

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

30 May 2025

Re: Uploading AML/CFT Policy

Dear Mr. Pietersz,

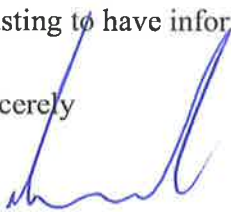
In order to comply with the due date for submission of the AML/CFT Policy, the applicant hereby uploads the draft version of the AML/CFT policy.

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

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

Trusting to have informed you accordingly.

Sincerely



Raoul Behr
Managing Director

ORANGE ENTERTAINMENT B.V.

ANTI-MONEY LAUNDERING AND COUNTER-

TERRORIST FINANCING POLICY

*(Adopted in accordance with the Curaçao AML/CFT regulatory
framework)*

Content

<u>I.</u>	<u>POLICY STATEMENT.....</u>	<u>3</u>
<u>II.</u>	<u>PURPOSE</u>	<u>3</u>
<u>III.</u>	<u>AUDIENCE</u>	<u>3</u>
<u>IV.</u>	<u>DEFINITIONS.....</u>	<u>3</u>
<u>V.</u>	<u>POLICY IMPLEMENTATION.....</u>	<u>4</u>
5.1	BUSINESS RISK ASSESSMENT (BRA)	4
5.2	CUSTOMER RISK ASSESSMENT (CRA)	5
5.3	CUSTOMER ACCEPTANCE POLICY (CAP)	6
5.4	CUSTOMER DUE DILIGENCE	7
5.5	ENHANCED DUE DILIGENCE (EDD).....	8
<u>VI.</u>	<u>ONGOING MONITORING</u>	<u>9</u>
<u>VII.</u>	<u>RELIANCE ON THIRD PARTIES TO PERFORM CUSTOMER DUE DILIGENCE</u>	<u>10</u>
<u>VIII.</u>	<u>REPORTING OF UNUSUAL TRANSACTIONS.....</u>	<u>11</u>
<u>IX.</u>	<u>ANTI-MONEY LAUNDERING COMPLIANCE PROGRAM</u>	<u>12</u>
<u>X.</u>	<u>COMPLIANCE AND CONSEQUENCES OF NON-COMPLIANCE.....</u>	<u>13</u>
<u>XI.</u>	<u>CONTACT INFORMATION.....</u>	<u>14</u>

I. POLICY STATEMENT

Orange Entertainment B.V. (“the Company”), is committed to preventing its operations from being used for money laundering, the financing of terrorism, or the proliferation of weapons of mass destruction. This Anti-Money Laundering Policy establishes the principles, requirements, and procedures the Company applies to detect, prevent, and report such activities. This Policy applies to all employees, contractors, and associated entities involved in the provision of gaming services under the Company’s license.

II. PURPOSE

This Policy is adopted to ensure compliance with the requirements set by the Curaçao Gaming Control Board, including the National Ordinance on Identification when Rendering Services, the National Ordinance on the Reporting of Unusual Transactions, and applicable international standards (e.g., FATF Recommendations). The objective is to establish a risk-based AML/CFT framework that includes internal controls, risk assessments, due diligence procedures, and reporting mechanisms to mitigate exposure to financial crime.

III. AUDIENCE

This Policy is mandatory for:

- All employees of the Company, including permanent and temporary staff;
- Members of senior management and the Board of Directors;
- The appointed Compliance Officer and all personnel involved in AML/CFT functions;
- Contractors, agents, or third parties acting on behalf of the Company who are involved in player onboarding, payment processing, or other activities subject to AML obligations.

IV. DEFINITIONS

The following terms are used throughout this Policy and have the meanings set out below:

- **Money Laundering (ML):** The process of concealing the illicit origin of funds, typically by introducing them into the financial system in a way that makes them appear legitimate. It consists of three stages: placement, layering, and integration.
- **Terrorist Financing (TF):** The provision or collection of funds, directly or indirectly, with the intention that they be used to support terrorist acts, terrorist organizations, or individual terrorists, regardless of whether the funds are of legitimate or illegitimate origin.
- **Proliferation Financing (PF):** The act of providing funds or financial services used for the development, acquisition, or transfer of nuclear, chemical, or biological weapons and their delivery systems, in violation of international obligations.
- **Customer Due Diligence (CDD):** The process of identifying and verifying the identity of customers, understanding the purpose and nature of the business relationship, and conducting ongoing monitoring to ensure consistency with the customer’s profile and risk level.
- **Enhanced Due Diligence (EDD):** Additional verification and scrutiny measures applied in situations of higher money laundering or terrorist financing risk, such as when dealing with PEPs or customers from high-risk jurisdictions.
- **Politically Exposed Person (PEP):** An individual who holds or has held a prominent public function, including their immediate family members and close associates, who may pose a higher risk of involvement in bribery or corruption.

- **Sanctions Screening:** The process of checking customers and transactions against international and national sanctions lists (e.g., UN, EU, local Curaçao lists) to ensure that the Company does not engage in prohibited relationships.
- **Beneficial Owner:** A natural person who ultimately owns or controls a customer or the person on whose behalf a transaction is being conducted. In legal entities, this typically includes individuals with 25% or more ownership or control.
- **Unusual Transaction Report (UTR):** A report submitted to the Curaçao Financial Intelligence Unit (FIU) in cases where a transaction is deemed suspicious or unusual based on objective or subjective indicators.
- **Risk-Based Approach (RBA):** A strategic approach whereby resources, controls, and procedures are tailored to the level of risk presented by a customer, product, service, or transaction.

V. POLICY IMPLEMENTATION

5.1 Business Risk Assessment (BRA)

The Company conducts a documented Business Risk Assessment to identify, evaluate, and mitigate the risks of money laundering, terrorist financing, and proliferation financing to which it is exposed through its operations. This assessment forms the foundation of the Company's risk-based approach and informs the design of internal policies, procedures, and controls.

The BRA considers the specific ways in which the Company's products, services, and distribution channels may be exploited for illicit purposes, and assesses the extent and likelihood of such misuse occurring. It also takes into account the following key risk factors:

- **Customer risk** — including types of customers and their potential for ML/TF activity.
- **Product and service risk** — such as products that offer higher anonymity or liquidity.
- **Delivery channel risk** — including non-face-to-face interactions and third-party intermediaries.
- **Geographical risk** — based on the jurisdictions involved in customer relationships or transactions, particularly high-risk or sanctioned countries.
- **National Risk Assessment (NRA) outcomes** — all relevant recommendations and findings from the NRA are incorporated into the BRA.

The Company defines its risk appetite and sets appropriate mitigation strategies, including enhanced controls for higher-risk areas. The BRA is reviewed and updated at least annually or upon any material change to the business environment, such as:

- Introduction of new products or payment methods;
- Expansion into new markets or jurisdictions;
- Implementation of new technologies or business models;
- Changes to applicable legislation or regulatory requirements.

The Business Risk Assessment is a documented process, approved by the Board of Directors, maintained by the Compliance Department, and made available to the Curaçao Gaming Control Board upon request.

Each BRA includes:

- The methodology used to assess risk;
- Justifications for risk classifications (low, medium, or high);
- The final outcomes and conclusions of the risk assessment;
- References to all internal and external data sources used.

5.2 Customer Risk Assessment (CRA)

The Company conducts a Customer Risk Assessment for each player during the onboarding process or prior to carrying out an occasional transaction. The purpose of this assessment is to identify the specific money laundering, terrorist financing, or proliferation financing risks associated with each customer and to assign an appropriate risk rating (low, medium, or high) that determines the level of Customer Due Diligence to be applied.

The Customer Risk Assessment is based on the following key risk factors:

Customer Risk

This includes analysis of the player's source of income, financial behavior, and any red flags such as:

- Use of multiple sources of income;
- Irregular or unverifiable income streams;
- High or disproportionate spending behavior;
- Use of third parties or agents to conduct transactions;
- PEP status;
- Use of multiple accounts to obscure transaction patterns;
- Redemption of large amounts without gameplay.

Geographical Risk

Based on the country of residence, nationality, and the origin of funds.

High-risk countries include:

- Jurisdictions with strategic AML/CFT deficiencies (as identified by FATF, CFATF, OFAC, etc.);
- Countries subject to international sanctions;
- Countries with high levels of corruption or terrorism activity;
- Countries appearing on the Corruption Perception Index or InCSR reports.

Product, Service, and Transaction Risk

Assesses the vulnerability of specific gaming products or services and payment channels to misuse, such as:

- Acceptance of high-risk payment methods (pre-paid cards, crypto, e-wallets);
- Peer-to-peer gaming;
- Use of casino accounts for deposit/withdrawal without real gambling;
- Transfers between gaming accounts;
- Access to multiple casino sites using the same backend.

Distribution Channel Risk

Assesses how the customer interacts with the casino.

Higher risk is attributed to:

- Non-face-to-face onboarding (unless mitigated with secure tech);
- Third-party intermediaries without AML oversight;
- Anonymous channels or remote operations.

Each customer's risk profile is dynamically maintained and is reassessed when significant changes occur (e.g. unusual transaction patterns, change in PEP/sanctions status, or updated source of funds).

The CRA outcome directly informs the applicable CDD measures under the Customer Acceptance Policy. The CRA, its underlying methodology, and customer risk profiles are documented and maintained by the Compliance Department and are subject to regular audit and regulatory review.

5.3 Customer Acceptance Policy (CAP)

The Customer Acceptance Policy defines the Company's rules, thresholds, and procedures for accepting and maintaining business relationships with players. It ensures that customers are only accepted when the ML/TF/PF risk is clearly understood, appropriately assessed, and mitigated through effective CDD measures.

The CAP is implemented in conjunction with the Customer Risk Assessment and incorporates the following core elements:

a) Risk-Based Acceptance Criteria

The Company only establishes business relationships with customers whose risk profiles fall within the Company's defined risk appetite.

The CAP outlines:

- The types of players likely to pose higher-than-average ML/TF/PF risk (e.g. PEPs, high-risk jurisdictions, disproportionate spenders);
- The indicators used to categorize customers as low, medium, or high risk;
- The CDD obligations per risk level, including ongoing monitoring frequency;
- Specific triggers for requiring enhanced due diligence.

b) Sanctions and PEP Screening

All customers are screened against the UN and EU consolidated sanctions lists, local sanctions published by the Curaçao authorities, as well as PEP databases and reputable sources such as Transparency International.

If a customer is identified as a PEP or is subject to sanctions, the relationship may only proceed upon:

- Senior management approval;
- Independent verification of source of funds and source of wealth;
- Application of enhanced monitoring throughout the relationship.

c) Grounds for Declining or Terminating the Relationship

The CAP includes specific conditions under which a customer must be declined or offboarded:

- 1) Inability or refusal to complete CDD within the required timeframe;
- 2) Submission of fraudulent or unverifiable documentation;
- 3) Confirmed or suspected links to sanctioned entities or terrorist financing;
- 4) Any suspicion of criminal activity, money laundering, or third-party proxy use.

d) Documentation and Governance

The Customer Acceptance Policy is reviewed and approved by the Board of Directors, enforced under the direct oversight of the Compliance Officer, and all decisions to decline or terminate a customer relationship under the CAP are documented with clear reasoning and supporting data; the CAP is reviewed annually or upon the emergence of new risk indicators, products, jurisdictions, or regulatory changes.

5.4 Customer Due diligence

The Company implements a robust, risk-based Customer Due Diligence process designed to identify and verify the identity of every customer, understand the nature and purpose of the relationship, and monitor the account and transactions to detect and prevent money laundering, terrorist financing, or proliferation financing activities.

Triggers for CDD

CDD measures are applied in the following situations:

- When a player engages in financial transactions equal to or above NAf. 4,000;
- When an occasional transaction exceeds the NAf. 4,000 threshold (individually or as a series of linked transactions);
- When there is suspicion of money laundering or terrorist financing;
- When there are doubts about the accuracy or adequacy of previously obtained customer information.

CDD Measures

The Company's CDD process includes the following key components:

a) Identification and Verification of the Customer

- Mandatory collection of the customer's full name, permanent residential address, date and place of birth, nationality, and identity number.
- Verification through valid, unexpired government-issued documents containing photographic evidence (e.g., passport, national ID).
- Verification of residential address, where required, through secondary documentation such as utility bills or bank statements (not older than six months).
- Where necessary, additional verification methods are used: biometric validation, video verification, cross-checks with geo-location/IP data, and device fingerprinting.

b) Customer Risk Assessment

A Customer Risk Assessment is conducted at onboarding to assign a preliminary risk rating based on the customer's characteristics, transactional behavior, geographical indicators, and product or channel risk; this risk profile determines the appropriate level of Customer Due Diligence and informs the frequency and intensity of ongoing monitoring.

c) Understanding the Purpose and Intended Nature of the Relationship

Although the purpose of opening a gaming account may appear self-evident, the Company collects sufficient information to understand the expected activity and funding pattern; in low-risk cases, a declaration of source of wealth may suffice, while high-risk scenarios require supporting documentary evidence, and statistical or behavioral modelling may be applied for ongoing profiling across broader customer segments where appropriate.

d) Sanctions and PEP Screening

All customers are screened prior to onboarding and on an ongoing basis against:

- UN and EU Consolidated Sanctions Lists;
- Any national lists published by the Curaçao authorities;
- Reliable databases (e.g. KnowYourCountry, Transparency International);

Customers identified as PEPs—whether foreign or domestic—require senior management approval to establish or maintain the relationship, verification of their source of wealth and source of funds, as well as the application of enhanced due diligence and ongoing monitoring.

Freezing of Funds and Reporting

Where a customer reaches the NAf. 4,000 threshold but fails to provide required documentation within 30 days:

1. The customer's account is suspended;
2. No further deposits or withdrawals may occur;
3. Funds are returned to the source account unless there is suspicion of ML/TF;
4. If ML/TF is suspected, the transaction is reported to the FIU Curaçao and, where warranted, escalated to the Public Prosecutor's Office.

If completing the CDD process would likely “tip off” the customer of a pending Unusual Transaction Report (UTR), the Company may suspend the process and instead file the report with the FIU without further customer interaction.

5.5 Enhanced Due Diligence (EDD)

The Company applies Enhanced Due Diligence measures in situations where the risk of money laundering, terrorist financing, or proliferation financing is assessed to be higher. EDD involves more intensive scrutiny and verification procedures and is a core component of the Company's risk-based approach to customer due diligence.

EDD is applied in the following situations, among others:

- The customer is a Politically Exposed Person (PEP) or a close associate/family member of a PEP;
- The customer resides in or is associated with high-risk geographic areas;
- The customer uses products or payment methods that favor anonymity;
- The relationship involves new delivery channels, business models, or the use of new or developing technologies.

EDD Measures

Where EDD is required, the Company applies one or more of the following enhanced controls, as appropriate to the level and nature of the risk identified:

- Obtain additional information about the customer (e.g., occupation, previous address, adverse media, public sources);
- Obtain additional information on the intended nature and purpose of the business relationship;
- Obtain documented evidence of source of funds and source of wealth (e.g., employment income, inheritance, property sale, gambling winnings);

- Obtain justification for intended or actual transactions, particularly where deviations from expected behavior are observed;
- Require senior management approval to initiate or continue the relationship;
- Conduct enhanced monitoring of the customer’s account activity and transaction history;
- Require that the first deposit be made from an account in the customer’s name held at a financial institution that applies equivalent CDD standards.

EDD measures are proportionate to the risk and documented in the customer file. The Compliance Officer is responsible for determining when EDD is required and ensuring that the enhanced procedures are properly applied and recorded.

Ongoing EDD Obligations

In cases presenting higher ML/TF risk, the Company may require source of funds documentation to be re-validated periodically, even if there is no change in the customer’s transactional pattern.

EDD is not a one-time procedure. Where higher risk persists, the Company continues to apply enhanced monitoring and controls for the duration of the relationship.

VI. ONGOING MONITORING

The Company performs ongoing monitoring of both customer identity and transactional behavior throughout the duration of the business relationship. This process ensures that the relationship remains consistent with the customer’s known profile and enables timely detection of potentially suspicious activity that may indicate money laundering, terrorist financing, or proliferation financing risks.

Ongoing monitoring is conducted on a risk-sensitive basis and includes two key components:

1. Ongoing Monitoring of Identity

The Company maintains accurate, up-to-date identification records for all active customers. Recognizing that certain personal details may change over time (e.g. address, payment method, identity document expiry), the Company:

- Periodically reviews and refreshes customer data;
- Verifies updated identification documents where changes are material;
- Tracks expiry dates of identity evidence and prompts re-verification;
- Reassesses the customer’s risk profile when identification changes are significant.

These measures ensure that any deviations or discrepancies in customer identity are identified promptly, re-documented, and evaluated for risk implications.

2. Ongoing Monitoring of Transactions

Transactional monitoring is conducted continuously to detect behavior inconsistent with the customer’s expected or previously observed activity. If the customer’s transactions diverge from their risk profile, the Company investigates the anomaly by:

- Reviewing the customer’s source of funds and transaction purpose;

- Comparing behavior to typical account activity and established customer profiles;
- Requesting supporting documentation for unusual or unexplained transactions.

Deviations may include large transactions inconsistent with declared income, use of new payment instruments without explanation, or a sudden change in betting behavior.

In such cases, the Company may:

- Revise the customer's risk rating;
- Apply enhanced due diligence measures;
- Determine whether the transaction qualifies as unusual and file a report with the Financial Intelligence Unit (FIU) Curaçao.

Monitoring Frequency and Risk Sensitivity

The intensity and frequency of ongoing monitoring are determined based on the customer's risk category (low, medium, or high). However, even in low-risk scenarios, the Company ensures a baseline level of oversight is maintained to confirm that the business relationship remains within acceptable risk thresholds.

VII. RELIANCE ON THIRD PARTIES TO PERFORM CUSTOMER DUE DILIGENCE

The Company relies on selected third parties to perform specific elements of the Customer Due Diligence process, including customer identification, identity verification, and understanding the purpose and intended nature of the business relationship. This reliance is implemented in full compliance with Curaçao AML/CFT regulations and is subject to strict internal control and oversight.

The third parties involved maintain an existing, independent business relationship with the customer and are subject to equivalent AML/CFT and record-keeping obligations. The Company retains full responsibility for the effectiveness and regulatory compliance of the overall CDD framework.

To ensure compliance, the following conditions are consistently fulfilled:

• Immediate Access to CDD Data

The Company receives the required CDD data and supporting documentation from the third party immediately upon reliance. This includes verified identity information and the purpose of the relationship, ensuring no operational delay or data deficiency.

• Written Agreements and Document Availability

The Company maintains formal agreements with each relied-upon party, guaranteeing access to underlying CDD documentation upon request. These arrangements are regularly tested to confirm that data provision, quality, and timing meet the agreed standards.

• Regulatory Oversight of the Third Party

The Company only relies on third parties that are subject to supervision or monitoring in accordance with international AML/CFT standards. Each third party has demonstrated sufficient policies, internal controls, and independent compliance frameworks aligned with Curaçao requirements.

• Country Risk Assessment

The Company takes into account the jurisdiction in which the third party operates, using publicly available country risk sources to validate that the regulatory environment supports reliable CDD performance.

The Company does not delegate the responsibility to conduct customer-specific risk assessments, determine PEP or sanctions exposure, or carry out ongoing monitoring. These remain fully under the Company's control.

VIII. REPORTING OF UNUSUAL TRANSACTIONS

The Company maintains a structured and risk-based procedure for recognizing, documenting, and reporting unusual transactions in full compliance with the National Ordinance on the Reporting of Unusual Transactions and applicable FATF Recommendations. This procedure ensures timely internal detection, proper documentation, and external reporting to the Curaçao Financial Intelligence Unit.

Recognition of Unusual Transactions

The Company identifies unusual transactions by continuously comparing player activity against the customer's established risk profile. An unusual transaction is defined as any transaction or pattern of transactions that is inconsistent with the player's known behavior, business, or source of funds.

This includes:

- Transactions that have no apparent economic or lawful purpose;
- Sudden deviations from historical spending or gameplay patterns;
- Use of funds or payment methods inconsistent with the player's declared profile.

Objective and subjective indicators of unusual transactions, as defined in the Ministerial Decree and NORUT, are integrated into the Company's detection systems and staff training programs.

Types of Unusual Transactions Identified

The Company considers the following to be unusual and subject to reporting:

1. Transactions related to suspected money laundering or terrorist financing;
2. Transactions by or on behalf of persons or entities listed under the Sanctions National Ordinance (N.G. 2014 no. 55);
3. Transactions of NAf. 5,000 or more (or the equivalent), regardless of payment method or medium (e.g., cash, chips, e-wallets);
4. Cashless transfers, deposits, chip sales, or cash-outs of NAf. 5,000 or more;
5. Linked transactions that together meet the NAf. 5,000 threshold in a single gaming day;
6. Transactions with no visible legal justification or that significantly exceed normal activity.

Internal Documentation and Compliance Review

All identified unusual transactions are reported internally to the Compliance Officer using the approved format. Supporting documentation (e.g., identification documents, payment confirmations, correspondence) is submitted with the report. Internally logged transactions not reported to the FIU are still documented with clear justification and approved by the Compliance Officer or senior management.

The Compliance Officer maintains a secure, auditable record of all reported and non-reported cases.

External Reporting Process to FIU Curaçao

The Company is registered with the Curaçao FIU and reports unusual transactions through the goAML online portal. The Compliance Officer submits the report, in English, along with supporting documents. Reporting occurs without delay following the identification of the unusual transaction or intended transaction.

All reports are submitted in accordance with Article 11 of the NORUT and the relevant FIU reporting regulations.

Prohibition of Disclosure

The Company, its management, and all personnel are strictly prohibited from informing the customer or any third party about the reporting of a transaction to the FIU. No information concerning the existence, status, or content of a report is disclosed, as this may compromise regulatory investigations or create tipping-off risks.

In high-risk cases, instead of blocking an account or terminating the relationship prematurely, the Company prioritizes increased monitoring and, where needed, continues filing reports.

IX. ANTI-MONEY LAUNDERING COMPLIANCE PROGRAM

The Company maintains a comprehensive Anti-Money Laundering Compliance Program designed to mitigate the risks of money laundering, terrorist financing, and the financing of proliferation.

The program establishes minimum standards and internal controls that ensure compliance across all business units, jurisdictions, and distribution channels. It is reviewed regularly to remain responsive to emerging risks, new regulatory developments, and internal audit findings. The AML Program is approved by senior management and applies to the entire organization, including any branches or group companies involved in onboarding or transaction handling.

Core Components of the AML Compliance Program

The AML Program consists of the following integrated elements:

- 1. Internal Policies, Procedures, and Controls**

The Company implements written AML/CFT policies and operational procedures that define its approach to customer due diligence, reporting of unusual transactions, record-keeping, sanctions compliance, and employee conduct. These policies are approved by senior management and clearly communicate the Company's zero-tolerance stance on financial crime.

- 2. Appointment of a Designated Compliance Officer**

A senior-level Compliance Officer, acting independently from operations, oversees the AML Program. The Officer is responsible for program design, implementation, staff training, internal investigations, review of reported transactions, and reporting to the FIU via goAML. The Officer has unrestricted access to CDD records and is supported by a compliance team.

- 3. Employee Screening and Training**

The Company screens all relevant staff for integrity risks and provides mandatory AML training tailored to employee roles. New employees are trained on AML basics and reporting obligations, while key functions (dealers, cashiers, supervisors, compliance and audit teams, senior management) receive role-specific education. Training records are maintained and refresher sessions are held at regular intervals.

- 4. Independent Audit Function**

The AML Program is audited annually by an independent internal audit team or an external firm not involved in day-to-day compliance operations. The audit includes review of manuals, transaction testing, staff interviews, and assessment of detection capability. Audit findings are escalated to senior management with recommendations and follow-up timelines.

Ongoing Risk-Based Management

The AML Program is structured around the Company's Business Risk Assessment and Customer Risk Assessment. Risk scoring and mitigation measures are applied at customer onboarding, during transactional activity, and through ongoing monitoring. High-risk areas receive increased scrutiny, and the program adapts to new threats such as emerging products, anonymous payment methods, and remote onboarding.

X. COMPLIANCE AND CONSEQUENCES OF NON-COMPLIANCE

The Company enforces full compliance with its Anti-Money Laundering, Counter-Terrorist Financing and Counter-Proliferation Financing policies and procedures as a critical part of its regulatory obligations and operational integrity. Adherence to this Policy is mandatory for all employees, officers, agents, contractors, and any other parties acting on behalf of the Company.

Compliance with this AML Policy ensures that the Company:

- Maintains its good standing under the applicable laws of Curaçao;
- Meets licensing conditions established by the Curaçao Gaming Control Board;
- Upholds its reputation as a responsible and law-abiding gaming operator;
- Mitigates exposure to financial, regulatory, and criminal risks.

Obligations of Staff and Management

All personnel are required to:

- Understand and follow the internal AML/CFT policies and procedures;
- Complete mandatory AML training relevant to their role;
- Promptly report any suspicious or unusual activity to the Compliance Officer;
- Cooperate fully with internal reviews, audits, or external regulatory inquiries;
- Preserve the confidentiality of any investigation or report made to the FIU.

Management is responsible for setting a culture of compliance, allocating sufficient resources to the AML function, and leading by example in the implementation of risk-based controls.

Consequences of Non-Compliance

Any breach of this AML Policy, whether through negligence, willful misconduct, or failure to act, may result in serious consequences for both the individual and the Company. These include, but are not limited to:

• Internal Disciplinary Action

Employees found to be in breach of AML requirements may face disciplinary action up to and including termination of employment. Contractors or agents may have their engagement suspended or terminated.

• Regulatory Sanctions

Non-compliance may lead to enforcement action by the GCB, including administrative penalties, license suspension or revocation, special monitoring conditions, and public reprimand.

• Civil and Criminal Liability

Individuals or the Company may be subject to criminal prosecution, civil fines, and imprisonment for knowingly or negligently facilitating money laundering, terrorist financing, or failure to report unusual transactions as required by law.

• Reputational Damage and Business Risk

AML failures may result in loss of customer trust, banking and payment processing restrictions, inability to expand into new markets, and long-term harm to the Company's commercial position and brand value.

Monitoring and Enforcement

The Company enforces compliance through:

- Ongoing internal monitoring and audit reviews;
- Periodic reviews of employee adherence to AML responsibilities;
- Root cause analysis of any detected deficiencies;
- Prompt corrective actions and reporting to senior management.

All staff are reminded that full cooperation with AML/CFT procedures is a condition of employment or engagement, and that failure to comply is treated as a material breach of duty.

XI. CONTACT INFORMATION

For any questions, clarifications, or further information regarding this Anti-Money Laundering Policy, please contact:

Paweł Pietak

Money Laundering Reporting Officer (MLRO)

mlro@lemon.casino

DOCUMENT CREATION				
Version		4		
Date Created		April 5, 2025		
Author(s) of Document		Paweł Piętak, MLRO		
Purpose of Document		This Policy defines the framework by which the Company conducts its operations and procedures to prevent Money Laundering, Fraud, and the Financing of Terrorism and Proliferation. It sets out the minimum standards applicable across all business lines and jurisdictions in which the Company operates. Where local or country-level AML/CFT laws impose more stringent requirements, those shall apply in addition to the standards established in this Policy.		
Authorised By		Paweł Piętak, MLRO		
CHANGE CONTROL				
Version	Date of Issue	Author(s)	Brief Description of Changes	Approved By
1.0	1 December, 2022	Paweł Piętak	Initial release	Paweł Piętak

2.0	1 January, 2023	Paweł Pięta	Updated document as per procedures changes	Paweł Pięta
2.1	31 May, 2023	Paweł Pięta	Restricted territories list update	Paweł Pięta
2.2	5 February, 2024	Paweł Pięta	Restricted territories list update - list moved to a separate Annex 1 document.	Paweł Pięta
3	1 August, 2024	Paweł Pięta	Updated document due to significant changes to Curaçao legislation.	Paweł Pięta
4	5 April, 2025	Paweł Pięta	Fully updated AML Policy to reflect the new regulatory framework introduced by the Curaçao Gaming Control Board in April 2025.	Paweł Pięta

Paweł Pięta