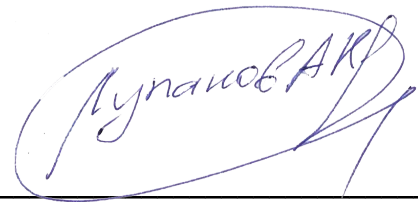


OPTIM DEVELOPMENT B.V.

Anti-Money Laundering And Terrorism Financing Prevention Policy



Alexei Lupanov, Director

Version 3.1
05/2026

Table of Contents

1. INTRODUCTION

1.1. Definitions

1.2. Policy purpose

2. SCOPE AND OBJECTIVE

3. APPLICABILITY

4. POLICY STATEMENT

5. VIOLATIONS

6. DEFINITION OF ML AND TF

7. MANAGEMENT OF ML/TF RISKS

7.1. Business risk evaluation and management

7.2. Risk Assessment Methodology

7.3. Risk Appetite Statement

8. INTERNAL CONTROL SYSTEM IN RELATION TO AML/CFT

8.1. Principles

8.2. Review and Audit

8.3. MLRO and Deputy MLRO Responsibilities

9. CUSTOMER RISK ASSESSMENT

9.1. Customer risk categorization

9.2. Prohibited Customers and Customer Acceptance Policy

10. KNOW YOUR CUSTOMER AND CUSTOMER DUE DILIGENCE

11. MONITORING AND CONTROL ACTIVITIES

11.1 Ongoing monitoring

11.2 PEP and Sanctions Screening

11.3 Targeted Financial Sanctions and Asset Freezing Procedures

11.4 Monitoring Alerts Handling and Escalation Procedures

12. UNUSUAL/SUSPICIOUS TRANSACTIONS REPORTING

12.1 Reporting through goAML System

12.2. Internal Suspicious Activity Register

13. TRAINING AND AWARENESS AND VETTING OF EMPLOYEES

14. RECORD-KEEPING

15. EXECUTION POLICY

16. POLICY REVIEW

1. INTRODUCTION

Optim Development B.V. (the Company) operates under Curaçao's regulatory framework and is fully committed to complying with the National Ordinance on Games of Chance (LOK), the FIU Curaçao requirements, and the guidelines issued by the Curaçao Gaming Control Board (GCB).

To ensure compliance, the Company follows these principles:

- Submission of Suspicious Transaction Reports (STRs) and Unusual Transaction Reports (UTRs) to FIU Curaçao in accordance with local reporting obligations.
- Implementation of risk-based customer due diligence (CDD) measures as per LOK and FIU Curaçao guidelines.
- Cooperation with the Curaçao Gaming Control Board (GCB) in providing ongoing reporting, audits, and compliance certifications.
- Ensuring that all record-keeping, risk assessments and AML/CFT procedures align with the LOK framework.
- The Company is registered with the goAML system and uses it as the official reporting channel for submission of Suspicious Activity Reports (SARs) and Unusual Transaction Reports (UTRs) to FIU Curaçao.

1.1. Definitions

For the purposes of this Policy, the following terms, definitions, and abbreviations shall be used:

AML/CFT	Anti-Money Laundering/Combating the Funding of Terrorism
Board/BOD	Board of Directors of each gaming operator
Business Relationship	Business relationship established with Customers for the provision of the Company's services with duration.
Criminal Activity	Any kind of criminal involvement in the commission of punishable criminal offenses as defined in AML Law including non exhaustively illicit drug trafficking, activities of criminal organisations, and corruption.
Customer	Natural person who has applied for or with whom a business relationship has been established for the provision of the Company's services.
EDD	Enhanced Due diligence
EU/EEA	Member States of the European Union and the European Economic Area (Iceland, Liechtenstein, and Norway).
FATF	Financial Action Task Force – an inter-governmental body the purpose of which is the development and promotion of national and international policies to combat ML/TF.

FIAU	Financial Intelligence Unit of EU country.
GCB	Curaçao Gaming Control Board
ML	Money Laundering
MLRO	Money Laundering Reporting Officer of Company

OFAC	Office of Foreign Assets Control of the US Department of Treasury which administers and enforces economic and trade sanctions based on policies of the United States of America
Politically exposed person (“PEP”)	means a natural person who is or who has been entrusted with prominent public functions and includes the following: a heads of State, heads of government, ministers and deputy or assistant ministers; b members of parliament or of similar legislative bodies; c members of the governing bodies of political parties; d members of supreme courts, of constitutional courts or of other high level judicial bodies, the decisions of which are not subject to further appeal, except in exceptional circumstances; e members of courts of auditors or of the boards of central banks; f ambassadors, chargés d'affaires and high-ranking officers in the armed forces; g members of the administrative, management or supervisory bodies of State-owned enterprises; h directors, deputy directors and members of the board or equivalent function of an institution of the European Union or any other international body. No public function referred to in points (a) to (h) shall be understood as covering middle-ranking or more junior officials

Prohibited countries	Afghanistan, Austria, Australia, Barbados, Belgium, Myanmar, Belize, Bulgaria, Czech Republic, China, Cyprus, Denmark, Estonia, Ethiopia, France, Great Britain, Greece, Grenada, Guiana, Germany, Haiti, Hong Kong, Iran, Israel, Italy, Indonesia, Jamaica, Lebanon, Libya, Macau, Nigeria, the Netherlands Antilles, North Korea, Portugal, Poland, Romania, Serbia, Slovenia, Spain, the Federation of Saint Kitts and Nevis, Saint Lucia, Saint Vincent, Sudan, Syrian Arab, Philippines, Trinidad and Tobago, Turkey, the United States of America, Vanuatu and Yemen.
LOK	National Ordinance on Games of Chance - Curacao regulatory framework
Shell Bank	Credit institution or an institution engaged in equivalent activities incorporated in a jurisdiction which it has no physical presence, involving meaningful mind and management, and which is unaffiliated with a regulated financial Company.
Sanctions	Restrictive measures aimed at preventing individuals, entities, or countries involved in illicit activities from accessing operator services. They require screening all parties against official sanctions lists to ensure compliance and prevent dealings with sanctioned entities.
TF	Terrorist Financing
UN	United Nations, an intergovernmental organization tasked to promote international cooperation and to create and maintain international order.

1.2. Policy Purpose

Financial Crime is a substantial threat to the integrity of financial services and products offered by companies, which can be abused to launder money or finance terrorist activities. It is the responsibility and obligation of the Company and all of its employees and officers to protect the Company against misuse of its business and its services for the conduct of criminal activity, money laundering purposes, for terrorist financing purposes and from attempts at contraventions of sanctions.

In order for the Company and its employees to safeguard the integrity of the Company at all times, the Money Laundering and Terrorism Financing Prevention Policy of the Company is established.

The Policy is designed to:

- Provide guidance to the Company and its officers and employees on the risks faced by the Company -
- Ensure appropriate management of the risks identified
- Detect and prevent possible attempts to abuse the Company's services for conduct of criminal activity,

money laundering purposes, for terrorist financing purposes and from attempts at contraventions of sanctions

- Ensure compliance with legal and regulatory requirements
- Ensure full cooperation with regulatory authorities
- Preserve the regulatory status and reputation of the Company towards national and international authorities, thereby also protecting the Company's partners and customers

The Policy lays down management procedures in relation to ML/TF risks arising as part of the conduct of its business and inherent to Customers. It further lays down:

- Principles and Measures to ensure ongoing compliance with the requirements introduced by the national and international laws, regulations, and sanctions regime
- Requirements on the implementation of a risk-based approach and risk assessment methodology, as well as its implementation in the context of conducting business, Customer risk and customer due diligence procedures
- Ongoing Customer and Customer activity monitoring principles
- Determination and reporting of suspicious transactions
- Internal control implemented by the Company
- Requirements on cooperation with regulatory authorities

2. SCOPE AND OBJECTIVE

This Policy is established to set high-level principles and standards to prevent the materialization, to mitigate and manage financial crime risks, which include money laundering, terrorist financing, and sanctions breaches.

The objectives of this Policy are :

- To ensure compliance with the national and international regulatory framework towards AML/CTF and for this purpose;
- To lay down the principles applicable to Company's framework of internal regulation that governs the Company's operations designed in accordance with legal and regulatory requirements.

The principles laid down in the Policy provide ground for elaboration of effective internal regulations to prevent, mitigate and manage risks of abuse of the Company's products and services for money laundering and terrorist financing purposes, and guarantee compliance with the regime on sanctions enforcement.

3. APPLICABILITY

The Policy applies to the operations of:

- Company's head office

- All Company offices, branches and other locations where the Company may establish operations.

This Policy and the Company's internal regulations stemming from it, which are developed in accordance with regulatory AML/CTF framework apply to all Company employees and officers wherever they are located in the performance of their duties.

4. POLICY STATEMENT

The company recognizes that financial crime is a substantial threat to the integrity of the services and products it offers which can be abused to launder money or finance terrorist activities.

The company is committed to contributing in the combat against money laundering and terrorist financing and to ensure that the services of the Company cannot be used for any illicit purposes.

Company shall conduct its business in conformity with high ethical and integrity standards and abide by all applicable laws and regulations on AML/CTF applicable to its operations in all jurisdictions they are conducted and has for this purpose:

- Established a risk-based AML/CTF approach which includes all necessary measures to mitigate against financial crime.
- Developed and implemented a comprehensive internal framework of policies, procedures, measures and controls to identify, manage and control risks that arise in the context of its business and at all stages of business relationships with Customers

To ensure compliance and prevent abuse of its services, the Company conducts its business in compliance with the following main general principles:

- The company takes reasonable steps to determine the true identity of all customers and ensure that none of its customers are subject to financial sanctions as listed by the EU, UN, OFAC, or another other applicable body established by which applies to the Company;
 - Company does not knowingly accept funds from, or engage in any business relations with customers whose money, Company reasonably believes, is derived from criminal activity;
- The company does not open anonymous accounts;
- Company does not cooperate with shell banks in any way possible;
 - The company monitors transactional activity of its customers to prevent the abuse of products and services for illicit purposes;
 - The company takes seriously any indications that a customer's money might potentially originate from criminal or other money laundering activities. If the Company becomes aware of facts that lead to a reasonable presumption that funds held by it are from criminal or other money laundering activity or that transactions entered into are themselves criminal in purpose, appropriate measures, consistent with the law, will be taken, including denial of provision of services to the customer, severing relations with the customer, closing or freezing transactions and filing of a suspicious activity report wherever required and appropriate;
 - Company does not support or assist customers seeking to deceive law enforcement agencies through the provision of false, altered, incomplete or missing information;
 - Company cooperates fully with law enforcement and regulatory agencies to the extent that it can under all applicable international and domestic laws; and,
 - Company reports all identified instances of suspicious activity to the extent that it can do so under all applicable foreign and domestic laws.

To ensure compliance with the above principles, the Company:

- Has appointed designated personnel responsible for compliance with anti-money laundering and terrorism financing provisions, including a Company Money Laundering Reporting Officer (MLRO), being a senior management position of the Company, independent in the performance of his duties and in the exercising of his own decisions. The MLRO, free from any conflicts of interest, is not a non-executive director, and the function is not outsourced.
- Established customer due diligence (“CDD”) and know your customer (“KYC”) procedures to be able to take reasonable steps in order to determine and verify the true identity of its customers, their economic profile, the source of funds and wealth.
- Established procedures for ongoing monitoring of its customers.
- Developed and implemented appropriate methods of control to detect suspicious activity of its customers and take appropriate actions.
- Established risk assessment procedures for identification of customers posing a high risk of money laundering where the application of enhanced due diligence (“EDD”) measures is required.
- Has identification and monitoring procedures in place to ensure that none of its customers are subject to local and international sanctions.
- Has procedures for identification and monitoring of customers falling in the category of PEP.
- Reports all identified instances of suspicious activity to government authorities in accordance with applicable requirements.
- Informs and trains all employees, including management, on the matters covered in this Policy.
- Complies with applicable requirements established by law for the obtaining of documents and record keeping.
- Cooperates fully with the government authorities to the extent that it can do so under all applicable foreign and domestic legislation.

Company’s officers and employees adhere to the company’s ethical and integrity standards as a condition of their employment with the Company and bear the responsibility of following the principles and provisions laid down in this Policy, developed in accordance with the framework towards AML/CTF and in ensuring full cooperation with Regulatory Authorities overseeing Company operations.

5. VIOLATIONS

Violations of the AML/CTF regime governing the Company’s operations can result in fines, lead to criminal charges, loss of licence, and sanctions for both the company and its officers and employees.

Any intentional violation of this Policy and relevant procedures and measures by any officer or employee of the Company will be considered by the Company to be a serious violation of terms of employment and the Company will take all appropriate steps, up to and including termination of the employment relations.

6. DEFINITION OF ML AND TF

In order to effectively comply with the regulatory framework, all employees are required to have a clear understanding of the process of Money Laundering and Terrorism Financing as well as the stages of the process that are considered to pose the greatest risk for the Company.

Money Laundering

Money Laundering is a process through which certain individuals convert illegal proceeds into legal assets by hiding their true criminal origin. If they succeed, they maintain control of their illegal proceeds and assets and provide legal cover on the source of their income.

Money laundering is an international problem which affects all countries. The criminals, in their effort to hide the source of their illegal income, may use payment institutions as well as a number of other professionals who may unknowingly assist them in legalizing their illegal gains.

Terrorism Financing

Terrorism Financing refers to activities, either legal or illegal, that provide financing or financial support to individual terrorists or terrorist companies, either locally or abroad, to support such an organization or solicit members or supporters for it. The source of funds for terrorism financing can be illegal or relatively legal, such as for example collection of membership dues and/or subscriptions; sale of publications; donations of a portion of their personal earning and etc. Often only small amounts are needed to commit acts of terrorism, increasing the difficulty of tracking the funds.

Generally speaking, the money laundering process, financing of terrorism, consists of three stages:

Placement - funds generated from illegal activities are placed into the financial system or retail economy or are smuggled out of the country. The aims of the launderer are to move the funds from its source so as to avoid detection from the authorities and to then transform it into other asset forms

Layering - funds are transferred or moved into other accounts or other financial institutions to further separate money from its illegal origin to concealment or disguise of the source of the ownership of funds by creating complex layers of financial transactions designed to disguise the audit trail and provide anonymity

Integration - the final stage in the process. It is at this stage at the money is integrated into the legitimate economic and financial system and is assimilated with all other assets in the system. Integration of the "cleaned" money into the economy is accomplished by the launderer making it appear to have been legally earned.

Gaming Operators can be used at any point in the money laundering or terrorism financing process.

Despite the fact that the Company does not accept cash, the Company is considered to possess higher risks at the layering and integration stages. Accordingly, when dealing with customers, potential customers, and customers' transactions, every relevant employee and officer of the Company needs to be alert to the possibility that customers may attempt to launder money using the Company's services.

Both money laundering and terrorism financing are considered criminal offenses, and merely facilitating such activities exposes the company, its employees, and officers to criminal liability which includes financial penalties as well as imprisonment for the individuals responsible.

To prevent the risk of money laundering and terrorism financing from materialising via the Company, a comprehensive set of Risk Management measures are implemented by the Company.

7. MANAGEMENT OF ML/TF RISKS

Laundering of proceeds of crime and financing of terrorism may arise diversely from various fields of activity. The implementation of a risk-based approach enables the Company to properly identify and measure the risks for potential money laundering arising from the Company's activities, prioritise risks, and allow for the appropriate actions to be taken in order to mitigate and control such risks.

7.1. Business risk evaluation and management

The company considers that the risk of the Company becoming unwillingly involved in ML/TF activity is related to the type of services it offers and differs depending on the service. Additionally, such risk can be effectively and efficiently mitigated and managed if the potential risk linked to the different services is known in advance. The company designs and implements measures and controls to mitigate such risks in relation to each of its services.

This also enables the Company to focus on services that present greater risks.

It is Company's responsibility to identify the inherent and residual risks of its ML/FT risks by applying pertinent risk factors and set out the respective mitigating controls to minimise such risks. The criteria and factors to be used for such categorisation shall be identified in line with regulatory requirements.,

7.2. Risk Assessment Methodology

The purpose of AML risk assessment is to identify, analyze, assess and mitigate any potential ML/FT risks and any other associated risks that the Company may be exposed to in relation to the laundering of proceeds of crime and financing of terrorism.

In conducting risk assessments, the company shall take into account risk factors emanating from the following primary categories:

- Customers;
- Countries or geographic areas;
- Products/services and transactions; and,
- Delivery channels.

The steps of the risk assessment methodology are as follows:

- Identification
- Analysis and Assessment
- Taking appropriate actions to ensure effective minimization or mitigation of identified risks.

This methodology also allows the Company to prioritise its actions and focus on risks presenting greater severity and likelihood of materialisation.

The company takes the appropriate measures required based on the business risk assessment ("BRA"). This consists of developing, implementing, and updating the internal control system in relation to AML/CFT. The control system is comprised of a set of comprehensive policies, controls, and procedures as well as undertaking necessary actions in response to the risks.

7.3. Risk Appetite Statement

The Company adopts a risk-based approach to the prevention of money laundering and terrorist financing and defines its risk appetite accordingly.

The Company has a low tolerance for money laundering, terrorist financing, fraud, sanctions violations and other financial crimes.

The Company does not knowingly conduct business with:

- individuals or entities subject to international sanctions;
- customers from prohibited jurisdictions;
- anonymous or unverified customers.

The Risk Appetite Statement is formally approved by the Board of Directors and is documented in Board meeting minutes.

It is reviewed at least annually or upon significant changes in the risk profile of the Company.

8. INTERNAL CONTROL SYSTEM IN RELATION TO AML/CFT

8.1. Principles

The company's Internal control system is built on a set of effective governing principles as its foundation: The company does not open anonymous accounts in fictitious names by adequately verifying the identity of its customers.

- The company applies due diligence in order to preclude at the outset cooperation with physical persons involved in money laundering and terrorist financing.

The company does not provide any services to customers until their identification and verification procedures have been completed, in the instances required by the local regulations. - The company subjects its Customers to a risk assessment and applies risk-based due diligence procedures commensurate with the risk category.

- The company ensures that the AML/CTF requirements are mandatory for all structural units, officers and employees of the Company, and in particular to all employees directly involved with customer communication and provision of services.

- The company ensures regular control over adherence to these principles and assessment of the effectiveness of their implementing elements and measures.

8.2. Review and Audit

Appropriate documentation of the business risk and customer risk assessments undertaken, and their results shall be kept for the purpose of ongoing monitoring of risks and their management. Application of, methodology and recording of the results of these risk assessments allows for a solid understanding of the inherent risks, as well as the subsequent evaluation of the effectiveness of the internal control measures implemented to mitigate and manage these risks.

Accordingly, the Company regularly assesses ML/TF risk and the applicable measures of the internal control in place for the prevention and suppression of money laundering and terrorist financing in order to determine the existing and residual level of the risk, and subsequently take appropriate corrective measures. Such overall assessments will ensure that the controls are effective and that the Company remains compliant with internal regulations and best standards.

Company is subject to an annual audit, the purpose of which is to independently assess the Company's

Operations. This audit shall cover the adequacy and appropriateness of the Internal Control System put in place by the Company for AML/CTF purposes, with reporting of findings as to compliance and recommended corrective actions to the Company's Board and the authorities.

8.3. MLRO and Deputy MLRO Responsibilities

The Company appoints a Money Laundering Reporting Officer (MLRO) responsible for the implementation and oversight of the AML/CTF framework.

In order to ensure continuity of AML/CTF functions, the Company also appoints a Deputy MLRO or establishes a documented succession framework.

The Deputy MLRO shall assume the responsibilities of the MLRO in case of absence, unavailability, or conflict of interest.

The Deputy MLRO has access to all necessary information, systems, and documentation required to perform AML/CTF duties.

The Company maintains a documented succession plan to ensure continuity of AML/CTF responsibilities at all times.

In the absence of both MLRO and Deputy MLRO, a temporary replacement is formally appointed by senior management.

9. CUSTOMER RISK ASSESSMENT

In line with AML/CTF requirements, this Policy and internal regulations putting it in effect, the Company has adopted Customer Risk Assessment Procedures for its implementation.

9.1. Customer risk categorization

Risks that are inherent in ML/TF can be managed effectively and efficiently if the potential risks linked to the different types of customers are understood in advance.

Having customers assessed and subsequently categorized by risk level enables the Company to adequately design and implement measures and controls that will assist the Company in properly mitigating these risks. Likewise, it will enable the Company to focus on customers that present a greater risk. In case a customer's risk becomes evident once the customer has started operating the account, monitoring of the customer's transactions is compulsory and fundamental to the application of the risk-based approach and in order to ensure appropriate measures are taken so as to mitigate/manage risks potentially materialising in the context of business relationships with Customers.

For this purpose, it is important to design and implement procedures for the risk assessment of customers in accordance to the level of ML/TF risk each customer presents in accordance with regulatory requirements by taking into account relevant factors including the reputation, nature and behavior of that customer. The criteria and factors to be used for such categorisation shall be identified in line with regulatory requirements and as explained in detail in the Business Risk Assessment ("BRA") of the Company. The timing for such customer risk assessment will be carried out depending on the requirements of national regulations, i.e. upon reaching the 2000 EUR threshold or at the onboarding of customers, and will be continuously updated

throughout the course of the customer business relationship. Each customer risk assessment will determine a risk score (High/Medium/Low) and the appropriate level of CDD measures to be applied.

Customer Risk Assessment methodology for ML/TF risks

The assessment is applied to all customers, with the following criteria taken into consideration: - **Geography risk.** The geographical location of the customer domicile, locations where the customer registers/logins from;

- **Product/Service & Transaction Risk.** Products and services provided to the customer, i.e. games types, net loss amounts, betting patterns, deposit/betting amount ratio

- **Payment Method Risk.** Payment methods being used, number and frequency of payment methods used/changed, whether the same payment method is used for deposits and withdrawals (and the reason for usage of different payment methods), deposit amount per transaction/ total deposits within a specific period of time, deposits/withdrawal ratio;

- **Customer risk.** This refers to the type of Customer that the Company is dealing with and confirms whether the customers fall under the PEPs category, High Net Worth Individuals, public figures, subject to adverse media findings, working/having business in high risk areas (i.e. unemployed, working/owning cash-intensive business, real estate, pharma, precious metals, crypto-related activities, Cannabis/CBD, dating/adult industry, companies doing business in high risk jurisdictions), customer's age; and,

- **Interface risk.** The method/channel used for interacting with customers: face-to-face or non-face-to-face.

Each risk category is then divided into subcategories, as follows

- Geography Risk:

- o Country of residence
- o Country of main business activity, if applicable
- o Country where the source of wealth is generated from, if applicable

- Product & Transaction Risk:

- o Type of games used
- o NetLoss amounts
- o Deposit/Betting ratio

- Payment method Risk:

- o Payment methods used
- o Number and frequency of changing the payment methods;
- o Single deposits amount;
- o Total deposits within a specific period of time;
- o Deposit/Withdrawal ratio

- Customer Risk:

- o Age
- o PEPs
- o Sanctions hits
- o Employment/involvement in high-risk business activities
- o Reputation, i.e. adverse media findings, public figures
- o BankID Registration
- o Verified customers

- Delivery Channel/Interface Risk:

- o Non -face -to- face

The different risk variables within each of the four risk categories and their subcategories are each awarded a score on a scale from 1 to 20, with extra high-risk triggers of 50 scores, where a score of 1 is the variable that poses the lowest risk and a score of 50 is the variable that poses the highest risk.

Once the scoring for each key risk category is calculated (i.e. by summing up the scoring of each sub-category), the Customer is then assigned with the overall Risk Score.

Upon calculation, every customer is assigned an internal risk level (Low, Medium and High) depending on the customer's profile.

In cases where the Company has determined that the customer is risk rated as High based on the CRA in place, Company has developed and implemented enhanced due diligence measures ("EDD") to be applied for such customers as part of its mitigation and minimisation measures. EDD measures to be applied will depend on the high-risk scenarios portrayed by that particular customer and will be different on a case-by-case basis.

9.2. Prohibited Customers and Customer Acceptance Policy

The Company does not establish a business relationship with, nor allows transactions from:

- Customers who are included in Curaçao FIU blacklists or FATF high-risk jurisdictions.
- Customers from jurisdictions that are subject to international financial sanctions (UN, EU, OFAC).
- Individuals identified as Politically Exposed Persons (PEPs) without Enhanced Due Diligence (EDD).
- Customers who refuse to provide the necessary identity verification documents or whose source of funds cannot be verified.
- Countries explicitly prohibited under Curaçao gaming regulations, including but not limited to: North Korea, Iran, Syria, Myanmar, and jurisdictions with AML deficiencies identified by FIU Curaçao.

The Company reserves the right to terminate any existing customer relationships if new regulatory sanctions arise or if the customer engages in activities that pose a financial crime risk.

Based on the business model of the company, i.e. online operations, the Company uses only non-face-to-face delivery channel and verifies its customers remotely via the technology provider.

- Customer categories and individual Customers who by their nature present excessive risks determined as non-acceptable in accordance with the Company's CRA procedures.

In the above circumstances, the customer business relationship is terminated by closing the account. The case might merit the raising of a suspicious transaction report ("STR") to the FIU and the returning of funds to the customer or the blocking of funds.

10. KNOW YOUR CUSTOMER AND CUSTOMER DUE DILIGENCE

Taking into consideration the potential risk for the Company to be used unwillingly as a channel for money laundering or terrorist financing processes, the Company is obliged to conduct customer identification and due diligence procedures in order to obtain adequate information regarding the customer.

Accordingly, the Company performs necessary controls and takes additional measures with respect to the:

- Identification and verification of the identity and address details of customers;

- Consistency between the income levels of customers, the activities they perform;

- Understanding the purpose and intended nature of the business relationship;
- Obtaining the source of funds, and source of wealth information where required;
- Possibility of the customers being involved in criminal and illicit activities or participating in ML/TF activities; and,
- Possibility of customers being included on national/international sanctions lists. Customers are screened for any financial sanctions, by using a third-party screening platform, at first deposit request and throughout the course of the customer business relationship

The company stops any business relations if the identification and verification of the Customer cannot be completed or where sufficient information is not obtained. The business relation should be terminated after 30 days (might be exceeded on an exceptional basis) of no response by the customer or where there is any suspicion related to the sufficiency and accuracy/authenticity of the previously obtained identity details of the customer.

Company's standard KYC and due diligence process at a minimum of measures include:

- Identification and verification of customers' identity details such as customer's full name, date of birth, identification number and residential address, email and mobile number.
- Screening of the customers for prevention of the risk of them being involved in the criminal, illicit activity or participating in ML/TF activity or processes. Documentation of searches carried out regardless of a match or not is kept as regulatory evidence (also indicating dates of when these were carried out).
- Screening of the customers to prevent of the risk of them being on national/international sanctions lists. Documentation of searches carried out regardless of a match or not will be kept as regulatory evidence.
- Determination of whether the customer is a politically exposed persons (PEPs). - For medium and high risk customers: identification and verification of the source of funds and source of wealth of the customers, substantiated with supporting documentation(for high risk). - Monitoring of customer transactions for detection of unusual transactions and monitoring of the updating of customer's information and data;
- Performance of periodic reviews of customer files; low risk: every 1.5 years; medium risk: every 1 year; and low risk: every 6 months.

Customer due diligence requirements depending on the risk level should consist of the following:

Low Risk

- Identity verification.
- Address verification.
- Payment Method ownership verification.

Medium Risk

- Identity and Address Verification shall obligatorily be performed via photograph. - Identity document.
- Proof of Address document.
- Payment Method ownership verification.
- Collection of Source of Wealth information.

High Risk

- High Risk Customers should undergo Enhanced Due Diligence, i.e.:
- Collection and verification of Identity documents.

- Collection and verification of Proof of Address document.
- Payment Method ownership verification.
- Source of Wealth information collection.
- Source of Wealth verification (collection of documentation).
- Provision of Selfies, if required
- Provision of Transaction Histories for any period of time
- Enhanced monitoring of the activity by KYC and Risk Teams

The onboarding procedure for the customers - natural persons should be performed remotely via the Company's e-Wallet system, i.e. by a mobile application.

In order to be granted an e-wallet account, the prospective customer will go through the identification and verification procedure. The procedure is as follows:

1. Register in the system by providing his personal details.
2. Upload his identification documents, and proof of address and complete online face scanning.
3. The system will immediately perform sanctions, PEP, adverse media screening of the potential customer as well as checks regarding the authenticity of the submitted documents and perform face recognition.
4. In case of potential screening matches, the Company will perform manual checks and further analysis on the customer.
5. If there are no potential alert matches, and the automatic ID and face verification are in order, the customer will be automatically approved and be able to complete the account opening form by providing information about the purpose of the account opening and expected usage (turnovers, currencies, geography), allowing Company to build a robust customer and risk profile and perform a CRA.
6. SOW and SOF verification should be performed at the outset of the business relationship
7. In case of High-Risk customers, additional manual assessment should be performed by AML function and further documentation requested (SOF/SOW detailed confirmations, business contracts etc) during the onboarding process.

The company conducts simplified due diligence ("SDD") measures to its customers only when the risk they are posing is low. In such instances the Company will limit itself by obtaining minimum personal information on the customer: full name, date of birth, and permanent residential address, and verify such information with reliable and independent documentation. SDD measures are not permitted for medium and high-risk scenarios.

In addition, enhanced due diligence measures are applied for customers possessing a high-risk as the result of the CRA performed or in instances prescribed by law as follows:

1. In relation to activities or services determined as high risk by the Regulator or/and FIU;
2. In the case of PEPs, their family members and persons known to be close associates;

The list is not exhaustive, EDD measures may include:

- Obtaining additional information and performing additional verification measures on Customers, i.e. enhanced adverse media searches, searches on the business activity, and searches in social networks.
- Obtaining a non-criminal record of UBO/other controlling persons (where required) or the Customer natural person himself.
- Additional scrutiny of the economic profile of the customer and in particular its correlation with volumes and level of transactions conducted with the Operator.

- Verifying source of wealth and funds (e.g. bank statements, pay slips, tax declarations and etc). -
- Increasing the frequency of periodic reviews.
- Enhanced account and transaction monitoring.

In the event where customers are politically exposed persons (“PEPs”), which are always to be treated as high risk, the following EDD measures are to be applied:

- Obtaining senior management approval;
- Establishing the source of wealth and source of funds of the PEP; and,
- Carry out enhanced ongoing monitoring.

Depending the type of PEP client, the measures to be carried out may be lighter.

In a nutshell, the Company is applying:

- SDD for Low-Risk customers;
- Normal CDD for Medium Risk customers; and,
- EDD for High-Risk customers.

The company does not accept any customers falling into Extra High Risk Category.

11. MONITORING AND CONTROL ACTIVITIES

11.1 Ongoing monitoring

Ongoing monitoring of customers’ activities and transactions is a critical aspect that the Company has adopted within its AML/TF framework. Robust, efficient and pertinent monitoring ensures that the Company identifies and manages ML and TF risks efficiently and that any potential new risks are identified in a timely manner.

The company does not accept cash deposits and does not provide cash transactions.

To comply with FIU Curaçao's AML/CFT regulations, the Company maintains a real-time transaction monitoring system, utilizing:

- Automated risk alerts for deposits and withdrawals above EUR 2,000.
- Unusual gaming patterns, including sudden spikes in bets, rapid withdrawals, or dormant accounts reactivating with large transactions.
- Automated flagging of repeated self-exclusion violations, bonus abuse, and fraudulent identity use.
- Review of customer accounts every 6 months for high-risk players.
- Identification of linked accounts based on IP, payment methods, and geolocation data.

Suspicious transactions are flagged for manual review, and reports are escalated to FIU Curaçao within 24 hours if necessary.

These alerts require AML Officer assessment and further actions as follows:

- AML Officer review
- Request for additional information/documents prior to proceeding
- Escalation to MLRO

- Pre-execution alerts, requiring manual investigation, will have to be reviewed and processed as soon as possible but no later than 3 working days once triggered.

Post-transaction monitoring alerts, requiring manual reviews and investigation, should be checked, escalated (if necessary), and closed within 3 working days from the day when they were triggered.

In both cases, the AML Officer may request to obtain and provide explanations/supporting documents from the Customer and update the Customer's profile, where necessary.

In addition to automated alerts and triggers implemented, the ongoing monitoring procedure should contain a list of examples of potentially suspicious transactions/activities related to ML/TF, such as refusal to provide supporting documentation, frequent changes of payment methods, etc. The list is non-exhaustive and is updated constantly. It assists all responsible departments in recognizing the main methods or red flags of ML/TF. Additionally, the MLRO circulates information in this regard on an ongoing basis.

Furthermore, if any responsible employees encounter anything suspicious under prevention of laundering of proceeds of crime and financing terrorism, customers shall undergo increased scrutiny as set in the applicable Company's internal procedures without tipping them off.

11.2 PEP and Sanctions Screening

The company strictly complies with EU and international regulatory requirements, including official blacklists and sanctions lists of competent authorities (FATF, UN, EU, OFAC, UK HM Treasury – Office of Financial Sanctions Implementation (OFSI), and the Australian Department of Foreign Affairs and Trade (DFAT)) against countries, legal entities, financial institutions and natural persons.

The screening procedure, taking place at first deposit and throughout the course of the business relationship, includes screening against Sanctions Lists, PEP Lists, and adverse media sources. All screening checks, be it matches or no matches, are kept on file (also evidencing dates) as per local record-keeping obligations.

The name and surname are screened by a 3rd party provider *Onfido* (onfido.com), which is integrated into the Company Platform. *Onfido* is an AI-based technology which assesses whether the customer's government issued ID is genuine or fraudulent and then compares it against facial biometrics. The technology extracts the name and surname of the customer and screens it against various databases (more than 130 sanctions lists, warnings and regulatory enforcement lists, PEPs, RCAs, and adverse media datasets), which are provided by IVXS UK Limited (complyadvantage.com). The solution allows monitoring in real-time the full spectrum of critical sanctions lists. Once there is a match (full or partial, true or false) the alert is generated to inform a responsible employee of KYC Team, who performs further in-depth investigation of the match.

Sanctions and PEP Screening of Customers shall be performed:

- individually during verification/ identification process;
- individually upon first deposit request;
- individually during periodic reviews;
- the whole client database annually;
- in every case when new data is released/available in relation to sanctions; and,
- wherever instructed by the Authorities.

Wherever a match with a sanctioned individual is determined to be a true match, the following steps will take

place:

- Relationship with the Customer are terminated or not established;
- MLRO informs Management;
- MLRO shall file a report to relevant FIU, if apart from the customer being sanctioned, there is also knowledge or suspicion on AML/CFT; and,
- MLRO shall report to the respective governmental agencies for further guidance in relation to blocking of the account and freezing of funds.

Wherever a PEP is identified, the following steps will take place:

- Senior management approval to service the PEP should be obtained;
- Source of wealth and, where applicable, their source of funds should be established; - Enhanced ongoing monitoring of the customer's activity should be conducted.

To avoid the risks of being used as a vehicle for sanctions contraventions or financing of terrorism, **the company maintains a zero-tolerance approach to any sanctions matches it identifies**. The Company also refuses to conduct business in any comprehensively sanctioned country, or with any sanctioned individual or legal entity, where it can be reasonably established that the match is genuine.

11.3 Targeted Financial Sanctions and Asset Freezing Procedures

In the event that a customer or transaction is identified as matching an individual or entity listed on applicable sanctions lists (including but not limited to UN, EU, OFAC or other applicable sanctions lists), the Company shall immediately take appropriate measures.

These measures include:

- Immediate suspension of the customer account and restriction of transactions;
- Freezing of any funds or assets associated with the sanctioned individual or entity;
- Immediate escalation to the MLRO;
- Notification to the competent authority or Financial Intelligence Unit where required by applicable law.

The MLRO is responsible for ensuring that appropriate sanctions procedures are followed and that all required notifications are made without delay.

The Company ensures that asset freezing is performed without delay and without prior notice to the customer.

All actions are taken in accordance with applicable sanctions laws and regulatory obligations.

The Company ensures immediate notification to the relevant competent authority where required and maintains records of all actions taken.

11.4 Monitoring Alerts Handling and Escalation Procedures

The Company utilizes automated and manual monitoring mechanisms to detect unusual or suspicious transactions.

Monitoring alerts generated by the system are reviewed by the responsible compliance personnel.

The alert handling process includes:

- initial review of the alert;
- collection of additional information where necessary;
- escalation to the MLRO if the alert cannot be reasonably explained;
- filing of a Suspicious Activity Report where required.

Escalation thresholds and timelines are clearly defined.

High-risk alerts must be escalated to the MLRO immediately and no later than within 24 hours.

All decisions and actions must be documented, including rationale for closure or escalation.

12. UNUSUAL/SUSPICIOUS TRANSACTIONS REPORTING

A Suspicious Transaction is evaluated on several factors which indicates that the transaction is extraordinary or conspicuous in nature in comparison with the Customer's known activity. Such unusual behavior is often an indicator or red flag of illicit activity taking place.

An Internal AML Report ("AML Report") is drawn up from respective employees by providing detail on the suspicious transaction or activity of that customer and is submitted to the MLRO for his further analysis and evaluation.

In relation to the scope of suspicious transaction identification and reporting, the Company's ongoing monitoring procedures:

- Require that AML function have an understanding of the normal and reasonable account activity of each customer (i.e. correlation with the monthly income of the customer if available);
- Require immediate submission of internal suspicious AML reporting to the MLRO for further investigation, whenever AML Officer and/or an employee generally dealing/communicating with the customer discovers signs of a transaction/activity being suspicious and determine that such transaction:
 - Could be related to funds derived from criminal activities or be designed to hide or disguise funds or assets derived from such activities;
 - Could compromise funds which directly or indirectly are to be used, totally or partially, to commit terrorism activities;
 - Are divided or structured to evade the reporting or record-keeping requirements of the applicable AML and TF laws and regulations.
- MLRO decision on reporting/non-reporting to the relevant governmental agencies and execution/non-execution of the transaction is clearly documented on the Report Report;
- In case of suspicion or knowledge of the transaction being related to ML/TF, SAR/STR report is submitted by MLRO to the relevant governmental agency 'promptly' (1 working day) through applicable channel (go AML portal), in accordance with respective procedure implemented by the authorities.

The investigation commenced by AML Officer shall include:

- Detailed analysis of the profile of the customer, its activity on the account
- Analysis of supporting and related documentation (proof of wealth, source of funds etc.) - Screening Results and publicly or commercially available information
- Analysis of conformity or lack thereof between customer's profile and transaction.

The employee who submitted the Internal Report is prohibited from discussing any aspects of the report with other employees of the Company apart from Executive Management, and from informing the customer about investigation in process due to 'tipping-off'. Any information provided to the customer in relation to delay/non-execution of the transaction may only be provided based on MLRO instructions after having communicated with the relevant authorities.

12.1 Reporting through goAML System

The Company confirms that it is duly registered with the goAML platform and uses it as the formal and exclusive reporting channel for submitting SARs/STRs and UTRs to FIU Curaçao.

All reporting is performed strictly in accordance with FIU reporting procedures and timelines.

12.2. Internal Suspicious Activity Register

The Company maintains a formal register of suspicious activity reports and internal alerts.

The register shall be maintained in a structured format (electronic system or secure database) and shall include:

- Unique reference number;
- Date of internal report;
- Reporting employee;
- Description of suspicion;
- Actions taken;
- MLRO decision;
- Date of submission to FIU (if applicable);
- Status (open/closed).

The register is maintained by the MLRO and is kept confidential. Access to the register is restricted to authorized personnel only.

13. TRAINING AND AWARENESS AND VETTING OF EMPLOYEES

The company has in place adequate and appropriate systems and specific procedures for the ongoing education and training of staff with regards to the relevant regulatory framework on prevention and suppression of money laundering and terrorist financing.

Special attention is given to the training of the employees who deal with customers, so they are able to recognise and handle transactions and activities suspected of being related to ML/TF.

All new joiners receive training as part of the induction process. Further training is provided periodically (at least annually) and ad-hoc (in case of an update of the regulatory framework, best standards or practices) so as to ensure all personnel is able to meet the Company's requirements and is aware of their responsibilities with regards to AML at all times. Focused AML/CFT training is also provided to the different lines of defense of the Company depending on their area of expertise.

For these purposes AML training covers the following areas:

- The concepts of laundering of proceeds of crime and financing of terrorism
- Requirements of the local and EU Law and Directives with regards to ML/CTF - The Company's Anti-Money Laundering Policy
- Internal systems and procedures for the prevention of money laundering and terrorism financing - Principles with respect to customer due diligence
- Statutory obligations of the Company and its employees to report suspicious transactions and to refrain from activity that would result in money laundering
- Recognition and handling of suspicious transactions and activities
- Sanctions to be applied in case of any failure to observe and fulfill the obligations.

The MLRO is to keep a training log (which includes the material and certification) and is to ensure that yearly training is being carried out/undertaken.

It is important that Company is aware of the potential for any of its managers, internal or external staff (“employees”) to engage in ML/TF conduct or assist somebody outside the Company in the foregoing. To prevent and detect any potential misbehavior by an employee, it is the policy of the Company to have stringent processes for employing new staff and for observing all relevant staff operations. The Company should consider the potential for risk associated with money laundering or terrorism financing in relation to individual positions in the organization and apply the appropriate employee due diligence and screening in each case.

The company is to screen new and existing employees.

- When employing a new person, the Company should collect the following information applicable to the person: the name; date of birth; current address; an identification number, which will be a government-issued identification number or one or more of the following: passport number and country of issuance, resident identification card number or number and country of issuance of any other government-issued document evidencing nationality or residence and bearing a photograph or other similar safeguard. The Company may collect other information applicable to the new employee. - Screening processes for employees should be done in advance of making any offer of employment and include:

- Verification of name, address, and date of birth;
- A criminal and PEP history check using an online database;
- Verification of academic qualifications and professional memberships (if any).

There may be instances where further screening is required once an individual has joined the Company. These could include a transfer to a position with additional responsibilities or regulatory requirements. Company checks may be similar to those outlined above but may not require as much detail as the initial screening checks. Post-employment screening checks must be reasonable, proportionate, and meet the Company’s business requirements. They should not be used as part of an ongoing investigation or disciplinary procedure.

Company is to screen any freelance or contract employees and consultants using similar screening criteria, to mitigate ML/FT risks they may represent. To verify the information provided by the employee, the Company may use verification procedures applied to the customers and specified in this Policy.

14. RECORD-KEEPING

All AML/CFT records shall be maintained for a minimum period of 5 years, extendable to 10 years upon request by FIU Curaçao or other regulatory authorities.

Documents to be retained include:

- Customer identification and due diligence records.
- Transaction records, including deposits, withdrawals, and gaming activity.
- Internal compliance reports, STRs, and UTRs submitted to FIU Curaçao.
- Employee AML training logs and compliance certifications.

- Audit reports and regulatory filings submitted to the Curaçao Gaming Control Board (GCB).

Records must be stored securely in a tamper-proof electronic system and be made available upon regulatory request.

The abovementioned documentation should be appropriately filed so that it is easily accessible, and its confidentiality is guaranteed. Documentation kept shall be of good quality and clearly legible, and any photographic evidence used in determining the identity of individuals should be sufficiently clear as to allow the individual concerned to be easily identified.

15. EXECUTION POLICY

The implementation of the Policy requires a top-down approach, with the senior management taking an active role in the oversight and implementation of this Policy.

The Board of Company shall approve any amendments made to the Policy and to any of the substantial policies and procedures.

The MLRO shall ensure that this Policy is made available to all employees and across all business lines. Where technical implementation is required, the relevant personnel is responsible for ensuring that internal working documents are established and the recommendations of the MLRO are implemented and operated to meet the provided requirements.

Each member of the Board and head of a structural unit should take the required actions to ensure that all staff in their areas of responsibility is fully informed regarding the Policy and relevant procedures and measures.

All employees of the Company shall be encouraged to submit suggestions for improvements of the Policy; such suggestions shall be submitted to the MLRO.

The MLRO is responsible for the monitoring, updating, and supervision of the measures outlined in this Policy.

Annual audits must be conducted to ensure the state of compliance of the relevant departments. The heads of departments or team leads are expected to provide full cooperation to ensure that there are no gaps in implementation.

Revision and updates of the Policy shall take place at least once a year and on an ad-hoc basis following updates in relevant requirements, regulations, and best practices.

16. POLICY REVIEW

The responsible parties for monitoring, updating, and Reviewing this policy are the MLRO in collaboration with the Compliance Team and the KYC team. Responsible for Approval of this Policy are the MLRO and the Company board.

The policy will be reviewed regularly by the compliance function and the Company MLRO, at minimum annually, and as set out by the following criteria;

- Annually: no later than 12 months from the date upon which the Policy was last reviewed;

- Upon the change of any relevant law or regulation which applies to the Policy;
- Upon the finding by any regulator, external or internal audit that an amendment to the Policy is required;
- Upon the award of any new gambling license in any new jurisdiction;
- Upon a new product implementation or acquiring a new product / vertical;
- Whenever significant changes occur in the business, that will have a direct or indirect impact on the area this document concerns

Any amendment of the Policy shall, as soon as is reasonably practicable, be distributed or informed to all persons within the scope of the Policy for information of the amendment. Any change in Policy giving rise to a Procedure review shall be identified and such changes shall be implemented to the relevant Procedure.