

Anti-Money Laundering, Counter-Terrorism Financing, and Counter-Proliferation Financing (AML/CTF/CPF) Policy

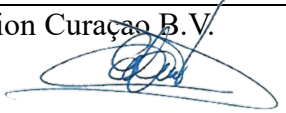
Table of Contents

1	VERSION HISTORY:	3
2	APPROVAL	3
3	PREFACE	4
3.1	COMPLIANCE STATEMENT	4
3.2	PURPOSE	4
3.3	AUDIENCE	5
3.4	DEFINITIONS	5
4	POLICY IMPLEMENTATION	7
4.1	BUSINESS RISK ASSESSMENT	7
	CUSTOMER RISK ASSESSMENT	8
4.2		8
4.2.1	<i>Customer Risk</i>	8
4.2.2	<i>Product/Service Risk</i>	9
4.2.3	<i>Geographic Risk</i>	9
4.2.4	<i>Delivery Channel Risk</i>	9
4.3	CUSTOMER ACCEPTANCE POLICY	10
4.4	TARGETED FINANCIAL SANCTIONS	10
4.5	POLITICALLY EXPOSED PERSONS (PEPs)	11
5	CUSTOMER DUE DILIGENCE (CDD)	11
5.1	IDENTIFICATION AND VERIFICATION	11
5.2	PURPOSE AND NATURE OF THE BUSINESS RELATIONSHIP	12
5.3	SIMPLIFIED DUE DILIGENCE (SDD)	13
5.4	ENHANCED DUE DILIGENCE (EDD)	13
5.5	ONGOING MONITORING	14
5.5.1	<i>Ongoing Customer Profile Monitoring</i>	14
5.5.2	<i>Ongoing Transaction Monitoring</i>	14
5.6	RELIANCE ON THIRD PARTIES TO PERFORM CDD	14
6	REPORTING OF UNUSUAL TRANSACTIONS	16
6.1	REPORTING OBLIGATIONS	16
6.2	RECOGNITION OF UNUSUAL TRANSACTIONS	16
6.3	INTERNAL REPORTING	16
6.4	COMPLIANCE OFFICER REVIEW AND ESCALATION	17
6.5	PROHIBITION OF DISCLOSURE	17
6.6	RECORD KEEPING	17
7	ANTI-MONEY LAUNDERING COMPLIANCE PROGRAM	18
7.1	APPOINTMENT OF A COMPLIANCE OFFICER	18
7.1.1	<i>Duties of the Compliance Officer</i>	18
7.2	EMPLOYEE SCREENING AND TRAINING PROGRAMS	19
7.2.1	<i>Employee Due Diligence</i>	19
7.2.2	<i>Training</i>	20
7.3	INDEPENDENT AUDIT FUNCTION	20
8	COMPLIANCE AND CONSEQUENCES OF NON-COMPLIANCE	21
9	APPENDIX I: INTERNAL DISCLOSURE FORM	22

1 Version History:

Version	Effective Date	Summary of Changes
1.1	19 November 2024	Policy Implementation
1.2	22 October 2025	Updated all legislative references and definitions, Expanded Definitions Section, Revised Business and Customer Risk Assessment sections, Updated CDD Framework, Addition of Reliance on Third Parties Section, Expanded the reporting procedure, Outlined disciplinary actions, partner termination clauses, and potential regulatory penalties for breaches of AML obligations, Formatting and Structural Updates

2 Approval

Approving Official:	Gouloud Hammoud obo Guardian Corporation Curaçao B.V. 22 October 2025 
Responsible Office:	Compliance Officer, 123 Global Media B.V.

3 Preface

3.1 Compliance Statement

123 Global 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/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/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.

3.2 Purpose

This Policy establishes the principles and internal controls governing the prevention and detection of money laundering, terrorist financing, and proliferation financing within 123 Global Media B.V. It outlines the obligations of the Company and its employees under Curaçao's AML/CFT/CPF framework and demonstrates the Company's commitment to full compliance with the National Ordinances, CGA Regulations, and relevant international standards.

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 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.;
- National Ordinance of the 20th December 2024 Containing Rules concerning Games of Chance (National Ordinance on Games of Chance) (PB 2024, no. 157)

- National Decree supervisor identification when rendering services gaming sector (L.B. 28.01.2019, no. 19/0282)
 - National Decree supervisor unusual transactions gaming sector (L.B. 28.01.2019, no. 19/0283)
 - 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);
- GCB'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.

3.3 Audience

This Policy applies to all employees, officers, contractors, affiliates, payment processors, and service providers acting on behalf of 123 Global Media B.V. Compliance with this Policy is a condition of employment and continued business partnership.

3.4 Definitions

Beneficial Owner: A natural person who ultimately owns or controls a customer and/or the natural person on whose behalf a transaction or activity is being conducted. This includes any person who ultimately exercises effective control over a legal entity or arrangement, directly or indirectly, through ownership of shares, voting rights, or other means.

Financial Intelligence Unit (FIU) Curaçao: The national authority established under the NORUT responsible for receiving, analyzing, and disseminating reports of unusual transactions. The FIU Curaçao acts as the central body for the collection and assessment of financial intelligence related to money laundering, terrorist financing, and proliferation financing.

Money Laundering (ML) is the process of concealing the true origins of illegally obtained funds, making them appear to originate from legitimate sources. Money laundering encompasses a broad range of activities, including attempts to turn criminally obtained money into 'clean' money, transferring the benefits of crimes like theft or fraud, and facilitating the laundering of criminal or terrorist property. This process typically occurs in three stages:

- *Placement*, where illegal proceeds are introduced into the financial system through financial institutions, casinos, or cash-intensive businesses, often by converting cash into monetary instruments or gaming chips. In the gambling industry, this is occasionally achieved by purchasing chips with cash and subsequently redeeming

their value without engaging in actual gameplay or with minimal play. It can also involve funding casino accounts using credit and debit cards, prepaid cards, checks, and cryptocurrency, followed by requests for payouts or inserting funds into gaming machines and immediately claiming those funds as credits.

- *Layering*, which involves transferring or moving these funds across various accounts or financial institutions to obscure their criminal origins. In the gambling industry, this may include transactions such as transferring funds between accounts, occasionally involving other casinos or jurisdictions, currency exchanges, structuring and refining transactions, as well as maintaining gambling accounts to store money and conceal it from regulatory authorities; and
- *Integration*, where the laundered funds are reintroduced into the economy, enabling their use in legitimate transactions such as purchasing luxury assets or investing in businesses.

As it is strict Company policy not to accept cash as means of payment, the Company's AML Policy is conducive the curtailment of AML risk.

Politically Exposed Person (PEP): 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."

Proliferation Financing (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.

Risk-Based Approach (RBA): An approach whereby the Company identifies, assesses, and understands the money laundering, terrorist financing, and proliferation financing risks to which it is exposed, and applies proportionate measures to mitigate those risks. This includes assigning different levels of customer due diligence, monitoring, and review based on the customer's risk profile.

Sanctions Lists: Lists of natural or legal persons, countries, or entities subject to restrictive measures under the Sanctions National Ordinance (N.G. 2014, no. 55), the Kingdom Sanctions Act (N.G. 2016, no. 54), and relevant resolutions of the United Nations, European Union, or other competent authorities. The Company is prohibited from conducting any transaction involving parties listed on these sanctions lists

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. Unlike money laundering, which always involves proceeds from illegal activities, terrorist financing may not necessarily derive from illicit sources; instead, it often utilizes legitimate funds from charitable donations, business profits, or foreign government sponsorships. While both terrorism financing and money laundering may employ similar methods – such as cash smuggling, structuring, wire transfers, and the use of debit and credit cards – the primary concern of TF is to obscure the intended use or end recipient of the funds rather than their origin. Additionally, funding for terrorist activities does not always require large sums of money, as it can accumulate over time through simple transactions.

The gaming sector, especially online platforms, can be particularly vulnerable to exploitation by terrorist groups looking to launder money or transfer funds discreetly, due to its inherent anonymity and high transaction volumes. Ultimately, the goal of terrorism financing is to facilitate the planning, preparation, and execution of acts that threaten both national and international security.

Unusual Transaction: A transaction or attempted transaction that meets the objective or subjective indicators established by Ministerial Decree pursuant to the NORUT, or that the Company otherwise suspects may be related to money laundering, terrorist financing, or proliferation financing. An unusual transaction must be reported to the FIU Curaçao even if the transaction is not completed.

Unusual Transaction Report (UTR): An internal report submitted by an employee to the Compliance Officer when there is knowledge, suspicion, or reasonable grounds to suspect that a transaction or attempted transaction may involve money laundering, terrorist financing, or proliferation financing. The Compliance Officer uses such reports to determine whether a formal Unusual Transaction Report (UTR) should be filed with the FIU Curaçao.

3.5 Policy Implementation Business Risk Assessment

The Business Risk Assessment (BRA) framework is an essential element of the Company's AML/CFT/CFP 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.

3.6 Customer Risk Assessment

The Customer Risk Assessment (CRA) will assess the particular risks the Company will be exposed to when providing its services or products to customers. The information collected to draw up the CRA will formulate the customer's risk profile. On the basis of the CRA, the proper level of CDD can then be applied.

The CRA is conducted before onboarding a customer and updated periodically or when there is a material change in customer behavior or risk indicators. Customers are classified as low, medium, or high risk, and this classification dictates the intensity of verification and frequency of monitoring.

3.6.1 Customer Risk

The Company evaluates the nature and background of each customer, including occupation, source of funds, and expected transaction patterns. Customers who present higher risk characteristics are subject to Enhanced Due Diligence (EDD) measures.

High-risk indicators include, but are not limited to:

- Politically Exposed Persons (PEPs) and their close associates or family members;
- Customers from high-risk jurisdictions or those with opaque ownership structures;
- Customers with inconsistent or disproportionate spending patterns relative to known income;
- Use of intermediaries, third parties, or multiple accounts to obscure ownership or transaction flow; and
- Customers who demonstrate reluctance to provide verification documents or explanations for unusual behavior.

The Compliance Officer ensures that identified high-risk customers receive enhanced monitoring and periodic review.

3.6.2 Product/Service Risk:

The Company assesses the vulnerability of its products and services to misuse for ML/TF/PF purposes.

Products or services that allow rapid movement of funds, anonymity, or peer-to-peer interactions are generally considered higher risk.

Increased risk may arise from:

- Anonymous or untraceable payment methods, such as pre-paid cards or certain e-wallets;
- Accounts used primarily for deposits and withdrawals without actual gaming activity;
- Fund transfers between customer accounts;
- The use of third-party payment instruments or accounts not in the customer's name; and
- Complex multi-operator gaming platforms that obscure the origin of funds.

Where higher-risk products or services are offered, the Company implements additional transaction monitoring, source of funds verification, and restrictions on payment methods.

3.6.3 Geographic Risk:

The Company considers the geographic location of customers, counterparties, and financial institutions when assessing risk.

Countries or territories with inadequate AML/CTF/CPF controls, high levels of corruption, or links to terrorist or proliferation activities are deemed higher risk.

To assess geographic exposure, the Company relies on credible and authoritative sources, including:

- The FATF lists of High-Risk Jurisdictions and Jurisdictions under Increased Monitoring;
- The CFATF Public Statement;
- The European Commission's list of third countries with strategic AML/CFT deficiencies; and
- The Transparency International Corruption Perceptions Index.

The Compliance Officer monitors updates to these lists and ensures that controls are promptly adjusted to reflect changes in risk.

3.6.4 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.

3.7 Customer Acceptance Policy

The Company accepts only those customers whose identities can be verified and whose activities and sources of funds are lawful and consistent with the Company's risk appetite.

Customers presenting unacceptable risk levels shall not be onboarded:

- Individuals under the age of 18.
- Individuals listed on sanctions imposed by UN, EU.
- Residents of countries classified as high-risk concerning AML/CTF/CPF risks.
- 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.

3.8 Targeted Financial Sanctions

We are committed to complying with targeted financial sanctions, which require the freezing of funds and assets of individuals and entities identified by the UN and 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 for 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 immediately proceed with freezing the funds of the particular customer(s), in accordance with the Sanctions Ordinance, and shall immediately file a report with the FIU. 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.

3.9 Politically Exposed Persons (PEPs)

The Company recognizes the elevated risk of money laundering, corruption, and bribery associated with business relationships involving PEPs. PEP screening is an integral component of the Company's CDD process and must be performed at onboarding, periodically throughout the relationship, and whenever there are changes in the customer's profile or ownership structure.

All customers and beneficial owners are screened for PEP status during registration and prior to account activation. Screening results are re-checked at least once every twelve (12) months and whenever the PEP lists are updated or the customer's personal or ownership information changes.

Where a customer or beneficial owner is identified as a PEP, or where there is doubt regarding PEP status, the case is immediately escalated to the Compliance Officer. The Compliance Officer performs an enhanced assessment to determine the level of risk and the legitimacy of the customer's source of wealth and source of funds. A relationship with a PEP may only be established or continued with prior written approval from Senior Management. The Compliance Officer documents the decision-making process, including the risk assessment, verification results, and rationale for accepting or rejecting the relationship. When a PEP relationship is approved, EDD measures are applied in accordance with this Policy.

4 Customer Due Diligence (CDD)

The Company applies Customer Due Diligence (CDD) measures to identify, verify, and understand the identity and activities of every customer with whom it establishes a business relationship. CDD procedures are applied in accordance with applicable legislation, and are designed to ensure that no relationship is established or maintained without proper verification. CDD measures are applied:

- When players engage in financial transactions equal to or above Cg. 4,000;
- carrying out occasional transactions above the monetary equivalent of Cg. 4,000;
- there is a suspicion of money laundering or terrorist financing; or
- the Company has doubts about the veracity or adequacy of previously obtained customer identification data.

4.1 Identification and Verification

The Company's CDD procedures require prospective customers to create a full profile at point of registration. Mandatory information required at registration stage includes:

- Full name;
- Date of birth;
- Permanent residential address;
- Valid identification document (passport, national ID card, or equivalent government-issued document); and

- Where applicable, verification of the Beneficial Owner for corporate customers or legal entities.

To complete the required customer identification and verification process, the Company asks its customers to upload a copy of valid identification documents. This request is sent to the customer's registered email address. If needed, the customer may also receive a phone call to help with the verification process. If the documents are in a different language, the Company will take necessary steps to ensure that the documents adequately prove the customer's identity, such as obtaining a translation of the relevant parts. This may involve asking the customer to submit documents with a certified true translation.

Only documents issued by government agencies that include a photograph are deemed reliable for verifying the customer's identity. A recent utility bill sent to your registered address, issued within the last 3 months or documents issued by the government that lack a photograph can be used to confirm the customer's current address, provided the address is included on the document.

If a document submitted by a potential customer does not meet the verification standards, the Compliance Officer or 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. If the customer cannot provide compliant documents within 30 days from the moment the Cg. 4,000 threshold is reached, the Company shall terminate the relationship with the customer and report the transaction to the FIU.

All actions taken in response to non-compliant documents must 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.

4.2 Purpose and Nature of the Business Relationship

The Company seeks to understand the intended purpose of each business relationship and the nature of the customer's expected gaming activity. This includes information on source of funds, typical transaction size, frequency of play, and use of payment methods.

Such information forms the baseline for the customer's risk profile and assists in identifying deviations that may indicate unusual or suspicious activity.

4.3 Simplified Due Diligence (SDD)

In low-risk scenarios, where the risks of ML/TF/PF are lower, SDD measures may be applicable, balancing the need for compliance with operational efficiency.

SDD is not permitted in situations involving:

- Politically Exposed Persons (PEPs);
- Customers from high-risk jurisdictions; or
- Any transaction involving funds or entities linked to sanctions lists or criminal activity.

The Compliance Officer reviews and approves all instances where SDD is applied, ensuring that justification is properly documented.

Such measures include but are not limited to:

- Not collecting specific information
- Verifying the identity of the customer and the beneficial owner after the establishment of the business relationship;
- Reducing the frequency of customer identification updates;
- Reducing the degree of on-going monitoring and scrutinizing transactions, based on a reasonable monetary threshold.

4.4 Enhanced Due Diligence (EDD)

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 senior management approval before establishing or continuing the relationship;
- Conducting independent verification of identity, source of funds, and source of wealth;
- Requesting supporting documentation for large or unusual transactions;
- Increasing the frequency of ongoing monitoring and account reviews; and
- Periodic re-verification of identity and risk profile.

4.5 Ongoing Monitoring

4.5.1 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.

4.5.2 Ongoing Transaction Monitoring

The Company shall perform 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.

4.6 Reliance on Third Parties to Perform CDD

The Company may rely on third parties to perform specific elements of CDD only where such reliance is permitted under Curaçao law and where adequate safeguards are in place to ensure that the third party complies fully with applicable AML/CTF/CPF obligations. Reliance on third parties does not exempt the Company from ultimate responsibility for compliance with its CDD and record-keeping obligations.

Reliance on a third party may be permitted only when all of the following conditions are met:

- The third party is itself a regulated and supervised institution under AML/CTF/CPF laws equivalent to those of Curaçao;
- The Company has obtained written confirmation that the third party will make available, without delay, copies of all identification and verification data, including beneficial ownership information, upon request;
- The arrangement is governed by a formal written agreement that clearly defines the roles, responsibilities, and information-sharing obligations of both parties; and
- The Compliance Officer has conducted a due diligence review confirming the third party's regulatory status, reputation, and competence before reliance is approved.

The Company retains full accountability for the integrity and completeness of all CDD information, even when reliance is placed on a third party.

If the third party fails to provide requested data promptly, or if deficiencies are identified, the Company shall immediately obtain the missing information directly from the customer and reassess the risk relationship.

Reliance on a third party shall be terminated immediately if:

- The third party ceases to be subject to adequate AML/CTF/CPF supervision;
- Material deficiencies are identified in its customer verification or reporting processes;
or
- The third party fails to provide data in a timely manner.

Any reliance terminated for non-compliance shall be documented, and where necessary, an Unusual Transaction Report (UTR) will be filed with the FIU Curaçao.

5 Reporting of Unusual Transactions

5.1 Reporting Obligations

The Company and its employees have a legal and regulatory obligation to identify and report any unusual transaction or attempted transaction that may be related to money laundering, terrorist financing, or proliferation financing.

All employees must remain alert to transactions or activities that appear inconsistent with a customer's known profile, account history, or declared purpose of play. The detection and reporting of unusual transactions form a key part of the Company's Anti-Money Laundering and Counter-Terrorist Financing framework.

5.2 Recognition of Unusual Transactions

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 following transactions or intended transactions are deemed unusual:

- a. Transactions which in connection with money laundering or terrorism financing are reported to the Police or to the Department of Justice;
- b. Transactions by or on behalf of a natural or legal person, a group or an entity, who is named on a list, adopted by virtue of the Sanctions National Ordinance (N.G. 2014 no. 55);
- c. Transactions in the amount of Cg. 5,000 or more, regardless whether the transaction is made in cash, by check or other form of payment, or through electronic or other non-physical means. This includes but is not limited to:
 1. A cashless transaction in the amount of Cg. 5,000 or more.
 2. Accepting or releasing a deposit in the amount of Cg. 5,000 or more at the request of the customer;
 3. Sale to a customer of chips in the amount of Cg. 5,000 or more. "Chips" include but is not limited to tokens and credits.
 4. A cash out in the amount of Cg. 5,000 or more;
- d. Transactions where there is cause to presume that they can be related to money laundering or terrorist financing.

5.3 Internal Reporting

All employees are required to immediately report any unusual or suspicious activity internally to the Compliance Officer using the Company's [Internal Disclosure Form](#).

Internal reports must be submitted within twenty-four (24) hours of detection or suspicion. Employees are strictly prohibited from investigating the matter further or discussing it with the customer.

The Compliance Officer maintains a secure register of all internal reports received, including the date, description, and action taken. Reports are kept strictly confidential.

5.4 Compliance Officer Review and Escalation

Upon receiving an internal report, the Compliance Officer promptly evaluates the information to determine whether it meets the criteria for external reporting under NORUT.

If the transaction qualifies as an objective indicator, the Compliance Officer must submit an UTR to the FIU Curaçao within forty-eight (48) hours of the transaction being executed, and the confirmation of submission must be retained by the Compliance Officer.

If the transaction qualifies as a subjective indicator, the UTR must be filed as soon as possible, but no later than ten (10) business days after the suspicion arises.

The Compliance Officer documents the rationale for each decision, including cases where a report is deemed unnecessary, and ensures that all supporting information and evidence are retained for at least five (5) years.

5.5 Prohibition of Disclosure

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

5.6 Record Keeping

The Company will retain 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.

6 Anti-Money Laundering Compliance Program

6.1 Appointment of a Compliance Officer

A senior compliance officer will be designated, responsible for overseeing the AML program and ensuring compliance with regulations.

6.1.1 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 Company'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 Company's efforts against money laundering and financing of terrorism and financing of proliferation.

6.2 Employee Screening and Training Programs

6.2.1 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.
- Is or has been subject to regulatory, court, or legal actions.
- Has leveraged bankruptcy laws for personal gain.
- 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.

6.2.2 Training

In delivering AML/CTF 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 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 matters will be provided in specific situations, including:

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

6.3 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/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.

7 Compliance and Consequences of Non-Compliance

123 Global Media B.V. is fully committed to complying with all applicable AML, CTF and CPF laws and regulations of Curaçao. Compliance with this Policy and related internal procedures is mandatory for all employees, officers, contractors, and business partners acting on behalf of the Company.

Every employee is individually responsible for understanding and adhering to this Policy, completing required training, and promptly reporting any unusual activity or suspicion of money laundering, terrorist financing, or proliferation financing to the Compliance Officer. Failure to comply with AML/CTF/CPF obligations — including failure to conduct due diligence, submit internal reports, or maintain confidentiality — may expose both the employee and the Company to regulatory or criminal sanctions.

Senior Management holds ultimate responsibility for ensuring that the Company's AML framework operates effectively and in accordance with Curaçao's legal requirements. Management must demonstrate a culture of compliance by supporting the Compliance Officer, allocating adequate resources, and ensuring that AML risks are effectively managed across all business areas.

Any employee who violates this Policy or fails to fulfill their AML/CTF/CPF obligations will be subject to disciplinary action, which may include:

- Formal warning or retraining;
- Suspension or reassignment;
- Termination of employment; and
- Where appropriate, reporting to law enforcement or regulatory authorities.

The Company applies a zero-tolerance approach to deliberate breaches, concealment of information, or any action that could compromise the integrity of the AML framework.

Non-compliance with Curaçao's AML/CFT/CPF legislation may result in administrative, civil, or criminal penalties, including substantial fines, license suspension, or criminal prosecution. The Curaçao Gaming Authority (CGA) and the FIU Curaçao may impose sanctions for failure to implement proper AML controls, inadequate reporting, or tipping-off violations.

8 Appendix I: Internal Disclosure Form

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:

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: