

ANTI-MONEY LAUNDERING, COUNTER-
TERRORISM FINANCING, AND COUNTER-
PROLIFERATION FINANCING
(AML, CTF AND CPF) POLICY

CONFIDENTIAL

Table of Contents

1	COMPLIANCE STATEMENT	5
2	PURPOSE	5
3	DEFINITIONS	6
4	POLICY IMPLEMENTATION	8
4.1	RESPONSIBILITY OF THE SENIOR MANAGEMENT	8
4.2	COMPLIANCE OFFICER	9
4.3	EMPLOYEES	9
	<i>Staff Reliability and Probity</i>	<i>9</i>
	<i>Professional Support and Training</i>	<i>9</i>
5	THE RISK-BASED APPROACH	9
5.1	EXPLANATION OF THE RISK-BASED APPROACH	9
5.2	BUSINESS RISK ASSESSMENT	10
5.3	TECHNOLOGICAL RISK ASSESSMENT	10
6	CUSTOMER ACCEPTANCE POLICY	11
6.1	CUSTOMER RISK ASSESSMENT	11
6.1.1	<i>Customer Risk</i>	<i>11</i>
6.1.2	<i>Product/Service Risk:</i>	<i>12</i>
6.1.3	<i>Geographic Risk:</i>	<i>12</i>
6.1.4	<i>Delivery Channel Risk:</i>	<i>13</i>
6.1.5	<i>Prohibited Accounts</i>	<i>13</i>
6.2	POLITICALLY EXPOSED PERSONS (PEPs)	13
6.3	SANCTIONS SCREENING	14
7	CUSTOMER DUE DILIGENCE MEASURES	14
7.1	CUSTOMER ONBOARDING AND IDENTIFICATION	15
7.2	VERIFICATION OF BENEFICIAL OWNERSHIP	15
7.3	CUSTOMER RISK ASSESSMENT AND PURPOSE OF RELATIONSHIP	16
7.4	7.4 SIMPLIFIED DUE DILIGENCE (SDD)	16
7.5	CUSTOMER DUE DILIGENCE (CDD)	17
7.6	TIMELINE FOR COMPLIANCE AND NON-COMPLIANT DOCUMENTS	17
7.7	ENHANCED DUE DILIGENCE	18
7.8	ONGOING MONITORING	19
7.8.1	<i>Ongoing Customer Profile Monitoring</i>	<i>19</i>
7.8.2	<i>Ongoing Transaction Monitoring</i>	<i>19</i>
7.9	RELIANCE ON THIRD PARTIES TO PERFORM DUE DILIGENCE	19
8	BUSINESS AFFILIATE AND SUPPLIER DILIGENCE	20
9	REPORTING UNUSUAL TRANSACTIONS	20
9.1	REPORTING OBLIGATIONS	20
9.2	RECOGNITION OF UNUSUAL TRANSACTIONS	21
9.3	PROHIBITION OF DISCLOSURE	22
9.4	RECORD KEEPING	22
10	ANTI-MONEY LAUNDERING COMPLIANCE PROGRAM	23

10.1	APPOINTMENT OF A MONEY LAUNDERING COMPLIANCE OFFICER	23
10.1.1	<i>Duties of the Compliance Officer</i>	23
10.2	EMPLOYEE SCREENING AND TRAINING PROGRAMS.....	24
10.2.1	<i>Employee Due Diligence</i>	24
10.2.2	<i>Training</i>	25
10.3	INDEPENDENT AUDIT FUNCTION	25
10.4	EXAMINATION BY THE CURAÇAO GAMING AUTHORITY	26
11	COMPLIANCE AND CONSEQUENCES OF NON-COMPLIANCE	26
12	APPENDIX I: COUNTRY RISK LIST	28
13	APPENDIX II: INTERNAL UNUSUAL ACTIVITY REPORT	29

CONFIDENTIAL

Document Information

Subject	Anti-Money Laundering, Counter-Terrorism Financing, and Counter-Proliferation Financing (AML, CTF and CPF) Policy
Audience	All Departments
Responsibility	Money Laundering Reporting Officer
Approval	Managing Director
Review	Annually or As Needed
Classification	Company Confidential

Version History

Date	Ver.	Author	Summary Changes	Approved by Management
December 2024	2.0	Arbol Media B.V.	Document created as part of AML Program review	
December 2025	3.0	Arbol Media B.V.	Updates in line with CGA AML Regulations	

1 Compliance Statement

Arbol Media B.V. (the Company), being established in and governed by the laws of Curaçao, is committed to implementing robust policies to prevent money laundering (ML), terrorism financing (TF), and proliferation financing (PF). In light thereof, the Company has developed a comprehensive Anti-Money Laundering, Counter Terrorism Financing and Counter Proliferation Financing (AML, CTF AND CPF) policy. Adherence to this Policy is obligatory and vital for guaranteeing that the Company remains in full compliance with relevant laws and regulations pertaining to AML, CTF AND CPF. As a responsible gaming enterprise operating in Curaçao, we acknowledge the paramount importance of upholding the integrity of our financial systems and preventing the exploitation of our operations for unlawful activities. Our commitment to compliance transcends mere legal requirements; it is a core component of our corporate responsibility and ethical principles.

2 Purpose

The local authorities in charge of the supervision of AML/CFT/CPF matters for the gaming sector are the Curaçao Gaming Control Board (GCB) and the Curaçao Financial Intelligence Unit (FIU). The purpose of this Policy is to ensure the Company's compliance with the relevant legal and regulatory requirements from the authorities in charge of the supervision of AML, CTF and CPF matters for the gaming sector, while simultaneously ensuring the integrity and sustainability of the operations of the Company.

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

- The Code of Criminal Law (Penal Code) (N.G. 2011, no. 48);
- The National Ordinance on Identification of Customers when Rendering Services (NOIS) (N.G. 2017, no. 92), last update June 2024;
- The National Ordinance on the Reporting of Unusual Transactions (NORUT) (N.G. 2017, no. 99), last update June 2024;
- Ministerial Decree with general operation of November 11, 2015, laying down the indicators, as mentioned in article 10 of the National Ordinance on the Reporting of Unusual Transactions (Regulation Indicators Unusual Transactions) (N.G. 2015, no. 73);
- National Decree penalties and fines reporting unusual transactions (N.G. 2021, no. 69) as amended by PB 2023, no. 6.;
- Sanctions National Ordinance (N.G. 2014, no. 55);
- Kingdom Sanction Act (N.G. 2016, no. 54);
- National Decree entering into force of Kingdom Sanction Law (N.G. 2017, no. 2);
- National Ordinance extension of validity sanction decrees 2018 (N.G. 2018, no. 34);

- National Ordinance of the 20th of December 2024 Containing Rules concerning Games of Chance (National Ordinance on Games of Chance) (PB 2024, no. 157);
- Curaçao Gaming Control Board's Regulations for the combating of Money Laundering, the Financing of Terrorism and Proliferation of weapons of mass destruction, last update January 2025..

The Company's operations are guided by collaboration with international regulatory bodies, including the Financial Action Taskforce (FATF) and the Caribbean Financial Action Task Force (CFATF), strengthening our compliance with global standards.

3 Definitions

"CGA/GCB"	Curaçao Gaming Authority or Gaming Control Board, used interchangeably
"Compliance Officer"	means a senior officer at management level and independent from the games' operations, responsible for the detection and deterrence of money laundering and terrorist financing.
"Financial Transactions"	include the purchase or cashing in of casino chips or tokens, the opening of an account, wire transfers and currency exchanges. Financial transactions do not refer to gambling transactions that include only casino chips or tokens. Amounts wagered and winnings are considered as gambling transactions. Gambling transactions are not considered as financial transactions.
"Financing of proliferation (PF)"	is the provision of funds for the manufacture, acquisition, possession, development, export, trans-shipment, brokering, transport, transfer, stockpiling or use of nuclear, chemical or biological weapons and their means of delivery and related materials.
"FIU"	means the Financial Intelligence Unit Curaçao, referred to in art. 2 of the NORUT.
"Money laundering (ML)"	is generally defined as engaging in acts designed to conceal or disguise the true origins of criminally derived proceeds so that the proceeds appear to have derived from legitimate origins or constitute legitimate assets. Money laundering may generally occur in three stages. Cash first enters the financial system at the 'placement' stage, where the cash generated from illegal or criminal activities is converted into monetary instruments, such as money orders or traveller's checks, or deposited into accounts at financial institutions. At the 'layering' stage, the funds are transferred or moved into other accounts or other financial institutions to further separate the money from its criminal origin. At the 'integration' stage, the funds are reintroduced into the economy and used to purchase legitimate assets or to fund other criminal activities or legitimate businesses.

"NOIS"	means National Ordinance on Identification of Clients when rendering Services (Landsverordening identificatie bij dienstverlening, N.G. 2017, no. 92).
"NORUT"	means National Ordinance on the Reporting of Unusual Transactions (Landsverordening Melding Ongebruikelijke Transacties, N.G. 2017, no. 99).
"Politically Exposed Persons (PEPs)"	means: Foreign PEPs are individuals who are or have been entrusted with prominent public functions by a foreign country and the direct family members or close associates of such persons. Examples are: Heads of State or of government, senior politicians, senior government, judicial or military officials, senior executives of state-owned corporations, important political party officials. Domestic PEPs are individuals who are or have been entrusted domestically with prominent public functions, for example Heads of State or of government, senior politicians, senior government, judicial or military officials, senior executives of state-owned corporations, important political party officials, and the direct family members or close associates of such persons. Persons who are or have been entrusted with a prominent function by an international organization refers to members of senior management, i.e. directors, deputy directors and members of the board or equivalent functions, and the direct family members or close associates of such persons.
"Source of Funds"	Refers to how the funds for a particular transaction were obtained by the player, like personal savings, pension release, property sales, share sales and dividends, gambling winnings, gifts, compensation from legal rulings.
"Source of Wealth"	is the origin of all the money a person has accumulated over their lifetime, like employment income, inheritances, investments, business ownership interests.
"Targeted financial sanctions"	are measures imposed by governments or international bodies to restrict the financial activities of specific individuals or entities linked to unlawful activities, such as terrorism or money laundering. These sanctions aim to prevent these parties from accessing the financial system. Unlike general sanctions that apply broadly to entire countries, targeted sanctions focus on specific individuals or entities. This approach minimizes the impact on the wider population while addressing particular risks. Targeted financial sanctions apply to individuals or entities listed on sanctions lists maintained by organizations like the United Nations or the European Union.
"Terrorism Financing (TF)"	refers to the provision of funds or financial support for terrorist acts, individuals, or organizations, and is characterized by the intent to intimidate populations or compel governments and international bodies to act or refrain from acting. Terrorist financing may not involve the proceeds of criminal conduct, but rather an attempt to conceal

	either the origin of the funds or their intended use, possibly for criminal purposes. Legitimate sources of funds are a key difference between terrorist financiers and traditional criminal organizations. In addition to charitable donations, legitimate sources include foreign government sponsors, business ownership and personal employment. Although the motivation differs between traditional money launderers and terrorist financiers, the actual methods used to fund terrorist operations can be the same as or similar to methods used by other criminals to launder funds. Funding for terrorist attacks does not always require large sums of money, such funding could be of cumulative nature over extended periods, and the associated transactions may not be complex.
"Unusual transaction"	A transaction that is considered as such on the basis of certain indicators, pursuant to Article 10 of the NORUT.
"(Ultimate) beneficial ownership (UBO)"	Refers to the natural person(s) who ultimately own(s) or control(s) a customer and/or the person on whose behalf a transaction is being conducted. It also incorporates those persons who exercise ultimate effective control over a legal person.

4 Policy Implementation

The Company internal controls are a set of policies and procedures aimed at securing the efficient and compliant business within the Company and provision of the safe and fair gambling environment for the customers. Internal controls in relation to ML&TF risks consist primarily of systematic application of the rules and procedures laid out in the corresponding sections of this Policy and the Regulations.

4.1 Responsibility of the Senior Management

The Senior Management is responsible for:

- setting and approving the general principles underlying the Policy for Prevention and Combatting of Money Laundering and Terrorist Financing
- appointing Compliance Officer and communicating to them the internal policies
- defining the duties and responsibilities of the Compliance Officer
- ensuring that effective and sufficient systems and controls are in place to enable compliance with all rules and regulations
- ensuring that the Compliance Officer have completed and timely access to all data required to effectively undertake their duties including, but not restricted to, data concerning customer identity, transaction documentation and other relevant information maintained
- ensuring that all employees are aware to whom they have to report any information concerning unusual transactions
- ensuring that the Compliance Officer have sufficient resources including competent staff and technological equipment

- assessing and approving the annual report and taking appropriate actions to remedy any weaknesses and/or deficiencies identified in the annual report.

4.2 Compliance Officer

The Compliance Officer has working knowledge of the Company's business environment, risks inherent to the Company's business model and AML, CTF and CPF provisions as stipulated in the Regulations as amended. General duties of the Compliance Officer include monitoring of the Company's compliance with the AML, CTF and CPF obligations, assessment of the business risks both internal and external, oversight of the AML, CTF and CPF related communication and training for employees and reporting of the findings and critical issues of the AML, CTF and CPF systems and procedures to the managers and executives of the Company.

4.3 Employees

Staff Reliability and Probity

The Company applies rigorous pre-employment and ongoing screening procedures to ensure staff integrity and suitability for their roles. This includes verification of identity, background checks, reference verification, and role-specific assessments where necessary. Additional screening measures apply to individuals in sensitive or senior positions.

Professional Support and Training

The Company provides AML training tailored to each employee's role and responsibilities. Training components include:

- Mandatory induction training for all new employees, covering AML, CTF and CPF principles, internal reporting procedures, and regulatory obligations.
- Annual refresher training to maintain awareness and reinforce responsibilities.
- Ad hoc training triggered by regulatory updates, product changes, or identified compliance weaknesses.

The Compliance Officer maintains a training register documenting attendance, content delivered, and testing outcomes where applicable.

5 The Risk-Based Approach

5.1 Explanation of the Risk-Based Approach

The Company adopts a risk-based approach in our AML compliance program, as recommended by FATF guidelines. This approach is essential for identifying and mitigating ML/TF risks specific to the online gaming industry. When developing its AML compliance program, the Company assesses risks in such a way that higher risks necessitate more robust measures to mitigate them. Conversely, for lower-risk scenarios, the Company may employ simplified measures.

To effectively apply the risk-based approach, the Company conducts a preliminary assessment of the risks associated with money laundering and terrorist financing within the organization, and

based thereon develops and implements suitable policies, procedures, and controls to manage and mitigate these identified risks, including the present Policy.

The Company shall continuously monitor and enhance the effectiveness of these policies, procedures, and controls, ensuring that it maintains thorough documentation of its risk assessments, detailing all actions taken and the rationale behind them. The Company shall also assess and manage risks associated with emerging technologies and new gaming products that may facilitate ML/TF/PF activities.

5.2 Business Risk Assessment

The Business Risk Assessment (BRA) framework is an essential element of the Company's AML/CFT/CPF compliance program. It offers a systematic risk-based approach to identifying, assessing, and mitigating the risks associated with money laundering, terrorist financing, and proliferation financing within the Company's operations.

The Company conducts comprehensive BRAs and evaluates potential risk factors related to customers, products, services, geographic locations, and delivery channels. Each identified risk factor is assessed based on its likelihood and potential impact, utilizing both quantitative and qualitative data. Appropriate controls and measures are then implemented to address the identified risks, tailored to the specific level and nature of the threat. All findings, evaluations, and mitigation strategies are documented and reported to senior management and relevant regulatory authorities.

BRAs are conducted regularly to ensure that the Company's risk profile stays current and accurate, with a comprehensive assessment performed annually. Additional assessments may be prompted by significant events, such as the launch of new products, changes in regulations, or substantial shifts in the business landscape.

The BRA, including the Company's risk appetite and key mitigation measures, shall be formally reviewed and approved by the Managing Director and/or Board of Directors at least annually. Evidence of such approval shall be documented and retained.

5.3 Technological Risk Assessment

In line with the risk-based approach the Company shall conduct a Technological Developments Risk Assessment in order to mitigate any ML, TF and PF risks. Where the Company is considering the implementation of technology, as indicated in the following section, a Responsible Person shall be appointed to complete the Technology Risk Assessment Form. The form will be completed by the Responsible Person appointed when any of the following criteria is being considered:

- The development of a new product;

- A new delivery mechanism;
- A new business practice emerges, in particular every time money and technology come together in a new way, whether that is a new payment channel, a new way to transfer money between services or a change in the payment infrastructure offered by technological developments, and

A new technology is used to deliver new or old services

6 Customer Acceptance Policy

6.1 Customer Risk Assessment

The Customer Risk Assessment procedure is a crucial component of the internal AML, CTF and CPF program at the Company, designed to evaluate the specific risks associated with providing services or products to customers. The assessment begins when a new customer applies for an account, at which point their risk profile is formulated based on the information collected. The initial Customer Risk Rating assigned helps determine the frequency and intensity of ongoing reviews; higher-risk customers will be subject to more frequent and rigorous monitoring.

The risk assessment process takes into consideration the following factors:

6.1.1 Customer Risk

This involves assessing the customer's background, occupation, and transaction patterns. High-risk customers, such as politically exposed persons (PEPs) and those from high-risk jurisdictions, receive particular scrutiny. Categories of customers whose activities indicate a higher risk include:

- Customers who have multiple sources of income;
- Customers with irregular income streams;
- PEPs;
- High spenders (money can be derived from illegal activities);
- Disproportionate spenders (inconsistent with casino's information about customer's known source of income/assets);
- Casual customers like locals/tourists, especially when spending pattern changes;
- Improper use of third parties, criminals use third parties to gamble to break up large amount of cash, to buy chips or to cash out on behalf of others to avoid CDD measures;
- Multiple casino player rating accounts to hinder a casino to track their gambling activities;
- Unknown customers (redeeming large amounts of chips);
- Junkets (junket operators monitor player activity and issues and collect credit).

6.1.2 Product/Service Risk:

This factor evaluates the risks associated with the products and services offered. The following products and services are considered to be at higher risk of criminal exploitation. This includes gaming products or services where customers can influence game outcomes, either on their own or in collaboration with others. Additionally, certain payment methods used by customers and accepted by casinos are seen as riskier for ML and TF. The following is a non-exhaustive list of high-risk factors:

- Anonymous payment methods: This includes pre-paid cards and virtual assets.
- Casino account usage: These accounts should only be used for gambling, not for depositing and withdrawing funds without playing or with minimal play.
- Specific game types: Games like roulette and craps, where bets are made even.
- Peer-to-peer gaming.
- Third-party accounts: Customers using accounts or cards that belong to someone else.
- Fund transfers: Moving money from one gaming account to another.
- Financial services: This includes services like credit markers, currency exchange, and check cashing.
- Multiple accounts or wallets: An internet operator might control several websites.
- Changes to financial accounts: Adjustments made to fund casino accounts.
- Identity fraud: Stolen financial account details used on websites, including stolen identities used to open financial accounts that are then used for gambling.
- Pre-paid card funding: Using cash to load a pre-paid card carries similar risks as cash transactions.
- Games with multiple operators: For example, poker platforms shared by different operators.
- Electronic wallets: Not all e-wallets are licensed in trustworthy countries, and some accept cash deposits. Moreover, e-wallets that only accept funds from financial accounts may not show the transaction to the online casino, which could help dishonest customers hide their gambling activities.

6.1.3 Geographic Risk:

This assessment considers the geographic location of the customer and the transaction, with countries that have weak AML/CFT regulations or high levels of corruption being deemed higher risk. The nationality, residence and place of birth of the player have to be considered as these might be indicative of a heightened geographical risk. The Company regards the following sources of information produced by the FATF and other well-known non-governmental bodies (not limited):

- 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 Company consistently monitors updates to the lists above and adjusts its CDD process to reflect relevant changes. Please see [Appendix I](#).

6.1.4 Delivery Channel Risk:

This factor looks at the risks associated with the methods used to establish a business relationship or through which transactions are carried out. The Company considers the increased risk of ML/TF of the use of channels that favor anonymity and interactions on a non-face-to-face basis and, to the extent possible, shall take all reasonable measures to address and mitigate said risks.

6.1.5 Prohibited Accounts

The Company's customer acceptance policy is formulated in accordance with legal requirements and aligns with the Company's risk appetite as well as the BRA. Therefore, certain categories of individuals are prohibited from being accepted as customers, either by preventing them from registering or by blocking their access to our site, as necessary:

- Individuals under the age of 18.
- Individuals listed on sanctions imposed by UN, EU or OFAC.
- Individuals for whom there are reasonable grounds to suspect involvement in ML/TF/PF or any other form of criminal activity.
- Self-excluded customers who are barred from our websites or included in any national self-exclusion registers as stipulated by licensing conditions.
- Individuals who have submitted documents or information that the Company has reasonable grounds to suspect are fraudulent or falsified.
- Customers for whom an elevated risk level in their profile has led the Company to terminate the customer relationship for any reason.

6.2 Politically Exposed Persons (PEPs)

The Company implements robust procedures for identifying and managing relationships with PEPs, defined as individuals entrusted with prominent public functions, as well as their close associates and family members.

- **Identification:** Comprehensive screening against reliable databases will be conducted during the onboarding process to determine PEP status.
- **Approval Process:** No business relationship shall be established or continued with a PEP without obtaining senior management approval.
- **Source of Wealth and Funds:** The Company will request a statement from the PEP regarding their source of wealth and verify this information through independent and reliable sources. Additional documentation may be requested if necessary.
- **Enhanced Monitoring:** The Company will conduct enhanced ongoing monitoring of PEPs, analysing their spending patterns to ensure they align with declared legal sources of funds.

6.3 Sanctions Screening

The Company is committed to complying with targeted financial sanctions, which require the freezing of funds and assets of individuals and entities identified by the United Nations (UN) and European Union (EU) as being involved in terrorism or proliferation activities. Mechanisms are established to ensure compliance with these sanctions. This includes, but is not limited to, the following:

- The Company shall comply with relevant sanctions decrees and regulations and monitor any and all amendments thereof and implement these without undue delay.
- The Company shall perform perpetual sanctions screening on customers and also perform trigger-based sanctions screening of customers at least in the following scenarios:
 - At the moment of registration;
 - At the moment of withdrawal request;
 - At the moment of any request for change of personal details or payment methods.

In the event that a true match is discovered, the Company shall freeze without delay and without prior notice the funds of the particular customer(s), in accordance with the Sanctions Ordinance, and shall immediately file a report with the FIU in line with the Process for the freezing of resources. Once the true match is confirmed by the supervisory authority, the Company shall terminate services and keep the frozen assets until further instruction from the supervisory authority.

7 Customer Due Diligence Measures

The Company applies a structured and risk-sensitive CDD process, beginning at the onboarding stage and continuing throughout the customer relationship. This framework ensures that the Company understands who its customers are, assesses the risk they pose, and applies appropriate verification and monitoring measures in line with Curaçao's AML, CTF

and CPF requirements under the NOIS and the NORUT**, and ensures that all CDD and transaction records are retained in accordance with the Company's record-keeping obligations (minimum five (5) years).**

7.1 Customer Onboarding and Identification

At the time of registration, all customers must provide:

- Full name;
- Date of birth;
- Permanent residential address;
- Nationality; and
- Identification number.

Customers must verify their identity using reliable, government-issued identification documents (e.g., passport, ID card, or driver's license). These documents must be valid, include a photograph, and be legible. If the document is not in a language understood by the Company, a certified translation may be required.

Proof of permanent residential address must be submitted and dated within the last six (6) months (e.g., utility bill or bank statement). The Company prohibits anonymous and fictitious accounts and applies robust internal controls to prevent their creation. All identification and verification information collected under this section shall be recorded and retained in accordance with the record retention requirements set out in this Policy (minimum five (5) years).

7.2 Verification of Beneficial Ownership

Customers must confirm they act on their own behalf. The Company monitors for indications of third-party control. The following safeguards apply:

- Payment method verification: deposits and withdrawals must be made using accounts in the customer's name.
- Monitoring for proxy activity or suspicious behaviour.
- Immediate verification upon withdrawal requests or Cg. 4,000 thresholds.

Where the Company establishes a business relationship with a legal person (including affiliates, suppliers, or other corporate counterparties), the Company shall identify and verify the Ultimate Beneficial Owner(s) (UBO(s)). A UBO is any natural person who ultimately owns or controls, directly or indirectly, twenty-five percent (25%) or more of the ownership interest or voting rights in the legal person, or who otherwise exercises ultimate effective control over that legal person.

For such legal persons, the Company shall obtain and verify, at a minimum: (i) legal name, registered address, and registration number; (ii) ownership and control structure; and (iii) the full name, date of birth, nationality, and residential address of each UBO holding $\geq 25\%$, supported by reliable independent documentation (e.g., registry extracts, shareholder registers, structure charts, notarized declarations, and/or reputable commercial databases). Where no individual meets the 25% threshold, the Company shall identify and verify the natural person(s) exercising senior managing control.

7.3 Customer Risk Assessment and Purpose of Relationship

Each customer is assigned a risk rating based on:

- Jurisdiction of residence;
- PEP or sanctions status;
- Payment method used;
- Anticipated transaction volumes and types.

The customer must provide their occupation and estimated annual income. This information is verified proportionally to the assessed risk. For High-Risk customers, supporting documentation (e.g., payslips, bank statements, tax returns) is required. Where relevant (including for higher-risk relationships), the Company may also request and verify Source of Funds (SOF) and/or Source of Wealth (SOW) information to ensure the customer's activity is consistent with the Company's knowledge of the customer and their risk profile.

7.4 Simplified Due Diligence (SDD)

SDD may be applied only where:

- The customer is classified as low risk;
- No suspicion of ML/TF exists;
- No indicators of PEP status or high-risk jurisdiction are present;
- The total transaction value is below Cg. 4,000.

Under SDD:

- Basic identification is collected;
- Verification may be delayed until specific thresholds are met;
- Monitoring is tailored based on risk, and must still detect unusual activity.

If risk increases or suspicious behaviour arises, SDD must be upgraded to CDD or EDD. SDD must not be applied where there are reasonable grounds to suspect ML/TF/PF, where sanctions or PEP indicators are present, or where the Company has doubts about the veracity or adequacy of previously obtained customer data.

7.5 Customer Due Diligence (CDD)

CDD must be performed:

- When the customer reaches the Cg. 4,000 thresholds (cumulatively or per transaction);
- On all withdrawals;
- When doubts arise about prior CDD data;
- When required under NORUT or due to suspicion of ML/TF/PF.

All financial transactions (excluding bonuses or winnings) are counted toward the threshold. Identification and verification must be complete before allowing further transactions. For the purposes of this Policy, “linked transactions” are two or more transactions that are connected by time, purpose, customer behavior, or other relevant indicators and which, taken together, may reasonably be considered part of a single transaction or series of transactions. Where linked transactions are identified, the Company shall aggregate the total transaction value for the purposes of determining whether applicable thresholds have been met, including the Cg. 4,000 threshold for mandatory CDD.

The Company shall ensure that CDD records, supporting documentation, and evidence of decisions taken (including risk ratings and any escalation to EDD) are maintained and retained for a minimum period of five (5) years in accordance with this Policy.

7.6 Timeline for Compliance and Non-Compliant Documents

If the customer cannot provide compliant documents within thirty (30) days from the moment the Cg. 4,000 threshold is reached, the Company shall terminate the relationship with the customer and consider filing an Unusual Activity Report with the FIU, provided that a presumption of ML or TF exists.

During the CDD process, customers may continue to access their accounts while the Company gathers the necessary information. However, if a deposit reaches the Cg. 4,000 thresholds, the customer will be prohibited from further deposits or withdrawals, although they may continue to play with their existing balance. Conversely, if the threshold is reached due to a withdrawal request, the account will be completely frozen, halting all gameplay.

If a document submitted by a (potential) customer does not meet the verification standards, the designated staff member must immediately flag it for further examination. The initial review should be thorough to pinpoint the specific reasons for non-compliance. Once a non-compliant document is identified, the customer must be informed without delay.

All actions taken in response to non-compliant documents shall be carefully recorded. This includes the initial identification of the issue, communications with the customer, any escalations, and the final outcome. Comprehensive records should be maintained in the customer's file to ensure a complete audit trail. All such records and audit trail evidence (including communications, re-submissions, decisions, and account restrictions) shall be

retained for a minimum of five (5) years from the end of the business relationship or completion of the occasional transaction, whichever is later.

7.7 Enhanced Due Diligence

Enhanced Due Diligence (EDD) will be implemented for customers identified as higher risk, consistent with the risks identified. In particular, they should increase the degree and nature of monitoring of the business relationship, in order to determine whether those transactions or activities appear unusual. Enhanced Due Diligence has to be conducted where the risks of money laundering or terrorist financing are higher. In any case, the following scenarios are subject to EDD:

- Residents of higher risk geographic areas;
- Politically Exposed Persons (PEP's);
- Products or transactions that might favor anonymity;
- New products and new business practices, including new delivery mechanism, and the use of new or developing technologies for both new and pre-existing products.

The applied measures must be consistent with the risks identified. They should increase the degree and nature of monitoring of the business relationship, in order to determine whether those transactions or activities appear unusual or suspicious. Examples of EDD measures include but are not limited to:

- Obtaining additional information on the customer, like occupation, previous address and information available through public databases, internet, etc.;
- Obtaining additional information on the intended nature of the business relationship;
- Obtaining information on the source of funds or source of wealth of the player:
 - **Source of Funds** refers to the origin of the specific funds involved in a particular transaction. This includes identifying how and where the money was generated, such as through salary, business income, or sale of assets.
 - **Source of Wealth**, on the other hand, pertains to the total accumulation of an individual's wealth over time. This includes understanding the broader context of their financial background, such as investments, property ownership, and other significant assets.
- Obtaining information on the reasons for intended or performed transactions;
- Obtaining the approval of senior management to commence or continue the business relationship;
- Conducting enhanced monitoring of the business relationship;
- Requiring the first payment to be carried out through an account in the customer's name with a bank subject to similar CDD standards.

7.8 Ongoing Monitoring

7.8.1 Ongoing Customer Profile Monitoring

During the periodic review of a customer, the Company verifies and confirms that the CDD information about the client, nature and purpose of the business relationship, and SOF is still accurate and up to date, evaluate if there are external signals (bad press/adverse news, incidents) that could give rise to a change in the business risk profile of the customer and ensure to perform screening against sanctions lists and PEP lists. The periodic review also includes an overall review of the transaction behavior of the client to determine if unusual activities have taken place, for instance in case of transactions which normally would not be expected.

The periodical review of the customer is based on the risk profile of the customer:

- For high-risk customers – once per year;
- For medium risk customers – once every 2 years;
- For low-risk customers – once every 3 years.

7.8.2 Ongoing Transaction Monitoring

The Company performs both real-time monitoring of transactions, as well as post-event monitoring, to ensure that such transactions and activity are consistent with the Company's knowledge of the client and their expected activity. More attention is paid to high amounts, high-risk clients and high-risk jurisdictions. Particular risk factors will be closely monitored concerning business relationships and transactions, including:

- Gambling or transaction patterns that diverge from what is considered normal or what the customer initially indicated when establishing the business relationship.
- Execution of unusually large transactions by the customer.
- Requests for withdrawals to accounts other than those verified to belong to the customer (such withdrawals are prohibited).
- Requests to transfer gambling accounts or winnings to third parties (such transfers are also prohibited).

7.9 Reliance on Third Parties to Perform Due Diligence

The Company recognizes that when contracting or outsourcing specific functions, there is a risk of increased AML exposure if the third parties involved are not properly vetted and their relevant processes are not assessed. Prior to entering into any service agreements that fall under this Policy, the Company performs due diligence to verify the legitimacy of the potential partners. This due diligence includes, at a minimum, establishing the identity of the party and where it concerns a legal person – of its beneficial owners and the persons authorized to represent it. Additionally, where applicable, potential third-party suppliers are required to submit a copy of their AML policies and procedures, proof of pertinent licensing or certification.

8 Business Affiliate and Supplier Diligence

The Company recognizes that when contracting or outsourcing specific functions, there is a risk of increased AML exposure if the third parties involved are not properly vetted and their relevant processes are not assessed. Prior to entering into any service agreements that fall under this Policy, the Company performs due diligence to verify the legitimacy of the potential partners. This due diligence includes, at a minimum, obtaining the following documents:

- Certificate of Incorporation and Memorandum & Articles of Association
- Identification of Directors and/or Shareholders
- Declaration of Beneficial Ownership
- KYC documentation for signatories, as applicable.

Additionally, potential third-party suppliers are required to submit a copy of their AML/CTF policies and procedures, where applicable. The Compliance Officer will review these documents for their accuracy and completeness prior to entering into any agreements.

9 Reporting Unusual Transactions

9.1 Reporting Obligations

All unusual activities and transactions, including attempted transactions, are initially reported internally. The officers responsible for transaction monitoring must immediately report any unusual activities to the Compliance Officer upon identification, providing a brief description of the specific mitigating measures taken.

All employees who engage with customers or have access to customer information receive anti-money laundering training. This training prepares them to identify actions by customers that may reasonably raise suspicions of money laundering or terrorism financing. Staff members are expected to recognize and understand any gaming or transaction behaviors that might indicate customer involvement in money laundering or terrorism financing. If they know, suspect, or have reasonable grounds to believe they are dealing with the proceeds of crime, they must submit an Internal Unusual Activity Report to the Compliance Officer (CO) in accordance with the Reporting Procedure. This ensures that the employee's legal obligation to report is fulfilled. Please see [Appendix II](#) for the Report form.

Employees are required to report any unusual activity to the Compliance Officer immediately, but no later than 24 hours after the transaction has been executed, using the Internal Unusual Activity Report form. If a more in-depth investigation is necessary, the Compliance Officer will complete this within ten (10) business days. During this time, the Compliance Officer may request additional information from relevant departments.

If the Compliance Officer concludes that the activity is unusual, a report shall be submitted to the FIU Curaçao regarding any unusual monetary operations or transactions within 48 hours. In any cases whereby the report is made under one of the objective indicators, as defined below, the report must be made to the FIU Curaçao no later than 48 hours after the transaction has been executed.

9.2 Recognition of Unusual Transactions

Staff will be trained to recognize unusual transactions based on customer profiles and specific indicators. Reporting procedures to the compliance officer will be established.

According to NORUT, the Company is observing both objective and subjective indicators to assess whether a customer's transaction is deemed unusual. All such transactions must be reported to the compliance officer in a format approved by management. Additionally, any supporting documentation, such as copies of identification, cash-out slips, and other relevant records, must also be submitted as supplements.

The Compliance Officer is tasked with maintaining an organized filing system for these records. If the casino fails to report internally identified transactions to the Financial Intelligence Unit (FIU), the rationale for this decision must be thoroughly documented and signed by the compliance officer and/or management. In accordance with the FATF Recommendations, the Company and its employees pay particular attention to all complex or unusually large transactions, as well as any unusual transaction patterns that lack a clear economic or legitimate purpose.

The following transactions or intended transactions are deemed unusual:

- a. A transaction, which is reported to the police or judicial authorities in connection with money laundering or the financing or terrorism;
- b. An intended transaction carried out by or for the benefit of a natural person, legal person, group or entity which is on a list compiled by virtue of the Sanctions National Ordinance (N.G. 2014 no. 55);
- c. A transaction amounting to Cg. 5,000.00 or more, regardless of whether this transaction is carried out in cash, via a check or another payment instrument or electronically or in any other non-physical manner. This includes but is not limited to:
 1. A cashless transaction in the amount of Cg. 5,000.00 or more.
 2. Accepting or releasing a deposit in the amount of Cg. 5,000.00 or more at the request of the customer;
 3. Sale to a customer of chips in the amount of Cg. 5,000.00 or more. "Chips" include but is not limited to tokens and credits.
 4. A cash out in the amount of Cg. 5,000.00 or more;

- d. Transactions where there is cause to presume that they can be related to money laundering or terrorist financing.

Please note that indicators (a) to (c) are referred to as “objective indicators”, while (d) is referred to as “subjective indicator”. While the objective indicators are based on measurable facts and do not require interpretation automatically classifying a transaction as unusual, the subjective criterion involves a more nuanced assessment, considering the context and behavior of the client. For the purposes of reporting unusual transactions under the objective indicators above, it is noted that the threshold of Cg. 5,000.00 resets per game day of the user.

9.3 Prohibition of Disclosure

All reports and investigations must be handled with the highest level of confidentiality in accordance with Article 20 of NORUT. Unauthorized disclosure of information related to unusual activity reports is strictly prohibited and may lead to legal and disciplinary action.

The Company has implemented a system of measures to ensure that employees and representatives who report suspicions of money laundering, terrorist financing, and/or financing of proliferation to the Financial Intelligence Unit Curaçao are safeguarded from threats or hostile actions by other employees, members of the management body, or customers. Additionally, they are protected from adverse or discriminatory employment actions.

9.4 Record Keeping

The casino retains all necessary records of transactions, both domestic and international, for a minimum of five (5) years to ensure compliance with information requests from regulatory authorities. These records must be detailed enough to allow for the reconstruction of individual transactions, including the amounts and types of currency involved, if applicable, to provide evidence for potential criminal prosecutions.

All records gathered through CDD measures, such as copies of official identification documents, account files, and business correspondence, will be stored for at least five (5) years after the business relationship has ended or after the date of an occasional transaction.

Records shall be stored in a manner that ensures their integrity, confidentiality, and accessibility. Electronic records shall be stored in secure, encrypted databases with access controls to prevent unauthorized access. Physical records shall be stored in locked, fireproof cabinets within secure areas of the office. Access is restricted to authorized personnel only. Regular backups of electronic records shall be conducted and stored in a separate, secure location to prevent data loss.

After the retention period, records shall be disposed of securely to prevent unauthorized access or disclosure. Electronic records must be permanently deleted using secure deletion software

that ensures data cannot be recovered. Physical records must be shredded using cross-cut shredders or incinerated to ensure complete destruction.

When properly ordered to do so by any enactment, rule of law or court order, the Company shall provide a document, customer due diligence information, or enhanced due diligence information and the Company will maintain a register of the documents and information provided, and will keep a copy of the same.

10 Anti-Money Laundering Compliance Program

The Company's Anti-Money Laundering, Counter-Terrorism Financing and Counter-Proliferation Financing (AML, CTF and CPF) Program, including this Policy and all related procedures, shall be formally approved by the Board of Directors.

The Board of Directors bears ultimate responsibility for the oversight of the Company's AML, CTF and CPF framework and shall ensure that the program is adequate, effective, and proportionate to the risks arising from the Company's business activities.

10.1 Appointment of a Money Laundering Compliance Officer

A senior compliance officer will be designated, separate from our gaming operations, responsible for overseeing the AML program and ensuring compliance with regulations. Our AML/CTF compliance officer will have timely access to customer identification data, transaction records, and other relevant information. This officer will operate independently to ensure robust compliance.

10.1.1 Duties of the Compliance Officer

The compliance officer shall be assigned at least the following responsibilities:

- To design and implement the AML program;
- To verify adherence to local laws and regulations regarding the detection and deterrence of money laundering and terrorist financing;
- To review compliance with the casino's policy and procedures;
- To organize training sessions for the staff on various compliance-related issues;
- To analyze transactions and verify whether any are subject to reporting according to the indicators mentioned in the Ministerial Decree regarding the Indicators for Unusual Transactions;
- To review all internally reported unusual transactions for their completeness and accuracy with other sources;
- To keep records of internally and externally reported unusual transactions;
- To execute closer investigation of unusual transactions if necessary;
- To prepare the external report of unusual transactions;

- To make necessary changes to the AML program;
- To remain informed on the local and international developments on money laundering and terrorist financing and to make suggestions to management for improvements; and
- To prepare periodic information on the casino's efforts against money laundering and financing of terrorism and financing of proliferation.

10.2 Employee Screening and Training Programs

10.2.1 Employee Due Diligence

Employee due diligence is a process employed to screen employees with the objective of identifying and reducing the Company's exposure to the risks associated with money laundering and terrorism financing. These procedures apply not only to the Company's contractual employees, but also to its contractors and subcontractors.

The employee due diligence process is informed by the Company's risk assessment and the specific roles within the organization.

Any employee whose position may enable them to facilitate money laundering or terrorism financing must undergo screening. This requirement applies to:

- Prospective employees prior to their hiring for such roles.
- Current employees before they are transferred or promoted to such positions.

To screen both current and potential employees, the Company should:

- Identify the individuals.
- Verify their identity.
- Confirm their employment history, such as through references.
- Determine their suitability for the position and assess whether they pose any risk to the Company.

The Company will consider the knowledge and qualifications required for the responsibilities and authorities associated with each role.

Positions that may render an employee vulnerable to collusion with or coercion by criminal organizations should undergo more rigorous checks. The Company must evaluate whether:

- The employee has a criminal record, which may be verified through a police check.
- The employee is or has been subject to regulatory, court, or legal actions.
- The employee has leveraged bankruptcy laws for personal gain.
- The employee has resided in high-risk countries or regions.

Regular updates and re-evaluations are essential for maintaining an effective compliance program against money laundering, terrorism financing, and proliferation financing. This process

includes conducting periodic reviews of all employees, with a particular emphasis on those in high-risk roles, to ensure their risk profiles are accurate and current. Additionally, reviews triggered by significant changes in an employee's job responsibilities, promotions, or external alerts that may influence their risk status are also initiated.

10.2.2 Training

In delivering AML, CTF and CPF training to the designated categories of employees, the Company will consider the necessary knowledge and qualifications required for their duties, responsibilities, and authorizations. As part of the training framework, the Company will outline the AML, CTF and CPF requirements and provide comprehensive information on the measures and activities that staff are expected to undertake within their roles.

The Company will ensure that documentation of the training provided to staff is maintained, capturing the following information:

- Details on the content of the training programs;
- The names of the staff members who have received the training;
- The date on which the training was provided;
- The results of any testing carried out to measure staff understanding of money laundering and terrorist financing requirements; and
- An ongoing training plan.

The Company will regularly update the training programs to reflect any changes in internal and external regulations, as well as developments in the availability of training programs in the market for external training. Furthermore, extraordinary training in AML, CTF and CPF matters will be provided in specific situations, including:

- The introduction of new internal and external regulations related to AML, CTF and CPF that apply to the Company's staff.
- The launch of new products or services that alter the AML, CTF and CPF risk exposure.
- Instances where an employee breaches internal or external AML, CTF and CPF regulations due to a lack of knowledge during the performance of their duties.

10.3 Independent Audit Function

An independent audit function will be established for the annual evaluation of the AML program, ensuring audit personnel are qualified and findings are documented. The audit must include several key assessments, such as:

- Reviewing the Company's AML, CTF and CPF manual.
- Examining customer files.
- Evaluating compliance management.
- Conducting transaction testing.

- Assessing the adequacy of training.
- Ensuring compliance with relevant laws and regulations.
- Evaluating the system's capacity to detect unusual activities.
- Interviewing employees involved in transactions and their supervisors.
- Sampling unusual transactions and reviewing compliance with internal and external policies and reporting requirements.
- Assessing the effectiveness of the record retention system.

The audit shall also evaluate the Company's responsiveness to previous audit findings. All testing scope and results must be documented, with any deficiencies reported to senior management, along with requests for prompt corrective actions.

10.4 Examination by the Curaçao Gaming Authority

The Company shall provide information and documentation regarding its money laundering and terrorist financing policies and procedures to examiners of the CGA during examinations or upon request. The following items must at all times be readily available and accessible:

- The written and approved AML Compliance Program addressing ML/TF/PF.
- Records of the Business Risk Assessment.
- The name and job description of the Compliance Officer responsible for the company's AML policies and procedures.
- Records of reported unusual transactions.
- Records of unusual transactions that required further investigation.
- Records of frozen accounts.
- A schedule of training provided to personnel on ML/TF/PF.
- Assessment reports on the company's policies and procedures regarding money laundering, terrorist financing, and proliferation financing from the internal audit department or an external auditor.
- Customer files, including risk assessments, CDD, customer acceptance, and transaction information.

11 Compliance and Consequences of Non-Compliance

The Company is fully committed to adhering to all applicable laws and regulations related to AML, CTF and CPF and sanctions enforcement as established by the jurisdiction of Curaçao, aligning with international best practices, including the FATF Recommendations. Compliance with this Policy is mandatory for all employees, officers, agents, and third-party service providers. Non-compliance may expose the organization and individuals to significant legal, regulatory, and reputational risks, including fines or penalties imposed by Curaçao's authorities, revocation or suspension of the Company's operational license, and potential criminal prosecution for wilful violations.

Additionally, non-compliance can lead to reputational damage, resulting in loss of customer trust, negative media exposure, and strained relationships with financial partners. Operational disruptions may also occur, such as freezing of funds, loss of access to financial systems, and increased scrutiny from regulators.

Employees who violate this Policy may face disciplinary actions, including formal warnings, suspension, or termination for serious or repeated breaches, as well as potential referral to law enforcement. Third-party providers may have their agreements terminated if found non-compliant. All employees must understand and comply with the AML, CTF and CPF Policy, participate in mandatory training, and report any unusual behaviour or breaches to the Compliance Officer, who will ensure that whistleblower protections are in place.

The Compliance Officer and senior management are responsible for investigating violations, determining appropriate disciplinary actions, and reporting serious breaches to relevant authorities. All enforcement actions are documented and reviewed periodically to improve the compliance program.

12 Appendix I: Country Risk List

Please note that the following list of high-risk and low-risk countries is subject to continuous review. Any changes in geographical risk will be reflected promptly to ensure the list remains current and accurate at the time of drafting.

High-risk countries

include:

- | | | |
|--|--------------------------|---|
| 1. Afghanistan | 28. Panama | 14. Saint Kitts and Nevis |
| 2. Algeria | 29. Philippines | 15. Saint Lucia |
| 3. Angola | 30. Russia | 16. Saint Vincent & the Grenadines |
| 4. Belarus | 31. Somalia | 17. Singapore |
| 5. Bulgaria | 32. South Africa | 18. Sint Maarten Kingdom of the Netherlands |
| 6. Burkina Faso | 33. South Sudan | 19. Suriname |
| 7. Burma (Myanmar) | 34. Syria | 20. Sweden |
| 8. Cameroon | 35. Tanzania | 21. Turks and Caicos Islands |
| 9. Central African Republic | 36. Uganda | |
| 10. China | 37. United Arab Emirates | |
| 11. Côte d'Ivoire | 38. Vanuatu | |
| 12. Croatia | 39. Venezuela | |
| 13. Cuba | 40. Vietnam | |
| 14. Democratic People's Republic of Korea. | 41. Yemen | |
| 15. Democratic Republic of the Congo | | |
| 16. Ethiopia | | |
| 17. Haiti | | |
| 18. Iran | | |
| 19. Iraq | | |
| 20. Kenya | | |
| 21. Lebanon | | |
| 22. Libya | | |
| 23. Mali | | |
| 24. Mozambique | | |
| 25. Namibia | | |
| 26. Nicaragua | | |
| 27. Nigeria | | |

Low-risk countries

include:

1. Antigua and Barbuda
2. Aruba, Kingdom of the Netherlands
3. Belize
4. Bermuda
5. Cayman Islands
6. Denmark
7. Dominica
8. Finland
9. Grenada
10. Guyana
11. Montserrat
12. New Zealand
13. Norway

Excluded markets include, but are not limited to:

1. Aruba
2. Australia
3. Austria
4. Belgium
5. Bonaire
6. Czech Republic
7. Curaçao
8. France
9. Germany
10. Greece
11. Lithuania
12. Saba
13. Sint Eustatius
14. Spain
15. The Netherlands
16. United States of America

13 Appendix II: Internal Unusual Activity Report

Internal Unusual Activity Report		
Date of report:		
Client full name:		
Client ID:		
Risk rating:		
Account status (Active/Suspended/Blocked):		
Account balance:		
Date of account registration:		
Client details: E-mail:		
Client details: Phone number:		
Client details: Brand registration:		
Date of birth:		
Nationality/Country of registration:		
Address:		
Due diligence documents held:		
Reason for reporting: explain what activity / transaction gave rise to the report. If necessary, please use the additional information section:		
Date of suspected criminal activity/transaction:		
Provide details (e.g. dates and amounts) of any known intended or pending transactions:		
Name (reporting employee):	Signature:	Date:

ARBOL MEDIA B.V. AML, CTF & CPF POLICY

Upon completion, please forward the form to the department responsible as soon as possible.		
Action taken by the responsible department		
Confirmation of receipt of the MLRO: I confirm that I have received this form from the person(s) named above.	Signature:	Date: