and proportionate to the nature, scale, and complexity of the Company's activities. Management also ensures that all employees understand their compliance obligations and that the AML framework remains an integral part of the Company's risk management and corporate governance systems.

4. RISK ASSESSMENT

Island Lukkly B.V. applies a comprehensive risk-based approach (RBA) in identifying and managing the risks associated with money laundering and terrorist financing. This approach is designed in accordance with the Curaçao Gaming Authority (CGA) requirements and the FATF Recommendations, ensuring that the Company allocates resources and implements controls proportionate to the nature and level of risk it faces.

The Company conducts an enterprise-wide risk assessment (EWRA) at least annually and whenever there are material changes to its products, services, technologies, or customer base. The assessment identifies the inherent money laundering (ML) and terrorist financing (TF) risks to which the Company is exposed, evaluates the adequacy of existing controls, and determines the residual risk that remains after mitigation. The

outcome of this analysis is documented, reviewed by senior management, and used to guide strategic decisions regarding AML/CFT compliance priorities.

The risk assessment process evaluates four main categories of exposure:

- **Customer Risk**, which considers the nature, background, occupation, reputation, and financial behavior of the customer, as well as potential political exposure or adverse media;
- **Geographical Risk**, which examines the jurisdictions with which the customer or transaction is connected, including countries identified by the FATF, the European Union, or the CGA as high-risk or under increased monitoring;
- **Product and Transaction Risk**, which assesses the complexity, transparency, and value of products and services offered, as well as the potential for misuse for money laundering or terrorist financing;
- **Delivery Channel Risk**, which takes into account how the customer interacts with the Company—such as remote or non-face-to-face onboarding, use of intermediaries, or third-party payment providers.

For each category, the Company determines inherent risk levels, evaluates the mitigating controls in place (such as customer due diligence, transaction monitoring, and sanctions screening), and calculates the residual risk. This residual risk is compared to the Company's **risk appetite**, as defined by the Board of Directors. Where the residual risk exceeds acceptable parameters, enhanced controls or additional mitigating measures are implemented.

The risk assessment also considers emerging threats and typologies identified by the CGA, FIU Curaçao, and FATF. These include the use of virtual currencies, payment intermediaries, affiliate marketing structures, and technological innovations within the iGaming sector. The Compliance Department ensures that these evolving risks are monitored and reflected in the Company's policies and systems.

All results of the risk assessment are documented in the **Risk Assessment Register** and made available for review by the CGA or FIU Curaçao upon request. The AML Compliance Officer ensures that the assessment remains a living document, continuously updated as new information or regulatory guidance becomes available.

Through this structured and dynamic approach, Island Lukkly B.V. ensures that AML/CFT risks are identified, understood, and effectively mitigated at every operational level, in full alignment with Curaçao's regulatory expectations.

5. RESPONSIBILITY OF MONEY LAUNDERING REPORTING OFFICER

Island Lukkly B.V. has appointed a qualified and independent Money Laundering Reporting Officer (MLRO), who serves as the central point of contact for all matters relating to anti-money laundering (AML) and counter-terrorist financing (CFT). The MLRO

is responsible for overseeing the Company's overall compliance with Curaçao's AML/CFT legislative framework, ensuring that all obligations established by the Curaçao Gaming Authority (CGA) and the Financial Intelligence Unit (FIU Curaçao) are effectively implemented and maintained.

The MLRO operates with full autonomy and has direct access to the Board of Directors and senior management. This ensures that the role is free from undue influence and has the authority to escalate AML/CFT concerns or breaches when necessary. The MLRO reports regularly to senior management on the Company's compliance status, identified risks, and any material breaches or suspicious activities.

Key responsibilities of the MLRO include the design, maintenance, and ongoing improvement of the Company's AML/CFT program. This includes implementing internal controls, coordinating periodic reviews of the compliance framework, and ensuring that the Company's procedures align with both local legislation and international standards. The MLRO oversees the development of customer due diligence (CDD), enhanced due diligence (EDD), sanctions screening, and transaction monitoring processes, ensuring their consistent and effective application.

The MLRO also serves as the primary liaison with FIU Curaçao and is responsible for ensuring that all reports of unusual or suspicious transactions are submitted promptly through the **goAML** platform, as mandated by Curaçao law. The MLRO reviews all internal reports of suspicious activity, conducts investigations to determine whether they meet the criteria for filing a Suspicious Transaction Report (STR), and ensures that such reports are submitted within the required timeframe. Where necessary, the MLRO coordinates with external authorities while maintaining strict confidentiality and protecting the integrity of the reporting process.

In addition to the reporting duties, the MLRO is responsible for maintaining a comprehensive record-keeping system for all internal and external reports, staff training records, and communications with regulatory authorities. The MLRO ensures that these records are securely stored and readily accessible for inspection by the CGA or FIU Curaçao.

A vital aspect of the MLRO's responsibilities is employee training and awareness. The MLRO develops and implements the annual AML/CFT training plan, ensuring that all staff members understand their roles in identifying and preventing financial crime. Training materials are regularly updated to reflect emerging typologies, regulatory updates, and internal procedural changes.

The MLRO also monitors the regulatory landscape and advises senior management on upcoming changes in Curaçao or international AML/CFT standards. This includes identifying gaps in the Company's compliance framework and recommending updates to policies, procedures, and systems.

Finally, the MLRO ensures that any identified deficiencies in the AML framework are promptly addressed and that remediation measures are tracked to completion. The MLRO's independence, expertise, and direct reporting line to senior management guarantee that Island Lukkly B.V. maintains a proactive and transparent compliance culture, fully aligned with the CGA's supervisory expectations.

6. STAFF TRAINING

Island Lukkly B.V. recognises that the competence and awareness of its employees are essential to the effective implementation of its AML/CFT framework. The Company therefore maintains a structured, ongoing training programme designed to ensure that all staff, regardless of their seniority or function, understand their obligations under Curaçao's AML/CFT legislation and the internal procedures established by the Company.

The training programme is coordinated and overseen by the Money Laundering Reporting Officer (MLRO) and the Compliance Department. It is delivered to all employees upon hiring and repeated annually thereafter, in line with the Curaçao Gaming Authority's (CGA) requirement for continuous professional development in AML/CFT matters. The purpose of this training is not only to provide theoretical knowledge, but also to build practical awareness of how to identify, assess, and report potential money laundering or terrorist financing risks within the context of online gaming operations.

The curriculum covers a wide range of topics relevant to the Company's business model and regulatory environment, including: the legal framework and regulatory obligations under Curaçao AML/CFT laws; the Company's internal policies and procedures; the identification of suspicious behaviour and transaction typologies; customer due diligence and enhanced due diligence practices; the identification and treatment of politically exposed persons (PEPs); sanctions screening; and the procedures for internal reporting to the MLRO.

The training content is regularly updated to reflect changes in legislation, FIU Curaçao guidance notes, and emerging typologies identified by the Financial Action Task Force (FATF). This ensures that employees remain informed about the latest trends and risk factors affecting the gaming and payments sectors. The MLRO also issues periodic internal bulletins to highlight relevant cases, enforcement actions, or typological updates that may enhance staff understanding of AML/CFT risks in practice.

All new employees must complete induction training before gaining access to customer or financial data. Employees working in higher-risk areas, such as payments, finance, and customer verification, receive additional specialised sessions tailored to their operational responsibilities. These targeted modules address the specific risks associated with high-value transactions, complex payment structures, and third-party service providers.

Training effectiveness is evaluated through short assessments, case study discussions, or scenario-based exercises. The Compliance Department monitors participation rates, assessment results, and feedback from attendees to measure the impact of the

programme. Employees who fail to complete or pass AML/CFT training are required to retake it promptly, and repeated non-compliance may result in disciplinary action.

The Company maintains comprehensive records of all AML/CFT training activities, including attendance logs, materials used, and evaluation results. These records are securely stored for at least five years and are available for inspection by the CGA or FIU Curaçao upon request.

Through this structured and continuously evolving training programme, Island Lukkly B.V. ensures that its workforce remains vigilant, competent, and fully capable of fulfilling the Company's obligations in preventing money laundering and the financing of terrorism.

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.

New employees are also 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.

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.

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. CUSTOMER DUE DILIGENCE

Island Lukkly B.V. applies a robust and risk-based Customer Due Diligence (CDD) framework to ensure full compliance with Curaçao's AML/CFT legislation and the guidance issued by the Curaçao Gaming Authority (CGA) and FIU Curaçao. The purpose of CDD is to verify the identity of customers, understand the nature of their activities, and ensure that their financial behavior is consistent with the Company's understanding of their profile and source of funds.

CDD is conducted before any business relationship is established or any transaction is processed. No player or business partner is allowed to access the Company's services until their identity has been satisfactorily verified. This applies equally to natural persons and legal entities. The Company does not accept anonymous or fictitious accounts under any circumstances.

As part of the identification and verification process, customers are required to provide the following information and documentation:

- Full legal name and surname;
- Date and place of birth;
- Nationality;
- Residential address (supported by a valid proof of address such as a utility bill, bank statement, or government-issued correspondence not older than three months);
- Valid email address and mobile phone number;
- Government-issued identification document (passport, national ID card, or residence permit);
- Confirmation of payment method ownership (e.g., screenshot or bank statement confirming the customer's name and account details);
- Declaration of the source of funds and, where applicable, source of wealth;
- For legal entities: certificate of incorporation or equivalent, company registration number, list of directors, and details of Ultimate Beneficial Owners (UBOs) including their identification documents.

All information provided must be verified against reliable and independent sources. Verification may be performed electronically through approved KYC platforms or manually by the Compliance Department. Certified or notarised copies of documents may be requested where necessary, particularly for high-risk customers or where automated verification is not possible.

The Company takes all reasonable measures to understand the purpose and intended nature of each business relationship, including details of the customer's occupation, income, and expected level of gaming activity. Deposits and withdrawals must always originate from and be directed to accounts held in the same name as the registered customer. Third-party transactions are strictly prohibited.

CDD measures are applied throughout the lifecycle of the customer relationship. Customer information is periodically reviewed and updated, especially when risk indicators change, when significant transactions occur, or when new information emerges. Both automated monitoring systems and manual reviews are used to detect unusual transaction patterns or inconsistencies that may signal elevated risk.

Where the Company's risk assessment identifies higher exposure to money laundering or terrorist financing, Enhanced Due Diligence (EDD) measures are applied. These

include additional verification of identity, detailed assessment of the customer's source of funds and wealth, and more frequent monitoring of their account activity.

Simplified Due Diligence (SDD) may only be applied in cases where the risk of money laundering or terrorist financing is demonstrably low and permitted under Curaçao law. In all cases, the extent of CDD measures remains proportionate to the assessed level of risk.

If a customer fails or refuses to provide the required documentation, or if the authenticity of the information cannot be confirmed, the relationship will not be established or will be terminated immediately. Such cases are escalated to the MLRO for review and potential reporting to FIU Curaçao.

Through this structured and transparent approach, Island Lukkly B.V. ensures that only legitimate, identifiable, and verifiable customers can access its services, in full alignment with the CGA's compliance standards.

8. ENHANCED DUE DILIGENCE AND ONGOING MONITORING

Given the elevated money laundering and terrorist financing risks inherent in the online gaming sector, Island Lukkly B.V. applies Enhanced Due Diligence (EDD) measures in all cases where a customer or transaction presents a higher-than-average risk profile. This approach aligns with the Curaçao Gaming Authority's (CGA) risk-based supervision principles and ensures that additional scrutiny is applied whenever risk indicators justify it.

Enhanced Due Diligence is applied in the following situations: when the customer is identified as high risk under the Company's risk assessment framework; when the customer or Ultimate Beneficial Owner (UBO) is a Politically Exposed Person (PEP), or a close associate or family member of one; when the customer's source of funds or wealth cannot be clearly established; when transactions involve high-risk jurisdictions as defined by FATF or the European Union; or when unusual or complex transaction patterns are detected that are inconsistent with the customer's known profile.

In such cases, the Company undertakes additional verification steps, which may include one or more of the following:

- Obtaining additional or alternative identification documents to confirm the customer's identity;
- Collecting more detailed information about the purpose and intended nature of the business relationship;

- Requesting verified documentation confirming the **source of funds** and, where relevant, the **source of wealth** (such as payslips, tax declarations, investment statements, or sale agreements);
- Conducting open-source and media checks to identify adverse information or reputational risks;
- Requiring the first transaction to be made from a bank account held in the customer's name in an EEA or FATF-compliant jurisdiction;
- Seeking senior management approval prior to establishing or continuing a high-risk relationship;
- Applying increased frequency of transaction reviews and periodic reassessment of the customer's risk profile.

The MLRO and Compliance Department document the rationale for applying EDD, the additional steps taken, and the outcome of each review. All actions are recorded in the customer's compliance file and retained in accordance with Curaçao's record-keeping requirements.

Ongoing monitoring forms an integral part of the Company's due diligence process. Island Lukkly B.V. continuously reviews customer activity to ensure that transactions are consistent with the Company's knowledge of the customer, their risk rating, and the expected pattern of behaviour. Automated tools are used to detect unusual or potentially suspicious activity based on transaction frequency, amounts, velocity, geolocation, or payment methods. These tools are complemented by manual reviews carried out by trained compliance staff.

Any irregularities, discrepancies, or patterns suggesting elevated risk are promptly escalated to the MLRO for assessment. Where necessary, the MLRO determines whether a Suspicious Transaction Report (STR) should be filed with FIU Curaçao.

Through the consistent application of Enhanced Due Diligence and ongoing monitoring, Island Lukkly B.V. ensures that all high-risk relationships are proactively managed, that red flags are promptly addressed, and that the integrity of the Company's operations remains aligned with Curaçao's AML/CFT regulatory expectations.

9. POLITICALLY EXPOSED PERSONS

Island Lukkly B.V. recognises that business relationships or transactions involving Politically Exposed Persons (PEPs) may pose a higher risk of money laundering or corruption due to their position and influence. In accordance with the Curaçao Gaming Authority (CGA) and FIU Curaçao guidance, the Company applies specific measures to identify, assess, and manage relationships with such individuals.

A Politically Exposed Person (PEP) is defined as an individual who holds, or has held, a prominent public function either domestically or internationally. This includes, but is not limited to, heads of state or government, senior politicians, members of parliament, senior government officials, judicial or military officers, senior executives of state-owned

enterprises, and high-ranking officials of international organisations. The definition also extends to **family members** (such as spouses, parents, and children) and **close associates** (persons known to have close business or personal relationships with a PEP).

The Company uses reliable screening tools and databases to identify PEPs during the onboarding process and throughout the customer relationship. Screening is performed automatically at account creation and is refreshed on an ongoing basis to detect any changes in a customer's status. Adverse media checks and name screening are also conducted using credible global databases and open-source intelligence.

When a customer or Ultimate Beneficial Owner (UBO) is identified as a PEP, the following Enhanced Due Diligence (EDD) measures are applied:

- Approval from senior management is required before establishing or continuing the business relationship;
- Additional information must be obtained to determine the source of funds and source of wealth, supported by reliable documentation such as tax declarations, payslips, or bank statements;
- The frequency and scope of transaction monitoring are increased to ensure that all account activity remains consistent with the Company's understanding of the customer's financial profile;
- The customer's risk rating is reviewed more frequently, at least every six months, or earlier if new information emerges;
- The MLRO documents the rationale for maintaining or discontinuing the relationship and ensures that all decisions are properly recorded.

If a person ceases to hold a politically exposed position, the Company continues to treat them as a PEP for at least 12 months, unless a documented risk assessment demonstrates that the relationship no longer presents a higher risk.

Where a PEP, family member, or close associate is identified, the MLRO must be notified immediately, and no transactions may be processed until the appropriate EDD measures are completed. If the source of wealth or funds cannot be satisfactorily verified, the relationship will not be established or will be terminated, and the case may be reported to FIU Curaçao as suspicious.

By applying a structured and consistent approach to the identification and management of PEPs, Island Lukkly B.V. ensures full alignment with the CGA's risk-based supervisory framework and international AML/CFT standards.

11. RECORD KEEPING

Island Lukkly B.V. maintains comprehensive records of all information collected and actions taken in connection with its Anti-Money Laundering and Counter-Terrorist Financing (AML/CFT) programme. Proper record keeping is essential to demonstrate

compliance with Curaçao's regulatory requirements and to provide a clear audit trail for the Curaçao Gaming Authority (CGA), the Financial Intelligence Unit (FIU Curaçao), and other competent authorities upon request.

All records are kept in a secure and readily accessible format, either electronically or in hard copy, in accordance with the Company's Data Retention and Security Policy. Access to such information is strictly limited to authorised personnel within the Compliance Department and senior management.

The Company maintains, at a minimum, the following categories of records:

- **Customer identification and verification data**, including copies of identity documents, proof of address, and Ultimate Beneficial Owner (UBO) information;
- **Records of transactions**, including deposits, withdrawals, transfers, and any other financial activity conducted through the Company's systems;
- **Internal and external reports**, including Suspicious Transaction Reports (STRs), Suspicious Activity Reports (SARs), and any supporting documentation or internal communications related to the case;
- **Risk assessment files**, including customer risk ratings, enhanced due-diligence documentation, and decisions made by the MLRO or senior management;
- **Training and awareness records**, including attendance logs, materials used, and evaluation results;
- **Audit and independent review reports**, documenting findings, recommendations, and remediation actions.

All AML/CFT records are retained for a minimum of **five years** after the end of the business relationship with the customer or the completion of an occasional transaction, whichever is later. Where required by law or requested by the CGA or FIU Curaçao, this retention period may be extended.

The MLRO ensures that records are maintained in a manner that allows for immediate retrieval when requested by regulators or law-enforcement authorities. The Company employs encrypted storage systems and secure servers located within approved jurisdictions to protect the confidentiality, integrity, and availability of AML-related data.

At the end of the retention period, records are securely destroyed using approved deletion or shredding methods, ensuring that personal data is handled in accordance with data-protection laws and internal privacy policies.

Through rigorous record-keeping practices, Island Lukkly B.V. ensures complete traceability of its AML/CFT activities and provides regulators with a transparent and verifiable compliance trail consistent with Curaçao's supervisory standards.

12. DEPOSITS AND WITHDRAWALS OF THE CLIENTS FUNDS

Island Lukkly B.V. maintains strict controls over all financial transactions involving customer funds to ensure that deposits and withdrawals are conducted only by verified account holders and in full compliance with Curaçao's AML/CFT framework. These controls protect both the integrity of the Company's financial systems and the transparency of its customer operations.

All deposits must originate from a financial account held in the customer's own name. The sender of the funds must be the same individual registered under the customer profile. Payments made by third parties or through anonymous methods are strictly prohibited. Similarly, all withdrawals must be transferred only to a financial account or wallet held in the same name as the verified account holder. Under no circumstances may funds be withdrawn or transferred to a third party.

Before processing any transaction, the Company verifies that the name associated with the payment method matches the verified identity of the customer. This verification process extends to both traditional and digital payment systems, including credit cards, e-wallets, and bank transfers. The Company employs automated systems to detect discrepancies or irregularities, and any mismatch automatically triggers a compliance review before the transaction is completed.

Where inconsistencies or red flags arise — such as payments from high-risk jurisdictions, unusual transaction patterns, or changes in payment instruments — the MLRO and Compliance Department conduct additional verification. This may include requesting proof of payment source, account ownership documentation, or bank statements confirming the origin of funds. If the authenticity or legitimacy of the transaction cannot be confirmed, the Company will block or reverse the payment and may file a Suspicious Transaction Report (STR) with FIU Curaçao.

The Company keeps complete records of all deposit and withdrawal activity, including transaction timestamps, payment provider details, and internal approvals, for a minimum of five years. These records are available for inspection by the Curaçao Gaming Authority or FIU Curaçao upon request.

Through these controls, Island Lukkly B.V. ensures that all client funds are handled securely, transparently, and in full alignment with Curaçao's AML/CFT and responsible gaming obligations.

13. TRANSACTION MONITORING

Island Lukkly B.V. maintains a comprehensive transaction monitoring system designed to detect, investigate, and report unusual or suspicious activity that may be indicative of money laundering, terrorist financing, or other financial crimes. The monitoring framework is built on a risk-based approach and integrates both automated detection systems and

manual compliance oversight to ensure continuous vigilance across all transactional activity.

All transactions, including deposits, withdrawals, transfers, and in-game movements of funds, are automatically screened using advanced monitoring tools. These tools apply pre-defined parameters and typologies aligned with the Financial Intelligence Unit (FIU Curaçao) indicators and the Curaçao Gaming Authority (CGA) guidance. The system is configured to flag transactions that deviate from the customer's established behavioural or financial profile.

Risk indicators that trigger alerts may include, but are not limited to: sudden spikes in transaction value or frequency; multiple rapid deposits and withdrawals without gameplay; frequent use of different payment instruments or currencies; activity originating from or directed to high-risk jurisdictions; and patterns suggesting potential structuring, layering, or misuse of gaming accounts.

In addition to automated screening, the Compliance Department performs periodic manual reviews of transaction data to identify trends or anomalies that automated tools may not detect. Transactions involving politically exposed persons (PEPs), high-risk customers, or new payment methods receive heightened scrutiny.

Each flagged transaction is reviewed by the Compliance team and, where appropriate, escalated to the Money Laundering Reporting Officer (MLRO) for investigation. The MLRO analyses the case, reviews supporting data such as account history, communications, and source-of-funds documentation, and determines whether the activity constitutes a reasonable suspicion of money laundering or terrorist financing.

If suspicion is confirmed, the MLRO prepares and files a **Suspicious Transaction Report (STR)** or **Suspicious Activity Report (SAR)** through the **goAML** portal in accordance with FIU Curaçao requirements. No STR or SAR is filed without the MLRO's approval, and strict confidentiality is maintained throughout the process.

The Company continuously updates its monitoring parameters to reflect emerging typologies, changes in regulatory guidance, and lessons learned from internal investigations or enforcement actions within the industry. The monitoring system is periodically tested and recalibrated to ensure it remains effective and proportionate to the Company's risk exposure.

All monitoring results, alerts, and STR/SAR filings are logged and retained for a minimum of five years in accordance with Curaçao's AML/CFT record-keeping obligations.

By combining advanced technological solutions with experienced human oversight, Island Lukkly B.V. ensures that all transactional activity is monitored in real time, that red flags are promptly investigated, and that any suspicions of financial crime are reported without delay, in full compliance with Curaçao's regulatory framework.

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

Island Lukkly B.V. maintains a clear and structured procedure for the identification, investigation, and reporting of suspicious transactions or activities. The objective of this process is to ensure that any activity potentially linked to money laundering, terrorist financing, or other financial crime is promptly detected and reported in accordance with Curaçao's AML/CFT legal framework and FIU Curaçao requirements.

All employees of the Company share responsibility for recognising and escalating unusual behaviour or activity. Staff members who identify a potentially suspicious transaction must immediately report it to the Money Laundering Reporting Officer (MLRO) using the Company's Internal Reporting Form. No employee should attempt to investigate independently or inform the customer of their concerns.

Upon receiving an internal report, the MLRO conducts a prompt and confidential review. The investigation includes examining transaction records, account activity, customer due-diligence information, communication history, and any other relevant data to determine whether the activity meets the threshold for suspicion.

If the MLRO determines that there are reasonable grounds to suspect that funds are linked to money laundering, terrorist financing, or related criminal conduct, a **Suspicious Transaction Report (STR)** or **Suspicious Activity Report (SAR)** is submitted to the **Financial Intelligence Unit (FIU Curaçao)** through the **goAML** online reporting platform. Reports are filed:

- within **24 hours** if the suspicion is based on a *subjective indicator* (an internal judgment that an activity appears unusual or inconsistent with the customer's known profile);
- within **48 hours** if the report is based on an *objective indicator* (a transaction meeting one or more FIU Curaçao pre-defined red-flag criteria).

All reports include detailed information on the parties involved, transaction type, date, amount, and a summary of the suspicious elements identified. Supporting evidence is attached to each submission. The MLRO ensures that the report is complete, accurate, and submitted within the required timeframe.

After submission, the MLRO maintains ongoing cooperation with FIU Curaçao, responding promptly to any requests for clarification or additional information. All communications with the FIU are treated as confidential and are documented within the Company's compliance records.

Strict confidentiality must be observed at all times. It is explicitly prohibited for any employee, officer, or agent of the Company to disclose, directly or indirectly, to the customer or to any unauthorised person that a suspicious report has been filed or that an

investigation is underway. This prohibition on **tipping-off** extends to all communications, including emails, phone calls, and verbal exchanges.

The MLRO keeps comprehensive records of all internal and external reports, investigations, decisions, and communications with FIU Curaçao for a minimum of five years. The MLRO also provides periodic summaries of reported cases and emerging patterns to senior management to improve internal awareness and strengthen the Company's risk-mitigation framework.

Through this structured STR/SAR process, Island Lukkly B.V. ensures full compliance with Curaçao's AML/CFT reporting obligations and contributes effectively to the jurisdiction's collective effort to combat financial crime.

15. PROHIBITED PARTIES

Island Lukkly B.V. is fully committed to ensuring that its operations and financial systems are not used to facilitate transactions involving sanctioned individuals, entities, or jurisdictions. The Company complies with all applicable international sanctions and restrictive measures issued by competent authorities, including those of the United Nations, the European Union, the United States, the United Kingdom, and Curaçao.

To achieve this, the Company performs automated sanctions screening on all customers, beneficial owners, and relevant third parties both at onboarding and continuously throughout the business relationship. Screening results are reviewed by the Money Laundering Reporting Officer (MLRO) and Compliance Department.

Island Lukkly B.V. strictly prohibits any direct or indirect business relationship, transaction, or service involving persons or entities listed under the following sanctions regimes:

United States: Office of Foreign Assets Control (OFAC)

The Company complies with all sanctions administered by the U.S. Department of the Treasury's Office of Foreign Assets Control (OFAC), including the Specially Designated Nationals (SDN) and Blocked Persons Lists. No business is conducted with individuals or entities appearing on these lists, nor with persons located in jurisdictions subject to comprehensive OFAC sanctions.

European Union: Consolidated Sanctions List

Island Lukkly B.V. adheres to EU Council Regulations and the EU Consolidated Financial Sanctions List. The Company screens all customers and counterparties to ensure they are not designated by the European Union for reasons including terrorism, proliferation financing, or human rights violations.

United Kingdom: Office of Financial Sanctions Implementation (OFSI)

The Company follows the UK Sanctions List maintained by the Office of Financial Sanctions Implementation (OFSI) under HM Treasury. This includes all financial and trade restrictions imposed by the UK government and applies to UK nationals and transactions processed through UK financial institutions.

United Nations: Consolidated Sanctions List

The Company observes the UN Security Council's Consolidated List of individuals and entities subject to sanctions relating to terrorism, proliferation, and other threats to international peace and security.

Curaçao and the Kingdom of the Netherlands

Island Lukkly B.V. complies with all sanctions adopted by the Government of Curaçao and the Kingdom of the Netherlands, including measures transposed from EU and UN resolutions. Screening tools are configured to detect matches against the national sanctions framework applicable to Curaçao-licensed operators.

Other Jurisdictions and Regulatory Bodies

Where relevant, the Company also considers sanctions and restrictive measures issued by other reputable authorities such as Canada, Australia, and FATF-designated high-risk or non-cooperative jurisdictions.

In the event that a sanctions screening match is identified, the MLRO immediately investigates to determine whether it is a true or false positive. Clear false positives are documented and closed. For confirmed or probable matches, the MLRO takes the following actions:

- Immediately freezes the relevant account or transaction;
- Notifies the appropriate regulatory or law-enforcement authority, including FIU Curaçao or the body maintaining the applicable sanctions list (e.g., OFAC or OFSI);
- Refrains from processing any transactions or releasing any funds until explicit authorization is received from the competent authority.

All sanctions-related alerts, investigations, and communications are documented and retained for at least five years. The Company also maintains an up-to-date sanctions policy, integrated into its broader AML/CFT compliance framework, and reviews it regularly to ensure alignment with evolving international obligations.

Through these measures, Island Lukkly B.V. ensures full adherence to global sanctions regimes, prevents prohibited transactions, and upholds Curaçao's integrity as a regulated iGaming jurisdiction.

Appendix 1

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 (specify) 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: _____

Appendix 2

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	
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 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.	Signature: _____ 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.