

ANTI-MONEY LAUNDERING AND COUNTERING THE FINANCING OF TERRORISM POLICY

CONFIRMED

Willemstad, on April 10, 2025

A handwritten signature in black ink is positioned to the left of a circular corporate seal. The seal features the Morganite logo (a stylized 'M' inside a square) and the text 'MORGANITE' and 'CORPORATE SERVICES B.V.' around the perimeter. Below the seal, the text 'Registered Office: Willemstad, Curacao' and 'VAT NO. 047198140' is visible.

Statutory Director
of Morganite Corporate Services B.V.,
acting on behalf of BAMLA LIMITED N.V.

Represented by:
Norine Josefa Erodita Clifton, Managing Director

Document Classification: CONFIDENTIAL						
Name:	Anti-Money Laundering and Countering the Financing of Terrorism policy					
Maintainer:	MLRO	Approver:	Statutory Director			
Status:	In effect	Version:	5.0	Effective Date:	April 10, 2025	Page 2 of 44

TABLE OF CONTENTS

1. POLICY STATEMENT.....3

2. PURPOSE 3

3. AUDIENCE 3

4. DEFINITIONS4

5. POLICY IMPLEMENTATION6

5.1. Business Risk Assessment6

5.2. Customer Risk Assessment7

5.3. Customer Acceptance Policy10

5.4. Customer Due diligence13

5.5. Ongoing Monitoring26

5.6. Reliance on third parties to perform customer due diligence28

5.7. Reporting of unusual transactions28

5.8. Anti-Money Laundering Compliance program33

6. COMPLIANCE AND CONSEQUENCES OF NON-COMPLIANCE 38

7. RELATED INFORMATION 38

8. CONTACT INFORMATION 39

9. POLICY HISTORY 39

10. POLICY URL 39

11. ANNEXES40

Document Classification: CONFIDENTIAL						
Name:	Anti-Money Laundering and Countering the Financing of Terrorism policy					
Maintainer:	MLRO	Approver:	Statutory Director			
Status:	In effect	Version:	5.0	Effective Date:	April 10, 2025	Page 3 of 44

1. POLICY STATEMENT

- 1.1. The Company is committed to ensuring full compliance with all applicable anti-money laundering (AML), counter-terrorist financing (CFT), and counter-proliferation financing (CPF) laws and regulations. This Policy establishes the minimum standards for detecting, preventing, and reporting suspicious activities, including money laundering and the financing of terrorism or the proliferation of weapons.
- 1.2. The Policy applies to all users and Customers engaging with RioPlay, a brand operated by the Company, by ensuring the implementation of appropriate verification procedures and proactive measures to mitigate money laundering risks.
- 1.3. A risk-based approach is adopted to ensure that AML/CFT/CPF resources are allocated proportionately to the level of identified risk, thereby enhancing the effectiveness and efficiency of the Company's compliance efforts.

2. PURPOSE

- 2.1. The purpose of this Policy is to establish Company's internal Anti-Money Laundering (AML), Counter Financing of Terrorism (CFT), and Counter Proliferation Financing (CPF) controls. It outlines the Company's approach to ensuring full compliance with applicable laws and regulations in Curaçao, while aligning with recognized international standards and best practices.
- 2.2. This Policy demonstrates the Company's commitment to maintaining the integrity of its operations and the broader gaming industry in Curaçao. It provides a structured framework for adhering to AML/CFT/CPF obligations, including:
 - 2.2.1. The National Ordinance on Identification when Rendering Services (NOIS);
 - 2.2.2. The National Ordinance on the Reporting of Unusual Transactions (NORUT);
 - 2.2.3. The Kingdom Sanctions Act;
 - 2.2.4. Applicable United Nations and European Union sanctions frameworks;
 - 2.2.5. Recommendations from the Financial Action Task Force (FATF);
 - 2.2.6. Relevant findings from national risk assessments (NRAs).
- 2.3. By implementing this Policy, the Company seeks to reinforce effective internal controls, Customer Due Diligence (CDD) procedures, comprehensive risk assessments, and timely reporting mechanisms – thereby proactively managing risks associated with financial crime.

3. AUDIENCE

This Policy applies to all individuals and entities directly or indirectly engaged with the Company, including but not limited to:

- 3.1. All departments and employees of the Company, including senior management, MLRO, Compliance Officers, and risk management personnel;
- 3.2. All operational staff involved in online gaming activities under the Company's license(s);
- 3.3. Third-party service providers engaged by the Company, including physical representatives of online operations;
- 3.4. Subcontractors, partners, or affiliates involved in Customer onboarding, payment processing, or risk-related functions on behalf of the Company;
- 3.5. Any individual or organization acting under the authority or representation of the Company in a regulated capacity.

Document Classification: CONFIDENTIAL						
Name:	Anti-Money Laundering and Countering the Financing of Terrorism policy					
Maintainer:	MLRO	Approver:	Statutory Director			
Status:	In effect	Version:	5.0	Effective Date:	April 10, 2025	Page 4 of 44

Responsibilities:

- 3.6.** The Fraud and Compliance Department and staff are responsible for monitoring all transactions to and from the Company and verifying the identity of all online registered Customers requesting a withdrawal. They must also establish parameters by which any suspicious activity can be immediately noted, and form procedures by which to solve these issues while keeping the risk to a minimum. Such staff must follow the guidelines and requirements set forth by Law. The Law requires the responsible persons to verify the Customer in such a way that the source of funds is also identified. The verification process will be documented in such a way that **every Customer will have a profile and if any Suspicious Transaction Report needs to be filed, all evidence in respect of the Customer will be in hand.**
- 3.7.** The following departments are directly targeted by the requirements of this procedure:
- 3.7.1.**Board of Directors** – Approval and Signature requirements, especially in high-risk scenarios;
 - 3.7.2.**KYC Department** – Understanding reporting requirements and applying DD requirements;
 - 3.7.3.**Finance Department**– Understanding the risks posed by ML/TF;
 - 3.7.4.**Fraud and Compliance Department** – Ensuring all legislation requirements are met and understanding the difference between a fraud case and an ML case;
 - 3.7.5.**MLRO** – Updating Policy and ensuring all relevant employees are aware of AML requirements.
 - 3.7.6.**Customer Service Department**, supported by electronic analytic systems, monitors unusual Customer behavior, such as depositing and withdrawing without gameplay, changing nationality, or using different payment methods.
- 3.8.** The scope of this Policy may be extended to other departments if the need ever arises and all employees need to be attentive and aware of the information flow regarding legislation.

4. TERMS USED IN THE POLICY

4.1. Definitions:

Beneficial Owner	the natural person, who ultimately owns or control the Customer and/or the natural person on whose behalf a transaction or activity is being conducted.
Business Relationship	a business, professional or commercial relationship which is connected with the professional services offered by the Company, and which was expected, at the time when the contact was established, to have an element of duration.
Company	BAMLA LIMITED N.V., registered № - 164689, legal address - 1 Abraham de Veerstraat, Willemstad, Curaçao.
Customer	any legal or physical person aiming to conclude a Business Relationship or conduct a single transaction with the Company.
Internal regulatory documents	documents drawn up, agreed, and approved by the Company (regulations, Policys, programs, procedures, regulations, by-laws, instructions, guidelines, process descriptions, etc.).
Law	means any Laws and Acts legally enacted from time to time in Curacao, or which are applicable and enforceable in Curacao.

Document Classification: CONFIDENTIAL						
Name:	Anti-Money Laundering and Countering the Financing of Terrorism policy					
Maintainer:	MLRO	Approver:	Statutory Director			
Status:	In effect	Version:	5.0	Effective Date:	April 10, 2025	Page 5 of 44

Policy	this Anti-Money Laundering and Countering the Financing of Terrorism policy
Politically Exposed Person (PEP)	a Politically Exposed Person (PEP) is a natural person who holds or has previously held a prominent public function, such as a Head of State, Head of Government, Minister, Deputy or Assistant Minister, or Parliamentary Secretary. The status of PEP may also extend to close family members and known close associates of such individuals. A person is not automatically considered a PEP if they have ceased holding a prominent public function for at least one year; however, the Company may still treat them as a PEP based on a risk-based assessment of their former position.
Money Laundering and Terrorist Financing / ML/TF	the money laundering offences and terrorist financing offences defined in the Law.
Occasional Transaction	any transaction other than a transaction carried out in the course of an established Business Relationship formed by a person acting in the course of financial or other business.
RioPlay	brand operated by Company
Tipping of	improper or illegal act of notifying a suspect that he or she is the subject of a suspicious transaction report or is otherwise being investigated or pursued by the authorities.
Website	https://rioplay.com/

4.2. Abbreviations:

AML	Anti-Money Laundering
CAP	Customer Acceptance Policy
CDD	Customer due diligence
CFATF	Caribbean Financial Action Task Force
CFT	Combating Funding of Terrorism
CMP	Compliance Monitoring Program
EDD	Enhanced due diligence
FATF	Financial Action Task Force
FIU	Financial Intelligence Unit of Curacao.
GCB	Curaçao Gaming Control Board - the official AML/CFT supervisor for all gambling in and from Curaçao
KYC	Know Your Customer
MLRO	Money Laundering Reporting Officer
SAR	Suspicious Activity Report
STR	Suspicious Transaction Report

Document Classification: CONFIDENTIAL					
Name:	Anti-Money Laundering and Countering the Financing of Terrorism policy				
Maintainer:	MLRO	Approver:	Statutory Director		
Status:	In effect	Version:	5.0	Effective Date:	April 10, 2025
				Page 6 of 44	

5. POLICY IMPLEMENTATION

This section outlines how the Company implements its Anti-Money Laundering and Countering the Financing of Terrorism Policy through a structured, risk-based framework. It assigns key responsibilities and describes core procedures in compliance with Curaçao's regulatory requirements.

5.1. BUSINESS RISK ASSESSMENT

5.1.1. The Company conducts a Business Risk Assessment (BRA) to identify and evaluate the specific risks of money laundering (ML), terrorist financing (TF), and financing of proliferation (CPF) to which its business model and operational environment are exposed. The BRA helps ensure that the policies, controls, and procedures adopted are adequate to prevent and mitigate these risks.

5.1.2. In conducting the BRA, the Company considers all relevant risk factors, including:

- 5.1.2.1. The nature of the products and services offered;
- 5.1.2.2. Distribution and delivery channels, including physical establishments and online platforms;
- 5.1.2.3. Types and risk profiles of customers served;
- 5.1.2.4. Geographic regions of operation and exposure;
- 5.1.2.5. Potential vulnerabilities in the business model that could be exploited for ML/TF/CPF purposes.

5.1.3. Special consideration is given to how the casino could be misused for money laundering, terrorist financing, and proliferation financing, as well as the likelihood and extent of such risks.

5.1.4. In addition to internal risk indicators, the Company takes into account the outcomes and recommendations of the National Risk Assessment (NRA) and incorporates these findings into the BRA to ensure a harmonized and risk-based approach.

5.1.5. Once the risks are assessed, the Company defines its risk appetite, determining the level and types of risk it is prepared to accept. This risk appetite forms the foundation of the Company's anti-money laundering and counter-terrorist financing (AML/CFT) compliance program.

5.1.6. The BRA must be documented, clearly explaining:

- 5.1.6.1. The methodology used for assessing risks;
- 5.1.6.2. The rationale behind categorizing each risk factor as low, medium, or high;
- 5.1.6.3. The outcome of the assessment, including identified high-risk areas;
- 5.1.6.4. Information sources and data used to support the assessment.

5.1.7. The Business Risk Assessment is reviewed:

- 5.1.7.1. At least once annually, even in the absence of changes;
- 5.1.7.2. Whenever there are significant changes to the Company's business activities, environment, or regulatory landscape (e.g., new markets, games, payment methods, or technologies).

5.1.8. The effectiveness of the BRA's implementation is monitored continuously, and improvements are made where necessary. The BRA is approved by the Board of Directors and is made available to the Curaçao Gaming Control Board (GCB) upon request.

5.1.9. To maintain a risk-based approach, the Company commits to keeping abreast of emerging ML/TF/CPF typologies and relevant regulatory developments.

Document Classification: CONFIDENTIAL						
Name:	Anti-Money Laundering and Countering the Financing of Terrorism policy					
Maintainer:	MLRO	Approver:	Statutory Director			
Status:	In effect	Version:	5.0	Effective Date:	April 10, 2025	Page 7 of 44

5.2. CUSTOMER RISK ASSESSMENT

5.2.1. The Customer risk profile is a document describing the various items taken into consideration, when enough information is gathered regarding a Customer, to determine the risk said Customer poses to the Company from an AML/CFT perspective within the confines of the Business Risk Assessment created for the Company.

5.2.2. The Customer risk assessment is created in one of the following situations:

- 5.2.2.1. The Customer reaches the threshold;
- 5.2.2.2. Suspicion has been raised internally regarding the Customer's activity;
- 5.2.2.3. Change in Customer's PEP status;
- 5.2.2.4. Increase in Customer risk classification;
- 5.2.2.5. On the detection of any red flags as defined in Annex B.
- 5.2.2.6. At registration an initial Customer risk assessment is undertaken although such assessment will be quite limited since the Customer wouldn't have made any use of the Company's products and no verification documentation would have been obtained at this stage.

5.2.3. In either of the above-mentioned cases a Customer risk profile is drafted and is filled in using information gathered during the business relationship. Should additional control measures be applied, the response, information and documentation provided shall also be taken into account when drafting such Customer risk profile.

5.2.4. **The Customer risk profile contains the following fields:**

5.2.4.1. Username as stored in the back office

When creating an account with the Company the Customer selects a username that will be stored within the Company back office and is used to further identify the Customer. The username itself cannot be utilized to identify the Customer unless access is provided to the secured Company back office and thus anonymization is achieved to satisfy GDPR regulation. The only way to establish a link between the Customer risk profile and the Customer sensitive data is to have access to both platforms. Access to said platforms is carefully monitored by the Company IT security team.

5.2.4.2. Funding method as described in the back office

The Company back office stores all possible funding methods for all jurisdictions within its back office and allocates these funding methods to Customers using them accordingly.

Each individual payment method has received an internal relevant risk score based on the strength of the controls applied on the Customers using said particular payment methods, as well as on the strength of the AML policies and procedures employed by the payment method providers themselves.

The risk scores are described as follows:

Risk Rating	Risk Score	Description
Low	5	- Local bank transfers within the operating regions - Debit cards issued by recognized financial institutions within the operating regions
Medium	10	- Credit cards issued by banks within the operating regions - Payment service providers (PSPs) that do not allow customers to fund with cash or quasi-cash

Document Classification: CONFIDENTIAL						
Name:	Anti-Money Laundering and Countering the Financing of Terrorism policy					
Maintainer:	MLRO	Approver:	Statutory Director			
Status:	In effect	Version:	5.0	Effective Date:	April 10, 2025	Page 8 of 44

High	50	• Prepaid cards • Vouchers • Cash transactions • Debit and credit cards issued by non-local banks • Virtual currencies (cryptocurrencies) • PSPs that allow funding with cash or quasi-cash, whether local or non-local
------	----	--

NOTE: Some of the risk categories found in the above ratings might not be currently present within the Company risk appetite, however they have been noted in the general risk assessment as to be used at any future date in case the Company deems it necessary.

The current payment methods have been adjusted to reflect the current status of the Company risk appetite in the individual scores.

5.2.4.3. Customer Jurisdiction

Countries banned via platform to avoid risks from an AML/CFT perspective and countries listed as High-Risk Jurisdictions subject to a Call for Action by the FATF. The Company takes into consideration Customer jurisdiction upon onboarding to ensure that the country the Customer comes from is within the Company risk appetite.

All countries accepted by the platform have been analyzed based on the individual controls applied by the Company on a case-to-case basis, as well as concatenating information from various online resources that offer insight on the risk specific jurisdictions pose from an AML/CFT perspective.

Each country supported by the platform has been given a risk score based on the data processed from the various resources.

The main documentation used for determining a country's risk rating are:

- Countries on the FATF list of High - Risk Jurisdictions subject to a Call for Action;
- Countries on the FATF list of Jurisdictions under Increased Monitoring;
- Countries on the CFATF Public Statement;
- Countries identified as Jurisdictions of Concern or Primary Concern in the U.S. Department of State's annual International Narcotics Control Strategy Report (INCSR);
- Countries on the European Commission's list of third countries having strategic deficiencies in their AML/CFT regime;
- Countries sanctioned by the OFAC;
- Countries identified by credible sources as providing funding or support for terrorist activities or have terrorist organizations operating within them;
- Countries on the Corruption Perception Index compiled by Transparency International.

The jurisdiction risk scores are described as follows:

Risk Rating	Risk Score	Description
Low	5	Countries that offer a strong AML/CFT regulation in line with Curaçao standards. Countries that offer a good AML/CFT regulation and show signs of constant improvement

Document Classification: CONFIDENTIAL						
Name:	Anti-Money Laundering and Countering the Financing of Terrorism policy					
Maintainer:	MLRO	Approver:	Statutory Director			
Status:	In effect	Version:	5.0	Effective Date:	April 10, 2025	Page 9 of 44

Medium	15	Countries that offer an acceptable AML/CFT regulation and have shown plans to improve in the future. Countries that offer a baseline AML/CFT regulation and controls can be put in place to mitigate risks
High	35	Countries lacking sufficient and/or effective AML/CFT regulation and controls in place to mitigate risks
Blocked/Extreme	PROHIBITED	Countries banned via platform to avoid risks from an AML/CFT perspective and countries listed as High-Risk Jurisdictions subject to a Call for Action by the FATF

NOTE: Not all countries present in the extended score description are currently available through the platform, however scores have been assigned to the above-mentioned countries to ensure a term of comparison where needed.

5.2.4.4. Game Types

The Company takes into consideration the main games played by each respective Customer as to understand how the Customer's capacity to influence the game odds and knowledge of the game mechanics can influence the capacity to circulate funds through the platform.

The categorization is mainly based on the guidance offered by the Curaçao FIU risk scoring and offers good insight on typology and risk rating.

All games offered by the Company have been broken down into the recommended categories based on the current offer.

The top 3 games played (by number of bets initiated) will be chosen and the average will count towards to final risk score. If less than 3 games have been played in total the average will change to account for the lower number of games.

The games are categorized as follows:

RISK RATING	RISK SCORE	DESCRIPTION
LOW	5	CASINO – SLOT GAMES
MEDIUM	10	LIVE CASINO VS HOUSE
HIGH	15	- P2P CASINO - VIRTUAL SPORTS GAMES - SPORTSBOOK (including E-SPORTS)

NOTE: Not all games available in the general scoring table are currently available on the platform, however scoring has been added for all possible games to ensure that a risk rating if these games are ever introduced as part of the Company risk appetite.

5.2.4.5. Customer registration channel

The Company offers the possibility of online registration for its Customer. On signing up Customers must input the details as described in section 5.4.13 and provide at least the first two point of level 1 controls for identification purposes. Once the Customer deposits and

Document Classification: CONFIDENTIAL						
Name:	Anti-Money Laundering and Countering the Financing of Terrorism policy					
Maintainer:	MLRO	Approver:	Statutory Director			
Status:	In effect	Version:	5.0	Effective Date:	April 10, 2025	Page 10 of 44

starts to wager, the account is monitored for any increase in risk or high-volume wagering/high amount wagering. Should it be deemed necessary, the Customer will be asked to verify the source of funds notwithstanding the fact that the relevant thresholds have not been met. Should it transpire that the information and documentation provided at this stage is fake, inaccurate or incorrect, the account will be suspended, and an investigation is initiated to determine whether there are sufficient grounds to file an STR.

5.2.4.6. Customer first deposit amount

The Company considers that the initial sum deposited by a specific Customer is crucial in determining the type of behaviour the Company needs to exhibit towards the Customer from both an AML perspective as well as a Responsible Gambling perspective. To this extent the possible first deposit amounts have been broken down to 3 categories beginning with the most common deposit amount and incrementing to the threshold for Due Diligence requirement.

The deposit amounts are broken down as follows:

Risk Rating	Risk Score	Amounts (USD)
Low	5	0 to 500
Medium	10	501 to 1000
High	15	1000 +

5.2.5. Customer withdrawal amount

The Company actively monitors the initial withdrawal amount to gain insights into the Customer's gaming behaviour and to identify potential risks or unusual activity. This monitoring helps determine the type of business relationship the Customer intends to establish and enables the Company to set appropriate monitoring flags on the Customer account for future withdrawal actions. By doing so, the Company can identify suspicious patterns that may indicate potential money laundering or other financial crimes.

If a Customer has actively participated in games and secured a large win based on legitimate wagers, the associated risk may not be high. The Customer's gaming history and transaction records can substantiate that the winnings are legitimate and consistent with game outcomes. In such cases, thorough record-keeping and monitoring ensure compliance while avoiding unnecessary risk escalation for valid Customer activities.

This balanced approach enables the Company to distinguish between genuine gaming activities and potential risks, ensuring fair treatment of Customers while maintaining robust compliance standards.

5.3. CUSTOMER ACCEPTANCE POLICY

5.3.1. The CAP follows the principles and guidelines described in this document, defines the criteria for accepting new Customers and defines the Customer categorization criteria which shall be followed by the Company and especially by the employees who have direct involvement in the obtainment of information and data relating to the Customer as well as employees who will be tasked with evaluating such Customer information in order to make recommendations as to whether such Customer falls within the Company's risk appetite in so far as the products or services being provided are concerned.

5.3.2. The Fraud and Compliance department shall be responsible for applying all the provisions of the CAP. In this respect, the Compliance Officer shall also be assisting the MLRO with the implementation of the CAP, as applicable.

5.3.3. The MLRO shall review and evaluate the adequate implementation of the CAP and its relevant provisions, at least annually, in accordance with the provisions of this policy, or

Document Classification: CONFIDENTIAL						
Name:	Anti-Money Laundering and Countering the Financing of Terrorism policy					
Maintainer:	MLRO	Approver:	Statutory Director			
Status:	In effect	Version:	5.0	Effective Date:	April 10, 2025	Page 11 of 44

at any other such interval as may be determined from time to time based on any changes in the Company's inherent and residual risk.

5.3.4. Failure or refusal to submit information:

5.3.4.1. Customers who fail or refuse to submit and provide the Company with the requisite data, information and/or documentation for their identification and verification and the creation of their profile, after they have made their first withdrawal or due to an increase in the Customer risk profile, without adequate justification, constitutes elements that may lead to the creation of a suspicion that the Customer is involved in money laundering or terrorist financing activities, although this cannot be taken as an absolute and more investigation may be required before coming to such conclusion. In such an event, the Company shall suspend the Customer's account or the execution of the transaction while at the same time the MLRO must also consider whether it is justified under the circumstances at hand to submit a report to the FIU.

5.3.4.2. If, during the Business Relationship or pending the execution of a transaction, the Customer fails or refuses to submit, within a reasonable timeframe (30 days from the date upon which the relevant threshold or circumstances have become effective), the required verification data and information in accordance with this document, the Company may inform the Customer of their intention to terminate the Business Relationship, provided that in so doing it will not be tipping off the Customer, in which case guidance shall be sought from the FIU on how best to proceed, while at the same time examine whether it is justified under the circumstances to submit a report to FIU (STR).

5.3.5. Special measures are implemented to block Customers who provide fake documentation, use restricted jurisdictions, or show gambling addiction or mental health issues.

5.3.6. General Principles of the CAP. The General Principles of the CAP are the following:

5.3.6.1. the Company shall classify Customers and/or products into various risk categories and, on the basis of the risk perception attached to such classifications will determine the amount and quality of information and documentation which will be required in order for a Customer to be accepted or rejected. Such information and data must not be below the minimum requirements as set in the FIU implementing procedures and the Laws in force at the time.

5.3.6.2. Customers may only sign up and be allowed to make use of the Company's products and services if they provide the following information: (a) name and surname; (b) permanent residential address; (c) date of birth; (d) place of birth; (e) nationality; and (f) identity reference number where applicable.

5.3.6.3. all documents and data described in this policy must be collected before allowing a Customer to continue making use of the services provided once the thresholds have been reached (Identity Documentation and Utility Bill).

5.3.6.4. no services shall be provided to anonymous Customers or Customers who are known to be operating under fictitious names(s).

5.3.6.5. no services shall be provided to high-risk Customers unless the prospective Customer is approved by:

5.3.6.5.1. one of the Company's Director and/or Senior Managers or

5.3.6.5.2. the MLRO.

Document Classification: CONFIDENTIAL						
Name:	Anti-Money Laundering and Countering the Financing of Terrorism policy					
Maintainer:	MLRO	Approver:	Statutory Director			
Status:	In effect	Version:	5.0	Effective Date:	April 10, 2025	Page 12 of 44

5.3.7. Criteria for Accepting New Customers (based on their respective risk)

- 5.3.7.1. This Section describes the criteria for accepting new Customers based on their risk categorisation. Following a risk-based approach one must on a case-by-case basis determine what level of due diligence should be applied on identification, business relationship and transaction level, provided that these do not fall below the minimum as set out by the various applicable laws and regulations in place at the time. Whether the level of risk is above or below the threshold the Company is willing to undertake, one needs to be able to provide evidence to regulatory bodies that the appropriate steps have been taken to mitigate risk. There are three commonly recognised categories of due diligence.

5.3.8. Low Risk Customers

- 5.3.8.1. The Company shall accept Customers who are categorised as low risk Customers, as these are defined under Section 5.4.25 as long as the general principles as discussed in the sections below are applied.
- 5.3.8.2. Moreover, the Company shall follow the Simplified Customer Identification and Due Diligence Procedures for low-risk Customers, as defined in this policy.

5.3.9. Medium Risk Customers

The Company shall accept Customers who are categorised as medium risk Customers as long as the general principles as defined in Section 5.3.6 of this policy are followed.

5.3.10. High Risk Customers

- 5.3.10.1. The Company shall accept Customers who are categorised as high-risk Customers as long as the general principles under Section 5.3.13 of the Policy are followed.
- 5.3.10.2. Moreover, the Company shall apply the Enhanced Customer Identification and Due Diligence measures for high-risk Customers, in accordance with the measures in this policy and the due diligence and identification procedures for the specific types of high-risk Customers as applicable.

5.3.11. Customer Registration

- 5.3.11.1. In order to open an account with Company from the web portal, a user must first complete the registration process and deposit some funds with which he/she can then start playing. A risk – based approach is adopted, therefore basic principles are followed, and a checklist approach is avoided in order to remain vigilant of the Customers being accepted
- 5.3.11.2. The registration details must be completed by all new Customers as specified in Clause 5.3.6.2. Additionally, all Customers must be at least 18 years old and may only have one account in their name. Therefore, minors are prohibited from playing on the website. Furthermore, users without a registered customer account will not be allowed to play.

5.3.12. Email Verification

When a new account is created, a verification link is sent to the email account specified during the registration process. When the user clicks on the link the account is then successfully created. Only at this point can the Customer deposit money and start placing bets.

Document Classification: CONFIDENTIAL						
Name:	Anti-Money Laundering and Countering the Financing of Terrorism policy					
Maintainer:	MLRO	Approver:	Statutory Director			
Status:	In effect	Version:	5.0	Effective Date:	April 10, 2025	Page 13 of 44

5.4. CUSTOMER DUE DILIGENCE

5.4.1. Customer due diligence can be split into 3 categories, which categories shall be dependent on the Customer's risk rating.

5.4.2. **Simplified due diligence** – this is the first stage of the process, which is carried out for the purposes of identifying and verifying the Customer. Registered details will be cross checked against any documentation and public information which includes confirmation of the name, surname, date of birth and address of the Customer. Such documents requested by the Company may be in the form of scanned documents such as scans of the I.D. card or passport to confirm their identity. In instances where the I.D. card does not also confirm the Customers' residence because no such residential information is provided on the document, then, a recent bill to confirm their address will be requested. This process may be initiated at registration or first deposit phase but does not become a requirement until the thresholds are reached. In this stage verification of source of wealth and source of funds will not require an in-depth analysis of the origin of the Customer's funds and the activities which have led to the accumulation of the Customer's wealth as the risk of ML/TF is relatively low. However, information about the mentioned source of wealth must still be obtained when the Customer exceeds the thresholds set in the Company's guidelines for verifying the origin of funds. The obtained information will then be reviewed to determine whether it is sufficient or if additional supporting documents are required.

5.4.3. **Customer due diligence** – this is the standard process which is to be followed for the vast majority of the Customer base, provided they fall within the respective risk categories requiring the application of CDD. In addition to verifying the Customer's identity and residential address, the Company must also identify and verify the source of the Customer's wealth and funds. This can be done using statistical data, and in some cases, obtaining a declaration from the Customer with relevant details (e.g., nature of employment/business, usual annual salary, etc.) may be sufficient. The Customer will be allowed to deposit and making use of the Company's products but will not be allowed to make any withdrawals until such time as the documentation is received. In the event that such documentation is not received within 30 days from when the Company requested such information and documentation from its Customers, the Customer's account shall be suspended, and the Customer will be precluded from depositing and making use of the Customer's products and services in addition to not allowing withdrawals to be made. A report should be sent to the MLRO within 24 hours of the happening of such an event. The MLRO shall then investigate and determine whether an STR or SAR are to be filed with the FIU.

The Company applies enhanced due diligence measures for Customers engaging in high-risk behaviour. Special verification processes include verifying account ownership, nationality, and transaction patterns.

5.4.4. **Enhanced due diligence** – This is the third and most crucial stage of the due diligence process, as further information regarding the Customer is acquired. Such information includes obtaining detailed knowledge and the respective supporting documentation to confirm the proof of the Customer's source of wealth. This involves gathering detailed information on the Customer's occupation, source of funds, and source of wealth. A higher level of staff with relevant experience will be involved in this stage, as it requires sound judgment when reviewing the documentation and information provided by the Customer. Upon any single or cumulative transaction, whether a withdrawal or deposit by any Customer, the Customer will be required to provide proof of the source of wealth and source of funds as part of the enhanced due diligence process.

Document Classification: CONFIDENTIAL						
Name:	Anti-Money Laundering and Countering the Financing of Terrorism policy					
Maintainer:	MLRO	Approver:	Statutory Director			
Status:	In effect	Version:	5.0	Effective Date:	April 10, 2025	Page 14 of 44

5.4.4.1. No further transactions may be processed until these documents are sent by the Customer and are checked and verified by the management.

5.4.4.2. This process is in line to lower the AML risks. Upon registration of a new Customer, his/her transactions and betting behaviour will be checked and monitored Policy daily. Mechanisms are in place that enforce a one account per person policy, and if an issue of multiple accounts is detected all relative accounts are suspended/frozen until the matter is resolved. Scripts are in place that detect strange or unusual behaviours from our Customers, and our software provider partners (Endorphina, Microgaming etc.) are immediately notified. This procedure enables the Company to analyse the way every individual uses the product from our website, making it possible to categorize the Customers and thus set limits to the individual Customers according to their betting habits.

5.4.5. Customer identification and verification guidelines

5.4.5.1. In order to do a first deposit with Company a Customer needs to provide the following mandatory details:

- 5.4.5.1.1. First name
- 5.4.5.1.2. Last name
- 5.4.5.1.3. Gender
- 5.4.5.1.4. Street and street number
- 5.4.5.1.5. City and postal code
- 5.4.5.1.6. Country
- 5.4.5.1.7. Email address (must be valid and unique within Company)
- 5.4.5.1.8. Date of birth
- 5.4.5.1.9. Password (will be encrypted)
- 5.4.5.1.10. Confirmation of password
- 5.4.5.1.11. Account currency
- 5.4.5.1.12. Mobile phone number

5.4.5.2. A newly registered Company account will be checked in the shortest time possible by the service department in order to find out if the details are correct (accounts with fancy names and addresses will be closed). Also, the registered country and the IP-country need to be compared. A mismatch is automatically to be noted in the Customers' account. This helps us close fake accounts before any pay-in can be processed.

5.4.5.3. Customers who are not registered are unable and not allowed to play for real money. Any online transaction, may it be pay-in or pay-out, will not be accepted or processed.

5.4.5.4. Once the registration process has been finalised, Customers will receive a welcome email with a link to access their accounts. This procedure aims at verifying the Customer's email address.

5.4.5.5. Customers reaching one of the specified thresholds (first withdrawal request, suspicion of ML/TF, or increase in Customer risk) go through an initial Risk assessment screening in order to determine if the Customer's risk profile falls within the Company's risk appetite. The following pieces of information are checked regarding each Customer in order to determine the initial risk profile:

- 5.4.5.5.1. Funding Methods
- 5.4.5.5.2. Requested Product Type(s)
- 5.4.5.5.3. Business Relationship Channel
- 5.4.5.5.4. Geo-Location
- 5.4.5.5.5. Politically Exposed Person (PEP) screening

Document Classification: CONFIDENTIAL						
Name:	Anti-Money Laundering and Countering the Financing of Terrorism policy					
Maintainer:	MLRO	Approver:	Statutory Director			
Status:	In effect	Version:	5.0	Effective Date:	April 10, 2025	Page 15 of 44

5.4.5.5.6. Sanctions Lists Screening

- 5.4.5.6. Each new Customer has to provide a copy of an ID document (passport, ID card or driving license) when relevant thresholds are reached. This is in line with the local transposition as well as the relevant Implementing Procedures and Guidance Notes.
- 5.4.5.7. The identity check has to include a copy of a utility bill and/or bank statement showing the name and address and cannot consist of a mobile telephony bill.
- 5.4.5.8. Furthermore, the identity check may include additional measures such as the provision of a copy of each credit card used in the specific account. Further details can be found in the Procedure detailing Due Diligence process.
- 5.4.5.9. Any remaining doubts concerning the identity of a Customer have to be reported based on the Procedure detailing reporting lines.
- 5.4.5.10. In such a case, further investigations have to be started. **These may include:**
- 5.4.5.10.1. Check of the IP used by the Customer
 - 5.4.5.10.2. Check of the provided phone number and/or call to the provided phone number
 - 5.4.5.10.3. Internet research on the Customer details
 - 5.4.5.10.4. Request to the official authorities in the country of the Customer – this has to be done by compliance management.
 - 5.4.5.10.5. More information available in the dedicated CDD chapter.

5.4.6. The due diligence criteria are set as follows:

- 5.4.6.1. ID documents must be official documents issued by a government entity that includes confirmation of the name and residential address or date of birth and a photo such as a passport can be used to verify an identity. Where this type of documentation is not available a government issued document confirming the name of the individual and supporting document supplied by a public authority, court or any finically regulated service provider that includes the individuals full name and either date of birth or residential address can be used.
- 5.4.6.2. The details in the passport are compared to other documents collected at the Company's discretion.
- 5.4.6.3. When in doubt of forgery, the Customer is requested to hold up the passport to his/her face in order to verify that such passport belongs to the said individual.
- 5.4.6.4. Online public databases are checked in order to cross check the information in the documents provided.
- 5.4.6.5. Public searches through social media and other sources are checked in order to build the Customer profile.
- 5.4.6.6. Finally, if it comes to our attention that the individual is a politically exposed person (PEP*), enhanced due diligence is immediately carried out and the account is monitored closely.
- 5.4.6.7. If the Customer comes from a high-risk jurisdiction, the enhanced due diligence process is initiated immediately, and the account is monitored closely. It is at the Company's discretion to refuse registrations from high-risk jurisdictions.

Document Classification: CONFIDENTIAL						
Name:	Anti-Money Laundering and Countering the Financing of Terrorism policy					
Maintainer:	MLRO	Approver:	Statutory Director			
Status:	In effect	Version:	5.0	Effective Date:	April 10, 2025	Page 16 of 44

5.4.7. Politically Exposed Persons (PEP)*

Company is aware of its duties towards identifying and carrying out due diligence in terms of politically exposed persons. The Company shall apply the following with respect to the accounts of "Politically Exposed Persons":

- 5.4.7.1. The establishment of a Business Relationship or the execution of an Occasional Transaction with persons holding important public positions in Curacao or in a foreign country and with natural persons closely related to them, may expose the Company to enhanced risks, especially if the potential Customer seeking to establish a Business Relationship or the execution of an Occasional Transaction is a PEP, a member of his immediate family or a close associate of or is known to be associated with a PEP.
- 5.4.7.2. The Company shall pay more attention when the said persons originate from a country which is widely known to face problems of bribery, corruption and financial irregularity and whose anti-money laundering laws and regulations are not equivalent with international standards or who have been flagged as having regulatory deficiencies by the FATF or any other regulatory and/or monitoring authority.
- 5.4.7.3. In order to effectively manage such risks, Company shall assess the countries of origin of its Customers in order to identify the ones that are more vulnerable to corruption or maintain laws and regulations that do not meet the 40+9 requirements of the FATF.
- 5.4.7.4. With regards to the issue of corruption, one useful source of information is the Transparency International Corruption Perceptions Index which can be found on the website of Transparency International at www.transparency.org.
- 5.4.7.5. With regard to the issue of adequacy of application of the 40+9 recommendations of the FATF, the Company shall retrieve information from the country assessment reports prepared by the FATF or other regional bodies operating in accordance with FATF's principles (e.g. Moneyval Committee of the Council of Europe) or the International Monetary Fund.
- 5.4.7.6. Without prejudice to the provisions of this document, Company will adopt the following additional due diligence measures when it establishes a Business Relationship or will carry out an Occasional Transaction with a PEP:
- 5.4.7.7. Company puts in place appropriate risk management procedures to enable it to determine whether a prospective Customer is a PEP. Such procedures may include, depending on the degree of risk, the acquisition and installation of a reliable commercial electronic database for PEPs, seeking and obtaining information from the Customer himself or from publicly available information. In the case of legal entities and arrangements, the procedures will aim at verifying whether the Beneficial Owners, authorised signatories and persons authorised to act on behalf of the legal entities and arrangements constitute PEPs. In the event of identifying one of the above as a PEP, then automatically the account of the legal entity or arrangement should be subject to the relevant procedures specified in this Section of the Policy
- 5.4.7.8. the decision for establishing a Business Relationship or the execution of an Occasional Transaction with a PEP is taken by an Executive Director of the Company and the decision is then forwarded to the MLRO. When establishing a Business Relationship with a Customer (natural or legal person) and subsequently it is ascertained that the persons involved are or have become PEPs, then an

Document Classification: CONFIDENTIAL						
Name:	Anti-Money Laundering and Countering the Financing of Terrorism policy					
Maintainer:	MLRO	Approver:	Statutory Director			
Status:	In effect	Version:	5.0	Effective Date:	April 10, 2025	Page 17 of 44

approval is given for continuing the operation of the Business Relationship by an Executive Director of the Company which is then forwarded to the MLRO

5.4.7.9. before establishing a Business Relationship or executing an Occasional Transaction with a PEP, the Company shall obtain adequate documentation to ascertain not only the identity of the said person but also to assess his business reputation (e.g. reference letters from third parties)

5.4.7.10. Company shall create the economic profile of the Customer by obtaining the information specified in Section 5.4.4 of the Policy. The profile shall be regularly reviewed and updated with new data and information. The Company shall be particularly cautious and most vigilant where its Customers are involved in businesses which appear to be most vulnerable to corruption such as trading in oil, arms, cigarettes and alcoholic drinks.

5.4.7.11. the account shall be subject to a shorter review period than would otherwise be assigned for a Customer of a similar risk, in order to determine whether to allow its continuance of operation. Such period shall take into account the position and measure of political influence the PEP has as well as the inherent risk and mitigating measures associated with the products being offered to such a Customer. A short report shall be prepared summarizing the results of the review by the person who is in charge of monitoring the account. The report shall be submitted for consideration and approval to the Partners and filed in the Customer's personal file.

5.4.7.12. Company is required to obtain a higher standard in relation to the quality of documents obtained.

5.4.7.13. Company may carry out or, in the case of applying enhanced on-going monitoring, implement these measures at any point in time between the establishment of the business relationship and the point in time when the Customer requests their first withdrawal. In the case of an occasional transactions, Company have to carry out the said measures, in so far as they are applicable, prior to carrying out the transaction in question.

5.4.7.14. Screening for PEP status will be carried out regularly but it is important that this is done within 30 (thirty) days of the Customer requests their first withdrawal of USD 5000, even where Company may have already screened Customers to determine if they were PEPs earlier on in the course of the business relationship. Should a Customer who had not been identified as a PEP at on-boarding stage result to have become one, the Company concerned has to carry out or implement obtain senior management approval to service the PEP as well as establish what the source of wealth and, where applicable their source of funds is within the thirty day window, failing which it would have to terminate the business relationship with the said Customer as described in the FIU implementing procedures.

5.4.7.15. The Company shall monitor the PEP registers so as to better ascertain if potential or current Customer is a PEP or whether any officials or related personal of a Customer are PEPs. Such registers are to be considered as guidance tools and one should always endeavor deeper to determine whether a person is to be considered as a PEP.

5.4.8. Sanction list Screening:

5.4.8.1. The Company shall on the occurrence of the following events or when it deems it fit and proper to do so, conduct a screening of the relevant sanction lists in line with its obligations and FIU implementing procedures respectively.

Document Classification: CONFIDENTIAL						
Name:	Anti-Money Laundering and Countering the Financing of Terrorism policy					
Maintainer:	MLRO	Approver:	Statutory Director			
Status:	In effect	Version:	5.0	Effective Date:	April 10, 2025	Page 18 of 44

5.4.8.2. Upon registration, Customer will be screened with the various sanctions lists issued by the United Nations or the Office of Foreign Assets Control (OFAC) of the US Department of the Treasury or the European Union or any other relevant body responsible for imposing sanctions at a worldwide level. Such screening will then be conducted periodically based on the Customer risk assessment conducted. The frequency of such sanction list screening will be increased should a Customer reach the USD 5000 threshold or the equivalent in another currency, although such frequency will still be determined according to the Customer's risk. Moreover, the frequency of such screening will also be impacted by the PEP status of the particular Customer.

5.4.8.3. In the event that Company becomes aware that one of its Customers, or potential Customers is subject to an international Sanction, or has ties to countries or entities subject to such sanctions, the Company must immediately inform without delay the Curaçao Gaming Control Board (GCB) via their email: info@gcb.cw or in writing through the following address: The Chairman, the Curaçao Gaming Control Board, Emancipatie Boulevard, Dominico F. "Don" Martina 23, Willemstad, Curaçao. All appropriate measure must be taken to ensure that any assets including funds held on behalf of such individual are frozen immediately until further instructions are given by the Curaçao Gaming Control Board.

5.4.9. Prohibited Countries

The list to be found in Annex A, includes all countries from which the Company will not be accepting any Customer traffic and/or registrations.

5.4.10. Customer Verification Procedure

5.4.10.1. Know Your Customer Policy:

5.4.10.1.1. If the Customer reaches the threshold for deposits or withdrawals, a full KYC process is mandatory. The Customer will be required to provide proof of identity, proof of address, and any other documents necessary to verify their identity.

5.4.10.1.2. Customers may be required to upload:

- 5.4.10.1.2.1. A copy of a government-issued document with a photo ID;
- 5.4.10.1.2.2. A selfie with the ID document;
- 5.4.10.1.2.3. A bank statement or utility bill issued within the last three (3) months;
- 5.4.10.1.2.4. Proof of source of wealth and source of funds;

5.4.10.1.3. The KYC process is a critical aspect of Customer verification. Customers who do not satisfy KYC requirements may have deposits and withdrawals restricted until compliance is achieved.

5.4.10.1.4. The Company may verify Customers through additional methods such as video calls or phone calls to confirm identity, transaction activities, and adherence to the platform's terms.

5.4.10.2. Customers will be requested to provide mandatory due diligence documents during the following stages:

- 5.4.10.2.1. Upon request for the first withdrawal;
- 5.4.10.2.2. Reaching the threshold of USD 5000 for deposits or withdrawals.
- 5.4.10.2.3. At any other stage that Company's systems or employees detect any suspicious behaviour of the Customer or have any doubt on the accuracy

Document Classification: CONFIDENTIAL						
Name:	Anti-Money Laundering and Countering the Financing of Terrorism policy					
Maintainer:	MLRO	Approver:	Statutory Director			
Status:	In effect	Version:	5.0	Effective Date:	April 10, 2025	Page 19 of 44

of the information provided during the Registration Process or a Customer Account classified as High Risk.

5.4.10.3. Customers are obliged to provide Company with documents which verify their identity and Address. The Company's employees should oversee this procedure and, where any red flags are raised or registration has been rejected and are unable to complete the registration process, the employees should manually review the documents provided and the reasons for rejection. In such cases, the employees should thoroughly check all the documents provided and third-party verification reports, and reconsider whether the documents should be accepted or rejected, and in case of rejection, whether to request the Customer to provide new documents or suspend the account and report the case to the Head of Compliance/MLRO in line with the Company's internal reporting procedures.

5.4.11. The Company's employees, in terms of Customer verification process, shall review the following documents:

5.4.11.1. Documents needed to verify Customers' identity: A clear, color, scan or photo, alongside with a selfie picture of any of the following:

5.4.11.1.1. Official ID card (both sides);

5.4.11.1.2. Passport (open and display the full photo ID page of the passport holder);

5.4.11.1.3. Driving License (both sides).

5.4.11.2. Documents needed to verify Customers' address: Customer' should follow should provide a clear scan, color photo, PDF or screenshot of any official document addressed to them, issued within the last 3 months, stating their full name and current address. This can include one of the following:

5.4.11.2.1. Utility bill (electricity, water, gas, landline phone bill, internet line account)

5.4.11.2.2. Bank statement or reference letter

5.4.11.2.3. Credit card statement

5.4.11.2.4. Tax/welfare letter

5.4.11.2.5. correspondence from a central or local government authority, department or agency or any other government-issued document.

5.4.11.3. Any additional documents - At any stage, Customers may be asked to provide any further information to those already provided or any additional documentation, at Company's sole discretion. Upon receiving the required documents and in order for the Customer's account to be validated, Company's employees shall conduct a Policy check on the information/documentation received and consider whether more information/documentation is needed. The following checks are to be performed:

5.4.11.3.1. Check whether Customer's personal data listed in the document provided matches the information provided during the registration;

5.4.11.3.2. Cross-Checking of any third-party report on similarity checks and whether Selfie meets the system requirements (clear photo of Customer's entire face without wearing sunglasses, hats, scarves, or any other accessory that covers the face, in whole or in part) have been adhered to;

5.4.11.3.3. Make sure that system does not allow registration of Customers who are underage (according to section Protection of Minors), coming from restricted counties or have another Customer Account in their name;

5.4.11.3.4. Policy Check of documents provided to verify Customers' address;

Document Classification: CONFIDENTIAL						
Name:	Anti-Money Laundering and Countering the Financing of Terrorism policy					
Maintainer:	MLRO	Approver:	Statutory Director			
Status:	In effect	Version:	5.0	Effective Date:	April 10, 2025	Page 20 of 44

5.4.11.3.5. Verify the validity and authenticity documents provided;

5.4.11.3.6. Verify and confirm that the documents provided contain all necessary information, according to the information it is meant to verify.

5.4.12. **Protection Of Minors**

5.4.12.1. Customers under the age of 18 will be denied registering an account. Customers will be required to register before playing for real money. Responsible gambling procedures will be put in place to ensure minors and persons under legal gambling age are denied access to gambling services.

5.4.12.2. The Company will not accept Customers unless they are of legal age (18 years or the legal age of majority in his/her jurisdiction, whichever is greater). The registration process requires confirmation of date of birth, as well as confirmation that the Customer is over 18 years of age.

5.4.12.3. Should a Customer still manage to go through the registration process and is under the age of 18, the Company has implemented controls in order to check and verify the age and identity of the Customer. This check is carried out instantaneously upon registration by the Customer through Location screening. Should this check however fail for some reason, the Company shall still request KYC documentation from the Customer upon first withdrawal. Should at any stage the Customer be found to be a minor, all stakes, winnings and bonuses are to be forfeited, the deposit returned (any part of it which remains) and the account blocked.

5.4.13. **APPLIED DUE DILIGENCE MEASURES AND ACCOUNT CONTROLS BREAKDOWN**

5.4.14. Based on Customer risk class, specific control levels will be applied to each Customer account in order to mitigate the inherent risk posed by any of these classes. The controls will be applied based on which risk criteria is more relevant when calculating Customer score. The list below is by no means exhaustive and Company employees will seek guidance and advice regarding specifically suspicious accounts and situations from middle management, compliance department, MLRO and Senior management when the need for more stringent controls arises.

5.4.15. **Level 1**

5.4.15.1. Proof of ID:

- birth certificates or
- bank statements or
- Passport or
- ID or
- Driving license.

5.4.15.2. Proof of address:

- bank statement or
- utility bill or
- letter from a public authority or
- rental agreement.

5.4.15.3. Proof of funds (where applicable).

5.4.15.4. Copy of Credit card (where applicable).

5.4.15.5. Sanctions screening and PEP status screening.

5.4.15.6. Customer identification updates:

Document Classification: CONFIDENTIAL						
Name:	Anti-Money Laundering and Countering the Financing of Terrorism policy					
Maintainer:	MLRO	Approver:	Statutory Director			
Status:	In effect	Version:	5.0	Effective Date:	April 10, 2025	Page 21 of 44

5.4.15.6.1. every 5 years, unless the Customer has updated their address, surname, or other personal details on their account;

5.4.15.6.2. when identification documents expire.

5.4.16. Level 2

Controls may include but are not limited to:

5.4.16.1. Proof of ID:

- Passport or
- ID or
- Driving license.

5.4.16.2. Proof of address:

- bank statement or
- utility bill or
- letter from a public authority or
- rental agreement.

5.4.16.3. Checking social media, telephone directories, companies' registries or media and news sources.

5.4.16.4. Copy of Credit card (where applicable).

5.4.16.5. Proof of Source of Wealth or Funds (where applicable). Only obtaining a declaration from the customer with some details (e.g. nature of employment/business, usual annual salary etc.) can be sufficient.

5.4.16.6. Sanctions screening and PEP status screening.

5.4.16.7. Customer identification updates:

5.4.16.8. every 5 years, unless the Customer has updated their address, surname, or other personal details on their account;

5.4.16.9. when identification documents expire.

5.4.16.10. Transaction monitoring in accordance with Company guidelines.

5.4.17. Level 3

Controls may include but are not limited to:

5.4.17.1. Proof of ID:

- Passport or
- ID or
- Driving license.
- Collection of additional personal details as necessary.

5.4.17.2. Proof of address:

- bank statement or
- utility bill or
- letter from a public authority or
- rental agreement.

5.4.17.3. Video call with Customer for verification purposes (where applicable).

5.4.17.4. Checking social media, telephone directories, company registries, and media or news sources. The Company can cross-reference the information in its possession with geo-location data, IP address data, funding method information, etc.

Document Classification: CONFIDENTIAL						
Name:	Anti-Money Laundering and Countering the Financing of Terrorism policy					
Maintainer:	MLRO	Approver:	Statutory Director			
Status:	In effect	Version:	5.0	Effective Date:	April 10, 2025	Page 22 of 44

- 5.4.17.5. Proof of Source of Wealth. Obtain detailed information on the Customer's occupation, source of funds, and source of wealth. This includes a copy of every credit card, proof of e-wallet use if the customer is using cryptocurrency, or professional/bank reference letters (in certain cases).
- 5.4.17.6. First Payment. The first payment must be made through an account in the customer's name at a bank that is subject to similar CDD standards.
- 5.4.17.7. Sanctions screening and PEP status screening.
- 5.4.17.8. Policy information review by MLRO
- 5.4.17.9. Approval from senior management is required.
- 5.4.17.10. Customer identification updates:
- 5.4.17.10.1. every 5 years, unless the Customer has updated their address, surname, or other personal details on their account;
 - 5.4.17.10.2. when identification documents expire.
- 5.4.17.11. Transaction monitoring in accordance with Company guidelines.
- 5.4.17.12. Daily account monitoring by relevant teams.
- 5.4.18. Company has multiple stages of Customer Due Diligence (CDD) in place in order to mitigate as many of the risk posed by the possibility of Money Laundering and Terrorist Financing as well as properly understand their Customers as well as the nature of the intended business relationship.
- 5.4.19. To this extent specific mechanism have been put in place in order to:
- 5.4.19.1. Determine who the Customers are;
 - 5.4.19.2. Verify whether that person is the person he/she purports to be;
 - 5.4.19.3. Determine whether a person is acting on his/her own behalf or on behalf of another person;
 - 5.4.19.4. Establish the purpose and intended nature of the business relationship, and the Customer's business and risk profile;
 - 5.4.19.5. In the case of a business relationship, monitor that relationship on an ongoing basis.
- 5.4.20. Company's applied Due Diligence measures consist in the following:
- 5.4.20.1. Identification and Verification of the Customer;
 - 5.4.20.2. Obtaining additional information on the Purpose and Intended Nature of the Business Relationship;
 - 5.4.20.3. Understanding and verifying the Customer's source of wealth and source of funds where applicable;
 - 5.4.20.4. Ongoing Monitoring.
- 5.4.21. **Simplified Due Diligence**
- Such measures shall only be applied on low-risk scenarios, provided none of the other CDD or EDD threshold are reached. In such a case level 1 controls will be applied.
- 5.4.22. **Customer Due Diligence**
- 5.4.22.1. Company requests all Customers to provide standard Customer Due Diligence in the following cases:
 - 5.4.22.1.1. Upon reaching the threshold of USD 5000, the Customer obtains a number of points that exceed the number of low-risk points, and these points cannot be reduced;

Document Classification: CONFIDENTIAL						
Name:	Anti-Money Laundering and Countering the Financing of Terrorism policy					
Maintainer:	MLRO	Approver:	Statutory Director			
Status:	In effect	Version:	5.0	Effective Date:	April 10, 2025	Page 23 of 44

5.4.22.1.2. Any reasonable suspicion towards the Customer is raised;

5.4.22.1.3. A change in the Customer's risk rating.

5.4.22.2. Standard due diligence contains but is not limited to the following documents:

5.4.22.2.1. **Proof of Identity** – This documentation will be used in order to begin verification of Customer identity and will create the basis of the Customer's profile. The proof of identity might consist of, but is not limited to: Copy of Local Government Issued ID, Copy of Passport, Copy of Driver's License, Copy of Residency Card (where applicable).

5.4.22.2.2. **Proof of Address** – This documentation complements the proof of identity and assures the Customer has their residency where they claim they do, so proper measures can be applied to cater to their specific jurisdiction requirements. The proof of address may consist of, but is not limited to Utility Bill, Lease Agreement, Bank Statement.

5.4.22.2.3. **Source of Wealth** – This piece of documentation will be used to determine the overall capacity of the Customer to use the funds they are using on the Company website, as well as to determine if the responsible gambling regulations are respected towards the Customers. Proof of source of wealth may consist of but is not limited to: Bank statement for a longer period of time, Letter from bank confirming the Customer's balances, Proof of transactions that might have provided the Customer with a large amount of funds.

5.4.22.2.4. **Proof of funds** – This piece of documentation is required in situations where a transaction is out of the ordinary or contrary to the estimated Customer rollover capacity per transaction. This is to ensure the funds used for an outstanding transaction have not been acquired by any predicate crime. Proof of funds may consist of but is not limited to: Letter from bank explaining said funds, Proof of sale (in case funds were obtained from the selling of a movable or immovable property), Bank statement specifically showing the provenience of funds used, proof of ownership of any security, proof of ownership of any legal entity and its related financial statements, dividend warrants.

5.4.22.2.5. **Ongoing Monitoring** – As per regulation all Customers need to undergo ongoing monitoring to a certain extent based on risk profile. A less stringent monitoring regime will be applied to Customers that have scored below High Risk (for more details on risk levels please see Onboarding Procedure).

5.4.23. Enhanced Due Diligence

5.4.23.1. As per Policy all Customers that pose a high risk of ML/TF, are politically exposed or it is determined that it will be more prudent to apply EDD measures, will be requested to provide extra documentation and proof of verification based on the most relevant risk factor(s). As described in the Onboarding Procedure each Risk rating warrants a different level of documentation, however if deemed necessary one or more of the following actions will be taken to ensure the Customer is properly verified and the risk of ML/TF is kept under control.

5.4.23.2. The following list describes the most common documents that can be requested for Enhanced Due Diligence purposes; however, it is not exhaustive, and Company reserves the right to request any documentation to the point where management is satisfied with the Customer verification:

Document Classification: CONFIDENTIAL						
Name:	Anti-Money Laundering and Countering the Financing of Terrorism policy					
Maintainer:	MLRO	Approver:	Statutory Director			
Status:	In effect	Version:	5.0	Effective Date:	April 10, 2025	Page 24 of 44

- 5.4.23.2.1. **Copy of Debit/Credit Card** – this piece of documentation is requested to verify that the deposit means used is indeed under the correct name that was collected during the initial identification and verification procedure.
- 5.4.23.2.2. **Bank Statement** – this piece of documentation is requested in cases where money has been transferred by means of bank transfer and helps verify that the account used for the transfer is indeed under the name collected during initial identification and verification. The Bank Statement is also used as supporting documentation for the proof of funds and wealth.
- 5.4.23.2.3. **Letter from the Bank** – this piece of documentation is requested a further proof of Customer's identity as well as to double check his reputability with a financial institution.
- 5.4.23.2.4. **Certified True Copies of Due Diligence Documentation** – certifying the copies of the required documents offers an extra control towards the accurate verification of the Customer's identity by means of a secondary licensed person checking that the documents are veritable. This can be requested when there is suspicion that the documentation might have been tampered with.
- 5.4.23.2.5. **Recorded Video Call** – this action is taken when there are doubts that the person using the Company account is actually the one whose due diligence documentation has been received. Specific interactions are required on behalf of the Customer to make sure that the footage is live. This procedure is not meant to eliminate the risk posed by a non-face-to-face relationship which will still be taken into consideration when analysing the Customer, however it will provide extra assurance of the legitimacy of the Customer's claims.
- 5.4.23.2.6. **Account Review by MLRO** – this action is taken when there is suspicion of ML/TF on behalf of the Customer but there is not sufficient information for filing an STR. The MLRO checks the account and gather all needed information to take a final decision regarding the ML/TF suspicion.
- 5.4.23.2.7. **Management Approval for Relationship Continuation** – In cases where the Customer poses a high risk of ML/TF but does not raise any suspicion based on behaviour or documentation, express approval from management will be required to continue the business relationship.
- 5.4.23.2.8. **More Stringent Account and Transaction Monitoring** – all accounts deemed as High Risk will be subject to more stringent scrutiny from the relevant teams.
- 5.4.23.2.9. **Proof of ownership** of movable/immovable assets.
- 5.4.23.2.10. **Proof of passive income** from investments.
- 5.4.23.2.11. **Proof of income** from the sale of movable or immovable assets.
- 5.4.23.2.12. **Proof of income** from employment.
- 5.4.24. **CDD: Customer Limits and Limit Monitoring** - Based on jurisdictional requirements Customers may need to set deposit limits upon opening an account with Company. Company staff will make sure these limits are applied. If a particular Customer sets their deposit limit higher than the approved amount, they will be contacted by Company's relevant departments and will be requested to provide reasoning for

Document Classification: CONFIDENTIAL						
Name:	Anti-Money Laundering and Countering the Financing of Terrorism policy					
Maintainer:	MLRO	Approver:	Statutory Director			
Status:	In effect	Version:	5.0	Effective Date:	April 10, 2025	Page 25 of 44

their limits. Where any ML or FT suspicions come up based on the Customer behaviour analysis the case will be escalated to Senior Management and a EDD requirement may be triggered.

5.4.25. CUSTOMER RISK LEVEL BREAKDOWN

5.4.25.1. Regardless of the risk level, any users who fail to meet the identification and verification requirements will be blocked.

5.4.25.2. The Customers will be classified as follows:

5.4.25.2.1. **Low-risk** (score 60 to 189) Customers will be required to undergo **Simplified Customer Due Diligence** when their total deposits or withdrawals reach USD 5000, or the equivalent in another currency. The Customers classified as low-risk will be monitored less frequently, and Level 1 account controls will be implemented. However, if their account activity changes significantly, they may be reclassified into a higher risk category.

5.4.25.2.2. **Medium Risk** (Score 90 to 160) – Customers with a medium risk score will be required to undergo **Customer Due Diligence** when their total deposits or withdrawals reach USD 5000, or the equivalent in another currency. The Customers classified as medium risk will be subject to stricter monitoring compared to medium - low risk Customers, and Level 2 account controls will be implemented. Specific Enhanced Due Diligence will be requested if necessary.

5.4.25.2.3. **High Risk** (Score 161 to 280) – Customers with a high-risk score will be required to undergo **Enhanced Due Diligence** when their total deposits or withdrawals reach USD 5000, or the equivalent in another currency. Customers classified as high-risk will be subject to the highest level of scrutiny in their ongoing monitoring, and Level 3 account controls will be implemented. Full Enhanced Due Diligence will be required. If a Customer is classified as high-risk, due diligence procedures should be initiated immediately, even if no withdrawal request or deposits has been made.

5.4.25.2.4. **PEPs (Politically Exposed Persons)** - will be classified as their own category and will receive exceptionally stringent attention and monitoring. All Customers that classify as PEPs will need to undergo Compulsory Due Diligence as well as full **Enhanced Due Diligence** including proof of wealth, as well as proof of funds for all transactions higher than USD 500. Level 3 account controls will be implemented.

5.4.25.2.5. **PROHIBITED (Score 281 and above)** – Customers with a risk score of 281 or higher are classified as prohibited and are not eligible to engage with the company's services. The company must immediately terminate any existing relationship with such Customers. Customers classified as prohibited will not be allowed to re-engage with the company under any circumstances, and any attempt to circumvent the prohibition must be flagged and reported immediately.

Document Classification: CONFIDENTIAL						
Name:	Anti-Money Laundering and Countering the Financing of Terrorism policy					
Maintainer:	MLRO	Approver:	Statutory Director			
Status:	In effect	Version:	5.0	Effective Date:	April 10, 2025	Page 26 of 44

5.5. ONGOING MONITORING

5.5.1.**General.** The regular monitoring of the Customers' accounts and transactions is an imperative element in the effective controlling of the risk of Money Laundering and Terrorist Financing. In this respect, the MLRO shall be responsible for maintaining, as well as developing the on-going monitoring process of the Company.

5.5.2.**Procedures.** The procedures and frequency relating to the monitoring of Customers' profiles, accounts and examination of transactions on the basis of Customer's level of risk shall include the following:

5.5.2.1.the identification of:

- 5.5.2.1.1. transactions which, as of their nature, may be associated with money laundering or terrorist financing;
- 5.5.2.1.2. unusual or suspicious transactions that are inconsistent with the economic profile of the Customer for the purposes of further investigation;
- 5.5.2.1.3. in case of any unusual or suspicious transactions, the administrator handling the specific Customer as well as the Head of that particular Department shall be responsible to communicate with the MLRO

5.5.2.2.further to Section (5.5.2.1.) above, the investigation of unusual or suspicious transactions by the MLRO. The results of the investigations are recorded separately and kept in the file of the Customers concerned;

5.5.2.3.the ascertainment of the source and/or origin of the funds credited to accounts;

5.5.2.4.the use of appropriate IT systems;

5.5.2.5.For the Company to comply with its monitoring requirements it shall review the Customer's file according to the timeframes, as per section 5.5.3 below and takes into consideration the following to assess whether any additional or replacement documentation / evidence might be required:

- 5.5.2.5.1.Update of any expired identification documentation
- 5.5.2.5.2.Update of any changes in the companies' structure and involved persons.
- 5.5.2.5.3.Changes in the Customers' activities which might have an impact of the Customers' economic profile;
- 5.5.2.5.4.Reviewing ways in which new products and services may be used by criminals for money laundering and/or terrorist financing purposes, and how these ways may change to conceal such illicit activities;
- 5.5.2.5.5.The compliance officer performs checks to ensure that the relevant reviews take place and documentation are kept accordingly;
- 5.5.2.5.6.Reporting and accountability by the compliance officer to the Board of Directors and Senior Management;
- 5.5.2.5.7.Liaising with the Curacao Gaming Control Board, FIU, or any other relevant/appliable authority in case where such liaising is required.

5.5.3.Timeframes

5.5.3.1. The time frames set below shall act as guidelines for the KYC officer when setting the dates for the re-review dates. Such time frames may be changed if justified notwithstanding the Customer has been risked as in a category, provided such justification is recorded. Furthermore, these time frames shall be changed and updated should any of the factors effecting the risk the Customer poses will change. The below time frames shall be taken as guidance points and not as a mandatory rule:

Document Classification: CONFIDENTIAL						
Name:	Anti-Money Laundering and Countering the Financing of Terrorism policy					
Maintainer:	MLRO	Approver:	Statutory Director			
Status:	In effect	Version:	5.0	Effective Date:	April 10, 2025	Page 27 of 44

Risk Classification	Time Frames
Low Risk	30 - 36 months
Medium Risk	18 - 30 months
High Risk	12 - 18 months

5.5.4. Pay-out Management Procedure:

Checks to be performed on each pay-out:

5.5.4.1. **Account check** - The owner of the Company account must be the same person as the owner of the bank account, credit card or any other payment method used to send and receive funds. All account information, like address, email, date of birth etc., must be complete and authentic. Withdrawals will be made to the same source where the funds originated (where possible).

5.5.4.2. **Deposits must have been used** - On each pay-out, the Company will verify whether the deposits have been used for stakes. All deposits need to have been wagered at least three times when a bonus was not credited before a withdrawal request can be made. A pay-out cannot be processed if the deposited amount has not been used for stakes. If the deposited amount has not been used, the pay-out has to be denied. Furthermore, the latest winnings have to be checked for correctness.

5.5.4.3. **Fulfilment of bonus rules** - Before a pay-out can be deducted from the Customer's account, the account has to be checked if a bonus has been given to the Customer since the last pay-out. When a bonus has been credited, the account has to be checked for fulfilment of the bonus rules applicable to that bonus. If bonus rules have not been fulfilled the requested pay-out cannot be completed.

5.5.4.4. **Deposit of funds**. Funds deposited in the gaming wallet can only be used for gaming activity. Should Company notice regular changes by Customers to the payment method linked to the gaming wallet, the account will be temporarily suspended until the necessary explanations are provided by the Customer for these changes.

Company does not allow Customers to transfer funds between accounts under any circumstances.

Company's KYC team continuously monitors Customers' deposit activity as well and has automated processes in place to receive notifications when Customers achieve the USD 5000 (five thousand) transaction limit.

5.5.5. Risk Profile for Company

5.5.5.1. The risk profile and Risk appetite for Company will be calculated based on the Business Risk Assessment done at a minimum once every three years. The Business Risk Assessment will take into consideration all Risks the Company faces constantly as well as the mitigating factors controlling the inherent risk. Modifications will be done to the policies and procedures for Company on the basis of the resulting residual risk, as soon as the need arises.

5.5.5.2. Withdrawals can only be paid to the same Customers' account used to deposit money. In the event that the payment method used does not allow for Company to settle payouts to the same payment method, then Company must identify and verify that the method used to settle the withdrawal request belongs to the Customer in question.

5.5.5.3. Company does not accept cash from Customers, and funds may only be received through online transfer. In the same manner no withdrawals can be processed as cash. Withdrawals will always be remitted to the same account

Document Classification: CONFIDENTIAL						
Name:	Anti-Money Laundering and Countering the Financing of Terrorism policy					
Maintainer:	MLRO	Approver:	Statutory Director			
Status:	In effect	Version:	5.0	Effective Date:	April 10, 2025	Page 28 of 44

from where the funds originated or to an account or payment method which has been verified as belonging to the Customer.

- 5.5.5.4. For every approved Customer withdrawal request the Company will do its utmost to process the transaction in the least possible time, in particular to not exceed 7 working days.
- 5.5.5.5. At all times management shall ensure that the total of all the Customers' account funds including any funds in transit shall be at least equal to the aggregate of the amount standing to the credit of the Customers' accounts held by the Company.
- 5.5.5.6. CDD documentation is always requested and verified for all Customers when a deposit or withdrawal reaches USD 5000 or more.
- 5.5.5.7. The system will automatically stop minors from playing as Customers inputting a date of birth below the age of 18 years of age or the applicable age within their country of residence will not be able to complete the registration process.

5.6. RELIANCE ON THIRD PARTIES TO PERFORM CUSTOMER DUE DILIGENCE

- 5.6.1. The Company shall be responsible to create and maintain its own Customer base, and, for the foreseeable future, shall not engage any intermediaries or Agents nor shall it accept Customers coming from such individuals or entities.
- 5.6.2. Should the Company decided to change its policy on the above, a more detailed policy is to be created and approved by the board of directors, highlighting the manner in which such entities will be handled in line with the applicable legislation and regulation at that time.
- 5.6.3. Introducers, such as affiliates do not fall within such category as their role is to merely introduce the Customer to the Company and will have no further involvement in the business relationship.

5.7. SUSPICIOUS ACTIVITY REPORTING

- 5.7.1. In any cases where the Company encounters, verifies or there exists a reasonable suspicion that any form of money laundering is taking place or being attempted, such activity will be reported to the Financial Intelligence Unit of Curacao, as required. The activity will be reported through the portal for filing and submitting of suspicious transaction reports (STR) and Suspicious Activity reports (SAR), as designated by the FIU (currently go AML portal - https://portal.fiucuracao.cw/goAMLWeb_PRD/Home). The Company, through its MLRO is responsible to ensure that when an STR is filed, all supporting documentation and information pertaining to why the transactions, as well as the Customer has been flagged as suspicious must also be submitted. Any employee and/or Company officer having suspicion that a Customer is involved in any stage of ML or TF, is attempting to launder money using the products and/or services of the Company must report such suspicion to the MLRO by not later than 24 hours from when such suspicion is formed. The MLRO, upon receipt of such report, must initiate an investigation into the suspicious activity and/or transaction and verify if such suspicion is objectively justified. This is to be done in the shortest time possible. This notwithstanding, the MLRO may still continue to investigate to gather the evidence required to submit a complete SRT/SAR.
- 5.7.2. The financial task force on money laundering site is checked regularly in order to keep abreast with the latest updates and blacklist jurisdictions as well as jurisdictions which do not abide to FATF and anti-money laundering regulations.
- 5.7.3. The definition of a suspicious transaction as well as the types of suspicious transactions which may be used for Money Laundering and Terrorist Financing are almost unlimited. Suspicion of ML/FT is subjective and one must consider a number of circumstances

Document Classification: CONFIDENTIAL						
Name:	Anti-Money Laundering and Countering the Financing of Terrorism policy					
Maintainer:	MLRO	Approver:	Statutory Director			
Status:	In effect	Version:	5.0	Effective Date:	April 10, 2025	Page 29 of 44

together in order to be able to come to a reasonable conclusion that suspicion does indeed subsist. A suspicious transaction or activity will often be one which is inconsistent with a Customer's known, transaction pattern/activities or with the normal deposit/wagering activity of the specific Customer, or in general with the economic profile that the Company has created for the Customer. The Company shall ensure that it maintains adequate information and knows enough about its Customers' activities in order to recognize on time that a transaction or a series of transactions is unusual or suspicious.

5.7.4. Knowledge. Knowledge may be deemed to be an objective criterion and therefore it is not difficult to ascertain whether there is ML/FT. If for any reason the MLRO, or any other employee of the Company, is aware or is in possession of information that indicates that any of the above activities may have taken place, are taking place, or will be taking place, the MLRO should immediately proceed with filing a report with the FIU.

5.7.5. Suspicious Transactions

5.7.5.1. The definition of a suspicious transaction as well as the types of suspicious transactions which may be used for Money Laundering and Terrorist Financing are almost unlimited. Suspicion of ML/FT is subjective and one must consider a number of circumstances together in order to be able to come to a reasonable conclusion that suspicion does indeed subsist. A suspicious transaction will often be one which is inconsistent with a Customer's known legitimate business or personal activities or with the normal business of the specific Customer, or in general with the economic profile that the Company has created for the Customer. The Company shall ensure that it maintains adequate information and knows enough about its Customers' activities in order to recognise on time that a transaction or a series of transactions is unusual or suspicious.

5.7.5.2. Examples of what might constitute suspicious transactions/activities related to Money Laundering and Terrorist Financing are listed in Annex B of the Policy. The relevant list is not exhaustive nor it includes all types of transactions or services that may be requested to be used, nevertheless it can assist the Company and its employees (especially the MLRO and the Head of the Know Your Customer Department) in recognising the main methods used for Money Laundering and Terrorist Financing. The detection by the Company of any of the transactions contained in the said list prompts further investigation and constitutes a valid cause for seeking additional information and/or explanations as to the source and origin of the funds for the payments and intended transactions, the nature and economic/business purpose of the underlying transactions requested, and the circumstances surrounding the particular activities.

5.7.5.3. In order to identify suspicious transactions, the MLRO shall perform the following activities:

5.7.5.3.1. Monitor on a continuous basis any changes in the Customer's financial status, business activities, type of transactions etc.

5.7.5.3.2. Monitor on a continuous basis if any Client is engaged in any of the practices described in the list containing examples of what might constitute suspicious transactions/activities related to Money Laundering and Terrorist Financing which is mentioned in Annex B of this Policy.

5.7.5.3.3. Provide any adequate training to any and all staff who will be in contact with any Customer, agents, Customer's officers, Customer's representatives, Customer's transactional information and / or documentation Customer's, operational information and / or

Document Classification: CONFIDENTIAL						
Name:	Anti-Money Laundering and Countering the Financing of Terrorism policy					
Maintainer:	MLRO	Approver:	Statutory Director			
Status:	In effect	Version:	5.0	Effective Date:	April 10, 2025	Page 30 of 44

documentation and any other information and/or documentation which can lead to knowledge or suspicion being detected.

5.7.5.4. Furthermore, the MLRO shall perform the following activities:

5.7.5.4.1. Receive and investigate information from the Company's employees, on suspicious transactions which creates the belief or suspicion of money laundering. This information is reported on the Internal Suspicion Report or any other form which may be deemed appropriate from time to time in accordance with the urgency and severity of the situation. The said reports are archived by the MLRO;

5.7.5.4.2. evaluate and check the information received from the employees of the Company, with reference to other available sources of information and the exchanging of information in relation to the specific case with the reporter and, where this is deemed necessary, with the reporter's supervisors. The information which is contained on the report which is submitted to the MLRO is evaluated on the Internal Evaluation Report, which is also filed in a relevant file;

5.7.5.4.3. if, as a result of the evaluation described above, the MLRO decides to disclose this information to the FIU, then he prepares a written report, which he submits to the FIU, according to Sections below.

5.7.5.4.4. if as a result of the evaluation described above, the MLRO decides not to disclose the relevant information to the FIU, then he fully explains the reasons for his decision on the Internal Evaluation Report.

5.7.6. MLRO's Report to the FIU

5.7.6.1. After the submission of STR/SAR reports, the Company may subsequently wish to terminate its relationship with the Customer concerned for de-risking reasons or to keep the account suspended until further notice/information is obtained from the FIU. In such an event, the Company exercises caution, according to the Law, not to alert the Customer concerned that a suspicious report has been submitted to the FIU. Close liaison with the FIU is, therefore, maintained in an effort to avoid any frustration to the investigations being conducted. If no information and/or directions are given by the FIU, it shall be up to the Company to decide on the best course of action, whilst at all times ensuring that no tipping-off takes place.

5.7.6.2. Furthermore, after the submission of a suspicious transaction/activity report, the Customers' accounts and services rendered concerned as well as any other connected accounts are placed under the close monitoring of the MLRO and cease to be operative if deemed appropriate to do so without tipping off or risking tipping off the reported individual or entity.

5.7.7. Submission of Information to the FIU.

The Company shall ensure that in the case of a suspicious transaction investigation by the FIU, the MLRO will be able to provide without delay the following information:

5.7.7.1. the identity of the holders for which the services have been provided;

5.7.7.2. the identity of the Beneficial Owners;

5.7.7.3. the identity of the persons authorised to act on behalf of the Beneficial Owners;

5.7.7.4. data of the volume of funds or level of transactions used for the services being rendered and flowing through the accounts created for the Company;

5.7.7.5. connected accounts, if any;

Document Classification: CONFIDENTIAL						
Name:	Anti-Money Laundering and Countering the Financing of Terrorism policy					
Maintainer:	MLRO	Approver:	Statutory Director			
Status:	In effect	Version:	5.0	Effective Date:	April 10, 2025	Page 31 of 44

5.7.7.6. in relation to specific transactions:

- 5.7.7.6.1. the origin of the funds
- 5.7.7.6.2. the type and amount of the currency involved in the transaction
- 5.7.7.6.3. the form in which the funds were placed or withdrawn, for example cash, cheques, wire transfers
- 5.7.7.6.4. the identity of the person that gave the order for the transaction
- 5.7.7.6.5. the destination of the funds
- 5.7.7.6.6. the form of instructions and authorisation that have been given
- 5.7.7.6.7. the type and identifying number of any account involved in the transaction.
- 5.7.7.6.8. any other information which is available and deemed to be essential to the investigation

In order to identify suspicious transactions, the MLRO shall perform the following activities:

- 5.7.7.7. Monitor on a continuous basis any changes in the Customer's financial status, business activities, type of transactions etc.
 - 5.7.7.8. Provide any adequate training to any and all staff who will be in contact with any Customer, agents, Customer's officers, Customer's representatives, Customer's transactional information and/or documentation Customer's, operational information and/or documentation and any other information and/or documentation which can lead to knowledge or suspicion being detected.
- 5.7.8. The MLRO shall belong hierarchically to the higher ranks of the Company's organisational structure so as to command the necessary authority. Furthermore, the MLRO shall lead the Company's Money Laundering Compliance procedures and processes and report to the Senior Management. The MLRO shall also have access to all relevant information necessary to perform his duties. The level of remuneration of the MLRO shall not compromise his objectivity.
- 5.7.9. Furthermore, the MLRO shall perform the following activities:
- 5.7.9.1. Receive and investigate information from the Company's employees, on suspicious transactions which creates the belief or suspicion of money laundering. This information is reported on the Internal Suspicion Report or any other form which may be deemed appropriate from time to time in accordance with the urgency and severity of the situation. The said reports are archived by the MLRO;
 - 5.7.9.2. evaluate and check the information received from the employees of the Company, with reference to other available sources of information and the exchanging of information in relation to the specific case with the reporter and, where this is deemed necessary, with the reporter's supervisors. The information which is contained on the report which is submitted to the MLRO is evaluated on the Internal Evaluation Report, which is also filed in a relevant file;
 - 5.7.9.3. if, as a result of the evaluation described above, the MLRO decides to disclose this information to the FIU, then he prepares a written report, which he submits to the FIU.
 - 5.7.9.4. if as a result of the evaluation described above, the MLRO decides not to disclose the relevant information to the FIU, then he fully explains the reasons for his decision on the Internal Evaluation Report.

Document Classification: CONFIDENTIAL						
Name:	Anti-Money Laundering and Countering the Financing of Terrorism policy					
Maintainer:	MLRO	Approver:	Statutory Director			
Status:	In effect	Version:	5.0	Effective Date:	April 10, 2025	Page 32 of 44

- 5.7.9.5. to act as a first point of contact with the FIU, upon commencement of and during an investigation as a result of filing a report to the FIU according as indicated above;
- 5.7.9.6. to ensure the preparation and maintenance of the lists of Customers categorised following a risk-based approach, which contains, among others, the names of Customers, their account number and the dates of the commencement of the Business Relationship. Moreover, the MLRO ensures the updating of the said list with all new or existing Customers, in the light of any additional information obtained;
- 5.7.9.7. to detect, record, and evaluate, at least on an annual basis, or on the happening of any even which might have an impact on the overall risk, all risks arising from existing and new Customers, new financial instruments and services and update and amend the systems and procedures applied by the Company for the effective management of the aforesaid risks should it be required and appropriate to do so;
- 5.7.9.8. to evaluate the systems and procedures applied by a third party with whom the Company has entered into a reliance agreement in terms of Customer Due Diligence including Customer Identification and Verification of the Customer, Identification & Verification of Beneficial Owners as well as the Purpose & Intended Nature of the Business Relationship applied, and approves the cooperation with such third parties;
- 5.7.9.9. to ensure that all the branches and subsidiaries of the Company, if any, have taken all necessary measures for achieving full compliance with the provisions of the Policy, in relation to Customer identification, due diligence and record keeping procedures;
- 5.7.9.10. to provide advice and guidance to the employees of the Company on subjects related to money laundering and terrorist financing;
- 5.7.9.11. to acquire the knowledge and skills required for the improvement of the appropriate procedures for recognising, preventing and obstructing any transactions and activities that are suspected to be associated with money laundering or terrorist financing;
- 5.7.9.12. to determine and whether the Company's departments and employees require further training and education for the purpose of preventing Money Laundering and Terrorist Financing and organising appropriate training sessions/seminars. In this respect, the MLRO shall prepare and apply an annual staff-training program. Also, the MLRO assesses the adequacy of the education and training provided;
- 5.7.9.13. to prepare the Annual Report, as required by the FIU and any other applicable authority;
- 5.7.9.14. to respond to all requests and queries from the FIU and provide all requested information and fully cooperate with the FIU, if required;
- 5.7.9.15. to maintain a registry which includes the reports of suspicious transactions, and relevant statistical information (e.g. the department that submitted the internal report, date of submission to the MLRO, date of assessment, date of reporting to the FIU), the evaluation reports and all the documents that verify the accomplishment of his duties.
- 5.7.9.16. To review the Customer's files and Customer Questionnaire and to approve or reject prospective High-Risk Customers.

Document Classification: CONFIDENTIAL						
Name:	Anti-Money Laundering and Countering the Financing of Terrorism policy					
Maintainer:	MLRO	Approver:	Statutory Director			
Status:	In effect	Version:	5.0	Effective Date:	April 10, 2025	Page 33 of 44

- 5.7.9.17. to develop and establish the Customer Acceptance Policy and submit it to the Directors for consideration and approval;
- 5.7.9.18. to review and update the Policy as may be required from time to time, and for such updates to be communicated to the Directors for their approval, at least annually or at any such period as may be deemed necessary by the MLRO;
- 5.7.9.19. to monitor and assess the correct and effective implementation of the policy practices, measures, procedures and controls and in general the implementation of the Policy. In this respect, the MLRO shall apply appropriate monitoring mechanisms (e.g. on-site visits to different departments of the Company) which will provide him with all the necessary information for assessing the level of compliance of the departments and employees of the Company with the procedures and controls which are in force. In the event that the MLRO identifies shortcomings and/or weaknesses in the application of the required practices, measures, procedures and controls, shall give appropriate guidance for corrective measures and where deems necessary informs the Directors and Senior Management.

5.8. ANTI-MONEY LAUNDERING COMPLIANCE PROGRAM

The Company maintains a comprehensive AML Compliance Program that includes:

5.8.1. Risk-Based Approach

- 5.8.1.1. The AML Laws imposes prevention and enforcement for subject persons. Therefore, Company applies the risk-based approach for the purposes of preventing and detecting money laundering and fraud.
- 5.8.1.2. The Company will assess each Customer's risk profile and implement ongoing monitoring to detect unusual transactions. Special attention will be paid to Customer that attempt to circumvent KYC measures or display suspicious behavior.
- 5.8.1.3. The following steps are followed in order to implement the risk-based approach:
 - 5.8.1.3.1. **Identification** – The identification process involves the identification of internal and external risk factors which increase the risks being faced by the Company. Predominantly, Company must assess the domestic and foreign money laundering risks affecting their target market/s. In the case scenario, whereby Customers are registering from countries that are non-compliant with AML Laws and fraud management procedures, an onus is imposed on the Company to ensure that all Customers comply with the procedures implemented by the Company. In order to actively assess and be aware of the risks the business is facing; the Company must update its business risk assessment on a yearly basis or whenever the need arises (whichever occurs first) so as to ensure that the Company is constantly aware of the ever-changing risk scenarios and mitigate such risks accordingly. The Company identifies and classifies risks in four main categories:
 - Customer Risk;
 - Product, service and transaction risk;
 - Geographical Risk;
 - Distribution channels Risk.
 - 5.8.1.3.2. **Assessment** – As an online gaming operator, management as well as the shareholder/s of the Company understand and are aware that there is susceptibility to a certain level of high risk. Furthermore, management must stimulate awareness to detect the lack of implementation of stringent

Document Classification: CONFIDENTIAL						
Name:	Anti-Money Laundering and Countering the Financing of Terrorism policy					
Maintainer:	MLRO	Approver:	Statutory Director			
Status:	In effect	Version:	5.0	Effective Date:	April 10, 2025	Page 34 of 44

measures in order to detect fraudulent activity; the sites may become an easy target to launder money, this is a clear example of inherent risk. When carrying out the necessary risk assessment, the Company must evaluate the risks identified in the four categories mentioned above:

5.8.1.3.3. **Customers:** Evaluating the risk level posed by individual customers, their background, and behavior.

5.8.1.3.4. **Geographic Areas:** Assessing risks based on the regions in which the company operates and where its customers are located.

5.8.1.3.5. **Products, Services, and Transactions:** Reviewing the nature of products/services offered and the types of transactions undertaken.

5.8.1.3.6. **Delivery Channels:** Evaluating the risk tied to how products and services are delivered, especially through online or remote channels where identity verification may be more difficult.

5.8.1.4. **Monitoring and Follow up** – The Fraud and Compliance department scrutinizes the risk assessments carried out in order to recognize gaps in procedures and areas of improvement in procedures to reduce inefficiencies. It is important to note that inefficiencies may be present in both procedures and lack of technical expertise adopted by staff. When there is a change in the Company AML policy, or implementing procedures or AML rules in the Law, this Policy, and associated materials, will be updated.

5.8.1.5. **Supervisory** – This process includes the review of risk assessments reviewed and the Fraud and Compliance department ensures that training is provided to staff involved to ensure that any updates in Laws are applied accordingly.

5.8.2. Internal Controls – Implementation Of The Risk Based Approach

5.8.2.1. Following the identification of inherent risk, management is required to implement the respective controls in order to mitigate such risks. The first step to adopting some form of internal control, the Company must appoint at least one individual (depending on the size of the Company) who is a member of the board of directors responsible for the compliance with this Policy.

5.8.2.2. Ensure that independent testing is carried out to ensure that such controls in place are in place and do not impose any risk to the Company due to present inefficiencies.

5.8.2.3. Furthermore, the Company would provide an independent audit function to test compliance (including sample testing) with their policies, procedures and controls. The independent testing must be conducted at least annually by an internal audit department or by an outside independent party such as the external auditor of the financial institution. These tests may include:

5.8.2.3.1. evaluation of the AML/CFT Policy;

5.8.2.3.2. review of financial records;

5.8.2.3.3. interviews with employees who handle transactions and with their supervisors;

5.8.2.3.4. a sampling of unusual transactions on and beyond the threshold(s) followed by a review of compliance with the internal and external policies and reporting requirements; and

5.8.2.3.5. assessment of the adequacy of the record retention system.

Document Classification: CONFIDENTIAL						
Name:	Anti-Money Laundering and Countering the Financing of Terrorism policy					
Maintainer:	MLRO	Approver:	Statutory Director			
Status:	In effect	Version:	5.0	Effective Date:	April 10, 2025	Page 35 of 44

5.8.3. Dynamic Risk Management

- 5.8.3.1. Risk management is a continuous process, carried out on a dynamic basis. Risk assessment is not an isolated event of a limited duration. Customers' activities and requests change as well as the services they require to be provided with.
- 5.8.3.2. In this respect, it is the duty of the MLRO to undertake regular reviews of the characteristics of existing Customers, new Customers, services and the measures, procedures and controls designed to mitigate any resulting risks from the changes of such characteristics. These reviews shall be duly documented as per the Policy's requirements, as applicable, and form part of the Annual Money Laundering Report.
- 5.8.3.3. It is also important for the MLRO to monitor and ensure that the proper procedures are being implemented, and the risk-based approach principle is truly being followed in all areas of the Company. By doing so, one will also be ensuring that although certain products or Customers may be of a higher risk, the Company may continue providing these services and assisting these Customers due to the risk being mitigated through the proper policies being implemented.
- 5.8.3.4. Company employs a combination of software tools and Policy oversight to ensure ongoing monitoring of transactions and Customer activities. These measures will be continuously updated to align with regulatory changes.

5.8.4. Implement and Clearly Communicate Policies and Procedures to Staff

- 5.8.4.1. Due to the size of the operation, management is principally responsible for most functions within the Company. Management is aware of the policies and procedures in place throughout the group of companies. For example: withdrawals can be requested only for amounts that have been wagered at least three times. If the deposited funds requested for withdrawal have not been put into play, a fee of 10% may be withheld from the withdrawal amount, or the request may be declined. This protects the Company from being abused for money laundering purposes and also protects Our system from free-of-charge deposits that may be abused to Our disadvantage.
- 5.8.4.2. All withdrawal requests are initially checked by the KYC department, which monitors all the withdrawal requests and denotes those which are suspicious, based on any suspected fraudulent background. Due the size of the operation and knowledge of the Customer database, various Customer/s due diligence and verification processes are carried out Policy and automatically by KYC department. In any case where a transaction is complex or unusually large or there is an unusual pattern of transactions and the transaction has no apparent economic purpose in relation to the nature of the business, such transaction is flagged Policy as suspicious, and investigations are immediately kicked off.
- 5.8.4.3. Checks for multiple accounts, individuals which may have been blacklisted by any relevant organization or Company, transaction and betting behaviour, handled amounts, deposit/withdrawal methods are carried out in order to identify any suspicious activity.
- 5.8.4.4. The Company is committed to ensuring that all employees handling financial transactions receive regular and comprehensive training on AML policies, including the identification of red flags for suspicious activity, appropriate procedures for escalating issues, and the use of internal reporting channels to ensure compliance with regulatory requirements.

Document Classification: CONFIDENTIAL						
Name:	Anti-Money Laundering and Countering the Financing of Terrorism policy					
Maintainer:	MLRO	Approver:	Statutory Director			
Status:	In effect	Version:	5.0	Effective Date:	April 10, 2025	Page 36 of 44

5.8.5. Training

- 5.8.5.1. The Company must ensure that training and updates are provided to staff and key persons involved in the prevention of AML and fraud within the Company. Such training may be in-house or from third party providers.
- 5.8.5.2. All training provided should be in line and in proportion to the roles and duties of the individual employee.
- 5.8.5.3. Training should be tailored to the tasks and duties of the employee and the Company should not adopt a one size fits all approach. Training should be provided regularly and when needed. However, a yearly refresher course should be provided to ensure that all staff are up to date on recent developments.
- 5.8.5.4. Records of such training received must be kept on file as proof of attendance of such training.
- 5.8.5.5. The Company provides annual training for all employees involved in AML procedures to ensure they are equipped to detect suspicious behavior. The training program is tailored to specific roles and updated regularly.

5.8.5.6. Employees' obligations:

- 5.8.5.6.1. The Company's employees shall be personally liable for failure to report any information relating to knowledge or suspicion, regarding money laundering or terrorist financing;
- 5.8.5.6.2. the employees must cooperate and report internally, without delay, and by not later than 24 hours, anything that comes to their attention in relation to transactions for which there are grounds for suspicion that the person is involved in money laundering or terrorist financing
- 5.8.5.6.3. according to the applicable Law, the Company's employees shall fulfil their legal obligation to report their suspicions regarding Money Laundering and Terrorist Financing, after their compliance with Section 5.8.5.7.2 above.

5.8.5.7. Employees' Education and Training:

- 5.8.5.7.1. The MLRO shall ensure that the employees are fully aware of their legal obligations according to the applicable Laws, regulations, and implementing procedures by introducing a complete employees' education and training program;
- 5.8.5.7.2. the timing and content of the training provided to the employees of the various departments will be determined according to the needs of the Company. The frequency of the training can vary depending on to the amendments of legal and/or regulatory requirements, employees' duties as well as any other changes in the system of Curacao;
- 5.8.5.7.3. the training program aims at educating the Company's employees on the latest developments in the prevention of Money Laundering and Terrorist Financing, including the practical methods and trends used for this purpose;
- 5.8.5.7.4. the training program will have a different structure for new employees, existing employees and for different departments of the Company according to the services that they provide. On-going training shall be given at regular intervals so as to ensure that the employees are reminded of their duties and responsibilities and kept informed of any new developments.

Document Classification: CONFIDENTIAL						
Name:	Anti-Money Laundering and Countering the Financing of Terrorism policy					
Maintainer:	MLRO	Approver:	Statutory Director			
Status:	In effect	Version:	5.0	Effective Date:	April 10, 2025	Page 37 of 44

5.8.5.7.5. The MLRO shall be responsible to refer to the relevant details and information in his/her Annual Report in respect of the employees' education and training program undertaken each year.

5.8.5.8. **MLRO Education and Training Program**

5.8.5.8.1. The MLRO shall be responsible for any updates in the Law and attend any external training necessary. Based on his/her training the MLRO will then provide training to the employees of the Company further to Section 5.8.5.7 above.

5.8.5.8.2. The main purpose of the MLRO training is to ensure that relevant employee(s) become aware of:

- 5.8.5.8.2.1. the Laws
- 5.8.5.8.2.2. the Company's Anti-Money Laundering Policy
- 5.8.5.8.2.3. the statutory obligations of the Company to report suspicious transactions
- 5.8.5.8.2.4. the employees own personal obligation to refrain from activity that would result in money laundering
- 5.8.5.8.2.5. the importance of the Customers' due diligence and identification measures requirements for money laundering prevention purposes.

5.8.5.9. The MLRO shall be responsible to include information in respect of his/her education and training program(s) attended during the year in his/her Annual Report.

5.8.6. **Record Keeping and Monitoring**

5.8.6.1. **General.**

5.8.6.1.1. The KYC Department and, in some cases, the Customer Service Department of the Company shall maintain records of:

- 5.8.6.1.1.1. the Customer identification documents obtained during the Customer identification and due diligence procedures, as applicable; and
- 5.8.6.1.1.2. the details of all relevant records with respect to the provision of investment services to Customers.

5.8.6.1.2. The documents/data mentioned above shall be kept for a period of at least five (5) years, which is to start running either from the termination of a business relationship or from the date on which an occasional transaction has been executed.

5.8.6.1.3. It is provided that the documents/data mentioned in Section 5.8.6.1.1 above which may be relevant to ongoing investigations shall be kept by the Company until the FIU confirms that the investigation has been completed and the case has been closed. Furthermore, should the Company require the documents for the institution, prosecution or to defend against any claim for which a longer prescriptive period exists, than such records will be kept until such time as the claim is extinguished or such prescriptive period has elapsed.

5.8.6.2. **Format of Records**

5.8.6.2.1. The MLRO shall retain the documents/data mentioned in this Policy, other than the original documents or their Certified true copies that are kept in a hard copy form, in other forms, such as electronic form, provided that the MLRO shall be able to retrieve the relevant documents/data

Document Classification: CONFIDENTIAL						
Name:	Anti-Money Laundering and Countering the Financing of Terrorism policy					
Maintainer:	MLRO	Approver:	Statutory Director			
Status:	In effect	Version:	5.0	Effective Date:	April 10, 2025	Page 38 of 44

without undue delay and present them at any time, to the FIU or any other relevant authority, after a relevant request.

5.8.6.2.2. In case the Company will establish a documents/data retention policy, the MLRO shall ensure that the said policy shall take into consideration the requirements of the Law.

5.8.6.2.3. The Internal Auditor shall review the adherence of the Company to the above, at least annually.

5.8.6.3. **Certification and language of documents**

5.8.6.3.1. The documents/data obtained, shall be in their original form or as a copy of the original. In high-risk cases or if deemed appropriate, the Company may request documents to be certified as true copies of the original and/or be apostilled. In the case that the documents/data are certified as true copies by a different person than the Company itself or by the third party with whom a reliance and or intermediary agreement has been reached, the documents/data must be apostilled or notarized or certified by a professional whose identity and professional capacity must be confirmed and verified. In certain high-risk cases, identification and verification of the certifier may also be necessary.

5.8.6.3.2. A true translation shall be attached in the case that the documents of Section (5.8.6.3.1) above are in a language other than English or a language which is not known by the person reviewing the document.

5.8.6.3.3. Each time the Company shall proceed with the acceptance of a new Customer, the Head of the KYC Department shall be responsible for ensuring compliance with the provisions of points above.

6. COMPLIANCE AND CONSEQUENCES OF NON-COMPLIANCE

6.1. The Company is committed to maintaining the highest standards of integrity and regulatory compliance. Compliance with this Policy is mandatory for all employees, agents, and relevant third parties.

6.2. Failure to comply with this policy may result in significant consequences, including but not limited to:

6.2.1. **Internal disciplinary action**, which may involve verbal or written warnings, suspension, or termination of employment or contract;

6.2.2. **Legal consequences**, including potential criminal or civil liability, regulatory fines, or prosecution under applicable anti-money laundering laws;

6.2.3. **Business risks**, such as reputational damage, regulatory sanctions, financial losses, or loss of licenses to operate.

7. RELATED INFORMATION

7.1. This Policy operates in conjunction with the Company's other governance documents, including but not limited to the Disaster Recovery Plan, Data Protection Policy, Player Complaints Policy, and Responsible Gaming Policy, to ensure comprehensive risk management and regulatory compliance.

7.2. All employees are required to familiarize themselves with and adhere to these policies. Any suspected or actual breaches must be reported immediately to the Compliance Officer.

7.3. The Board of Directors of the Company is aware of the stages of money laundering and is committed to taking all necessary preventative measures to combat, prevent, and detect money laundering. Prevention is ensured by implementing the following measures:

Document Classification: CONFIDENTIAL						
Name:	Anti-Money Laundering and Countering the Financing of Terrorism policy					
Maintainer:	MLRO	Approver:	Statutory Director			
Status:	In effect	Version:	5.0	Effective Date:	April 10, 2025	Page 39 of 44

- 7.3.1. Implementation of AML/CFT policies and procedures across the group of companies;
- 7.3.2. Clear communication of these policies and procedures to all staff;
- 7.3.3. Adoption of a risk-based approach;
- 7.3.4. Customer Risk Assessment (CRA) procedures;
- 7.3.5. Customer Acceptance Policy (CAP);
- 7.3.6. Internal controls;
- 7.3.7. Customer due diligence (CDD) procedures;
- 7.3.8. Record keeping and ongoing monitoring;
- 7.3.9. Internal reporting procedures;
- 7.3.10. Suspicious activity reporting (SAR);
- 7.3.11. Ongoing AML training and awareness for staff.

- 7.4.** The Company applies a risk-based approach to detect money laundering and terrorist financing (ML/TF), allowing for the prioritization of resources in higher-risk situations while maintaining compliance in lower-risk areas.
- 7.5.** The Company utilizes specialized software and internal operational measures to ensure compliance with applicable AML laws and to prevent Customers from engaging in illicit or suspicious activities.

8. CONTACT INFORMATION

- 8.1.** For any questions regarding this policy, please contact Sintija Zalane, Compliance Officer of BAMLA LIMITED N.V., at phone number: +371 29681682 or email: legal@baltent.com.

9. POLICY HISTORY

- 9.1.** This is an updated version of the Anti-Money Laundering and Countering the Financing of Terrorism (AML/CFT) Policy. It replaces all previous versions listed below:

Policy Title	Effective Date	Version
Anti-Money Laundering and Countering the Financing of Terrorism Policy	08.09.2023	1.0
Anti-Money Laundering and Countering the Financing of Terrorism Policy	16.10.2024	2.0
Anti-Money Laundering and Countering the Financing of Terrorism Policy	05.12.2024	3.0
Anti-Money Laundering and Countering the Financing of Terrorism Policy	05.03.2025	4.0

- 9.2.** This version reflects updates made to enhance compliance with current regulatory requirements and internal risk management practices.
- 9.3.** This Policy shall be reviewed at least on a yearly basis to determine if any updates and/or amendments are required. The frequency of such updates can be less should there be any regulatory change or change in the policies and procedures to be applied due to any change in the risks faced by the Company or due to any changes in the assessment of certain risk factors arising out of publications made by the FIU, FATF, National Risk-Assessments and/or supra-national Risk Assessments. It shall be the MLRO's responsibility to ensure that this document is reviewed and updated if and when required. Any updates and/or changes made to this document shall be presented to the board of directors who shall review and approved such changes. **Next Scheduled Review Date: April 04, 2026.**

10. POLICY URL

- 10.1.** The KYC and AML Policy is publicly accessible on the Company's website at <https://rioplay.com>, located further down the webpage under the sections: "Terms and Conditions"; "KYC"; and "AML".

Document Classification: CONFIDENTIAL						
Name:	Anti-Money Laundering and Countering the Financing of Terrorism policy					
Maintainer:	MLRO	Approver:	Statutory Director			
Status:	In effect	Version:	5.0	Effective Date:	April 10, 2025	Page 40 of 44

Annex A

Afghanistan	Russia
America Samoa	Saba
Aruba	Samoa
Australia	Saudi Arabia
Bonaire	Serbia
Curaçao	Singapore
Cyprus	Sri Lanka
Ethiopia	St. Eustatius
France	St. Maarten
Great Britain	Syria
Guam	Trinidad and Tobago
Guyana	Uganda
Iran	Ukraine
Iraq	United Kingdom
Israel	United States of America
Laos	Vanuatu
Latvia	Venezuela
Malta	Yemen
Netherlands	any other jurisdiction that the Central Government of Curacao (formerly the Netherlands Antilles) deems online gambling illegal.
North Korea	
Pakistan	
Palestine	

Document Classification: CONFIDENTIAL						
Name:	Anti-Money Laundering and Countering the Financing of Terrorism policy					
Maintainer:	MLRO	Approver:	Statutory Director			
Status:	In effect	Version:	5.0	Effective Date:	April 10, 2025	Page 41 of 44

Annex B

EXAMPLES OF SUSPICIOUS TRANSACTIONS/ACTIVITIES RELATED TO MONEY LAUNDERING AND TERRORIST FINANCING

A. MONEY LAUNDERING

Under the laws of multiple jurisdictions money laundering is a serious offence. Money laundering involves various acts committed with the intention to conceal or convert property or the proceeds derived from such property (such as money) knowing or believing that these were derived from the commission of a designated offence. In this context, a designated offence means an offence under the Criminal Law (Penal Code) of Curacao or any other applicable law or the equivalent law in the jurisdiction within which such offence has or is suspected to have taken place. It includes but is not limited to those offences relating to illegal drug trafficking, bribery, fraud, forgery, murder, robbery, counterfeit money, stock manipulation, tax evasion and copyright infringement amongst other.

Suspicious transactions are financial transactions that you have reasonable grounds to suspect are related to the commission of a money laundering offence. This includes transactions that you have reasonable grounds to suspect are related to the attempted commission of a money laundering offence.

Suspicious transactions also include financial transactions that you have reasonable grounds to suspect are related to the commission of a terrorist activity financing offence. This includes transactions that you have reasonable grounds to suspect are related to the attempted commission of a terrorist activity financing offence.

"Reasonable grounds to suspect" is determined by what is reasonable in your circumstances, including normal business practices and systems within the industry. While the Laws do not specifically require the Company to implement or use an automated system for detecting suspicious transactions, we do have such a system in place.

The Company's compliance regime includes an assessment in the course of our activities, of the risk of money laundering or terrorist financing. According to this assessment, in higher risk situations, we take reasonable measures to conduct ongoing monitoring for the purpose of detecting suspicious transactions.

Suspicious transactions in interactive gambling:

1. The Customer deposits funds into the game account and later requests a withdrawal, even though the game has not been played or has only been played for a small amount;
2. The Customer deposits funds into the game account and intentionally loses the funds to another Customer (accomplice) in the card game tournament, who may also be registered with another gambling operator, including a foreign gambling operator;
3. The Customer may use persons who bet against each other using criminally acquired funds, with the winner receiving the winnings, thereby laundering the criminally acquired funds;
4. A person buys interactive gambling or lottery accounts from their beneficial owners (for a price exceeding their monetary value);
5. The Customer regularly deposits money into their game account and withdraws it over time, without gambling;
6. The Customer keeps funds in the game account for a long period of time, does not gamble or gambles little and makes a withdrawal to the bank account;

Document Classification: CONFIDENTIAL						
Name:	Anti-Money Laundering and Countering the Financing of Terrorism policy					
Maintainer:	MLRO	Approver:	Statutory Director			
Status:	In effect	Version:	5.0	Effective Date:	April 10, 2025	Page 42 of 44

7. A Customer attempts to open multiple accounts using the credentials of the same person;
8. The registered card or bank account details do not match the Customer's registration details;
9. Payment to the game account is made by a third party;
10. The Customer is identified as being on the international sanctions list;
11. The Customer attempts to make a deposit using the company's bank card, paying particular attention to the company's bank cards that are linked to a public administration body or a municipality;
12. The Customer requests one or more cryptocurrency withdrawals from a gambling account within a single gaming day, forming a pattern or combination of transactions with a total amount equivalent to or exceeding 5000 in any cryptocurrency (e.g., USDT, USDC, EURT, etc.).
13. The Customer deposits uncharacteristically large sums into their Customer account for their playing habits and it is impossible to trace the origin of the funds;
14. Customer identification problems (Customer is unwilling to provide or provides minimal identification information, provides fictitious information, provides information that is difficult to verify, there is reasonable suspicion that the identity document is forged);
15. The Customer carries out a large number of small, identical transactions, suggesting a deliberate avoidance of the threshold declaration;
16. There are reasonable grounds to suspect that the Customer or the beneficial owner may be involved in terrorism, even though they are not on a terrorist list and have not previously been reported to the FIU ;
17. The Customer attempts to make contact with an employee or employees of Company (outside working hours);
18. The Customer logs into their interactive gambling or lottery account from a high-risk country;
19. A Customer logs into an interactive gambling or lottery account from multiple countries within a short period of time;
20. There are reasonable grounds to suspect that the transaction involved proceeds of crime;
21. The Customer makes a transaction that is not in line with his financial situation;
22. The Customer uses forged or inappropriate documents;
23. The Customer carries out atypical or fraudulent activities;
24. The Customers takes a defensive stance on the questions asked or makes too many excuses;
25. The Customer avoids the Customer's identification and due diligence measures required by law;
26. The Customer hides the amount of money deposited for gaming in order to make it more difficult to detect the total amount of transactions and cross-transactions;
27. The transaction is linked to another suspicious transaction already reported to the FIU;
28. The transaction has no apparent legitimate purpose;

Document Classification: CONFIDENTIAL						
Name:	Anti-Money Laundering and Countering the Financing of Terrorism policy					
Maintainer:	MLRO	Approver:	Statutory Director			
Status:	In effect	Version:	5.0	Effective Date:	April 10, 2025	Page 43 of 44

29. Suspicious transactions are reported by others (media, police, internal security, credit institutions).

Transactions related to terrorist property

If an employee and/or Company officer suspects that a transaction, whether completed or attempted, is related to terrorist financing, such person must raise a suspicious transaction report with the MLRO.

If such person has knowledge, rather than suspicion, that a transaction is related to funds owned or controlled by or on behalf of a terrorist or a terrorist group, then such transaction should be suspended. Accounts and/or any pending actions will be frozen or put on hold accordingly and a SAR/STR should be raised immediately.

1. Transactions with no discernible purpose or are unnecessarily complex.
2. Use of foreign accounts of companies or group of companies with complicated ownership structure which is not justified based on the needs and economic profile of the Customer.
3. The transactions or the size of the transactions requested by the Customer do not comply with his usual practice and play activity.
4. Large volume of transactions and/or money deposited or credited into, an account when the nature of the Customer's business activities or sources of income would not appear to justify such activity.
5. There is no visible justification for a Customer using the services of a particular organization. For example, the Customer is situated far away from the particular organization and in a place where he could be provided services by another organization.
6. There are frequent transactions in the same Company without obvious reason and in conditions that appear unusual (churning).
7. There are frequent purchases of services by a Customer who settles in cash or transferring amounts, mainly large, with the Customer's instructions, in an account other than the usual account used for the services rendered.
8. Any service requested the nature, size or frequency appear to be unusual, e.g. cancellation of an order, particularly after the setting of the instruction.
9. The settlement of any transaction but mainly large transactions, in cash or cash equivalents.
10. Settlement of the transaction by a third person which is different than the Customer which gave the order, other than in the case of an approved intermediary.
11. Instructions of transferring payment to a third person that does not seem to be related with the instructor.
12. Transfer of funds to and from countries or geographical areas which do not apply or they apply inadequately FATF's recommendations on Money Laundering and Terrorist Financing.
13. A Customer is reluctant to provide complete information when establishing a Business Relationship about the nature and purpose of the intended business activities, anticipated accounts activities, does not disclose his source of wealth or support it adequately with documentation. The Customer usually provides minimum or misleading information that is difficult or expensive for the Company to verify.

Document Classification: CONFIDENTIAL						
Name:	Anti-Money Laundering and Countering the Financing of Terrorism policy					
Maintainer:	MLRO	Approver:	Statutory Director			
Status:	In effect	Version:	5.0	Effective Date:	April 10, 2025	Page 44 of 44

14. A Customer provides unusual or suspicious identification documents that cannot be readily verified.
15. A Customer's home/business telephone is disconnected.
16. A Customer that makes frequent or large transactions into their accounts and has no record of past or present employment or income.
17. Difficulties or delays on the submission of the financial statements or other identification documents, of a Customer.
18. A Customer who has been introduced by a by a third person whose countries or geographical areas of origin do not apply, or they apply inadequately FATF's recommendations on Money Laundering and Terrorist Financing.
19. Shared address for individuals involved in transactions with cash, or other payment methods which make it easy to disguise ownership of funds (prepaid cards, cash vouchers), particularly when the address is also a business location and/or does not seem to correspond to the stated occupation (e.g. student, unemployed, self-employed, etc.).
20. The stated occupation of the Customer is not commensurate with the level or size of the executed transactions.
21. Unexplained inconsistencies arising during the process of identifying and verifying the Customer (e.g. previous or current country of residence, country of issue of the passport, countries visited according to the passport, documents furnished to confirm name, address and date of birth, etc).