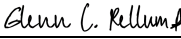


Anti-Money Laundering, Counter-Terrorism Financing, and Counter-Proliferation Financing (AML/CTF/CPF) Policy

Version History

Date	Ver.	Author	Summary Changes	Approved by Management
October 2024	1.0	Compliance Officer	Policy implementation	Signed by:  562CBB825608451...
January 2025	1.1	Compliance Officer	Policy revision to align with GCB AML Regulations	Signed by:  562CBB825608451...

o.b.o. the director

o.b.o. the director

Table of Contents

1.	<i>Introduction</i>	5
1.1.	AML, CTF and CPF Compliance Statement	5
1.2.	Legislative Framework	5
1.3.	Document Maintenance and Review	6
1.4.	Definition of Money Laundering	6
1.5.	Definition of Financing of Terrorism	6
1.6.	Definition of Financing of Proliferation of Weapons	7
2.	<i>The Risk-Based Approach</i>	8
2.1.	Explanation of the Risk-Based Approach	8
2.2.	Business Risk Assessment	8
3.	<i>Customer Acceptance Policy</i>	9
3.1.	Customer Risk Assessment	9
3.1.1.	Customer Risk	9
3.1.2.	Product/Service Risk:	9
3.1.3.	Geographic Risk:	10
3.1.4.	Delivery Channel Risk:	10
3.2.	Prohibited Accounts	10
4.	<i>Customer Due Diligence (CDD) Measures</i>	12
4.1.	Simplified Customer Due Diligence (SDD)	12
4.2.	Customer Due Diligence (CDD)	13
4.2.1.	Identification and Verification of the Player	13
4.2.2.	Identification and Verification of the Beneficial Owner	13
4.2.3.	Understanding the Purpose of the Business Relationship	14
4.2.4.	Timeline for Compliance and Non-Compliant Documents	14
4.3.	Enhanced Due Diligence (EDD)	15
4.4.	Targeted Financial Sanctions	16
4.5.	Politically Exposed Persons (PEPs)	16
4.5.1.	CDD Measures Specific to PEPs	17
4.6.	Business Affiliate and Supplier Diligence	18
4.7.	Reliance on Third Parties to Perform CDD	18
4.8.	Ongoing Monitoring	18
4.8.1.	Ongoing Customer Profile Monitoring	18
4.8.2.	Ongoing Transaction Monitoring	19
5.	<i>Reporting Unusual Transactions</i>	20
5.1.	Reporting Obligations	20
5.2.	Recognition of Unusual Transactions	20
5.3.	Prohibition of Disclosure	21

5.4. **Record Keeping**..... 21

6. ***Anti-Money Laundering Compliance Program***23

6.1. **Appointment of a Compliance Officer**..... 23

6.1.1. Duties of the Compliance Officer 23

6.2. **Employee Screening and Training Programs** 23

6.2.1. Employee Due Diligence 23

6.2.2. Training 24

6.3. **Independent Audit Function**..... 24

6.4. **Examination by the Gaming Control Board** 25

7. ***Appendix I: Country Risk List***26

8. ***Appendix II: Business Affiliate and Supplier Due Diligence***.....27

9. ***Appendix III: Internal Unusual Activity Report***.....28

1. Introduction

1.1. AML, CTF and CPF Compliance Statement

Media4 Curaçao N.V. (hereinafter the “Company”), being established in and governed by the laws of Curaçao, is committed to implementing robust policies to prevent money laundering (hereinafter “ML”), terrorism financing (hereinafter “TF”), and proliferation financing (hereinafter “PF”). In light thereof, the Company has developed a comprehensive Anti-Money Laundering, Counter Terrorism Financing and Counter Proliferation Financing (hereinafter “AML, CTF and CPF”) policy (hereinafter the “Policy”).

Adherence to this Policy is obligatory and vital to guarantee that 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.

1.2. Legislative Framework

The authorities in charge of the supervision of AML, CTF and 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:

- National Ordinance of the 20th of December 2024 Containing Rules concerning Games of Chance (National Ordinance on Games of Chance) (PB 2024, no. 157);
- Code of Criminal Law (Penal Code) (N.G. 2011, no. 48);
- National Ordinance on Identification of Customers when Rendering Services (NOIS) (N.G. 2017, no. 92), last update June 2024;
- National Ordinance on the Reporting of Unusual Transactions (NORUT) (N.G. 2017, no. 99), last update June 2024;
- National Decree penalties and fines reporting unusual transactions (N.G. 2021, no. 69), as amended by PB 2023, no. 6.;
- 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);
- 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 Decree for general measures, of the 10 July 2015, for the implementation of article 2 of the Sanctions National Decree containing implementation of the United Nations’ Security Council resolutions concerning Libya (Sanctions Ordinance Libya) (N.G. 2015 no. 28);
- National Decree for general measures, of the 10 July 2015, for the implementation of article 2 of the Sanctions National Ordinance, containing implementation of Resolutions 1695 (2006), 1718 (2006), 2087 (2013) and 2094 (2013) of the United Nations Security Council (Sanctions Decree People’s Democratic Republic of Korea 2015) (N.G. 2015 no. 30);
- National decree for general measures, of the 10th of July 2015, for the implementation of article 2 of the Sanctions National Ordinance, containing implementation of United Nations’ Security

Council Resolutions concerning Al-Qaeda c.s., the Taliban of Afghanistan c.s., ISIL c.s. ANF c.s. and persons and organizations to be designated locally (N.G. 2015, no. 29);

- Curaçao Gaming Control Board 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

1.3. Document Maintenance and Review

This Policy is designed to meet the legal requirements as outlined by the Curaçao Gaming Control Board (hereinafter the "GCB") and to foster a culture of compliance within our organization.

Regular reviews and updates will be conducted to adapt to evolving regulations and business needs. The maintenance and review of this document will take place annually.

1.4. Definition of Money Laundering

Money laundering (ML) is the process of concealing the true origins of illegally obtained funds, making them appear to originate from legitimate sources. ML 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.

1.5. Definition of Financing of Terrorism

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 ML, 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.

1.6. Definition of Financing of Proliferation of Weapons

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.

2. The Risk-Based Approach

2.1. 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/PF 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.

2.2. Business Risk Assessment

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

The Company performs thorough BRAs, evaluating potential risk factors related to customers, products and services, geographic locations, and delivery channels. Each risk factor is assessed for its likelihood and potential impact using both quantitative and qualitative data. Tailored controls and measures are then implemented to address these risks. All findings, evaluations, and mitigation strategies are documented and reported to senior management and relevant regulatory authorities.

BRAs are conducted regularly to maintain an accurate risk profile, with comprehensive assessments performed regularly. Additional assessments may be triggered by significant events, such as the introduction of new products, regulatory changes, or major shifts in the business environment.

3. Customer Acceptance Policy

3.1. Customer Risk Assessment

The Customer Risk Assessment assesses 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. The determination of the Customer Risk Rating is first assigned when a new customer applies for an account. This rating helps decide how often and in what way the customer will be reviewed in the future: the higher the risk, the more frequent and robust the ongoing monitoring of the customer would be. The risk assessment will categorize customers as low, medium, or high risk, with due diligence and ongoing monitoring applied proportionately.

For customers assessed as low risk, the Simplified Due Diligence process will be applied, insofar as the customer does not display any risk-increasing elements and remains below the threshold of NAf. 4,000.

For those assessed as medium or high risk, additional information and documentation will be required in accordance with this Policy.

Accounts classified as high risk or exhibiting potentially suspicious behaviors will be subject to review by compliance personnel and reported to the Compliance Officer (CO) for further investigation.

The Customer Risk Assessment process takes into consideration the following factors:

3.1.1. 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).

3.1.2. 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.

3.1.3. Geographic Risk:

This assessment considers the geographic location of the customer and the transaction, with countries that have weak AML, CTF and CPF 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 takes into account 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, CTF and CPF 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. See [Appendix I](#).

3.1.4. 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/PF 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.

3.2. 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 residing in any of the countries on the FATF list of High-Risk Jurisdictions subject to a Call for Action.
- 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 exclusion registers as stipulated by licensing conditions.
- Individuals who have been declared bankrupt, or have otherwise lost the control or disposal of all or part of his or her property.
- 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.

4. Customer Due Diligence (CDD) Measures

In accordance with the risk-based approach, a risk assessment regarding potential ML, TF and PF risks posed by the customer will be conducted during onboarding based on the information provided and established checks. The CDD measures to be taken are as follows:

- *Identifying* the player and *verifying* that customer's identity using reliable, independent source documents, data or information;
- *Identifying the beneficial owner* and taking reasonable measures to *verify the identity of the beneficial owner*, such that the Company is satisfied that it knows who the beneficial owner is. For legal persons and legal arrangements this should include understanding the ownership and control structure of the customer;
- Understanding and, as appropriate, obtaining information on the purpose and intended nature of the business relationship;
- Conducting *ongoing due diligence* on the business relationship and *scrutiny of transactions* undertaken throughout the course of that relationship to ensure that the transactions being conducted are consistent with the Company's knowledge of the player, its business and risk profile, including, where necessary, the source of funds.

4.1. Simplified Customer Due Diligence (SDD)

The Company collects identification information from each customer at the account registration stage. In cases where the risks of ML/TF/PF are deemed Low, the Company implements SDD measures that reflect this reduced risk in alignment with the risk-based approach that the Company adopts.

At a minimum the basic identification information includes the full name, date of birth and permanent residential address of the customer. Screening for Politically Exposed Persons (PEPs), and sanction checks is conducted at registration.

The Company may verify the identity of the customer and any beneficial owners after the establishment of the business relationship. While the basic identification details must be verified, the Company has discretion over the verification of any additional personal information. This should be based on the level of comfort and confidence that the Company has in knowing the customer. The extent of identity verification can be adjusted based on the perceived risk. In low-risk situations, casinos may use alternative reputable sources for verification, even if they lack photographic evidence (e.g., birth certificates, bank statements). If there are any concerns regarding the player's identity, further verification should be pursued.

The frequency of player identification updates may be reduced. As a general rule, updates should occur at least once every 3 years. If there are significant changes in the player's risk profile or activities, updates should be conducted sooner.

Ongoing monitoring of player transactions should be tailored to the assessed risk level. In low-risk situations, the degree of monitoring may be less intensive. Transactions should be scrutinized primarily based on reasonable monetary thresholds. Any transactions that exceed these thresholds or that appear unusual should trigger heightened scrutiny and potentially further investigation.

Simplified CDD measures are not permitted whenever there is suspicion of money laundering or terrorist financing, or where specific higher-risk scenarios apply, as laid out in this Policy.

4.2. Customer Due Diligence (CDD)

The Company has an obligation to undertake CDD measures when:

- players engage in financial transactions¹ equal to or above the monetary equivalent of NAf. 4,000;
- carrying out occasional transactions above the monetary equivalent of NAf. 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 player identification data.

4.2.1. Identification and Verification of the Player

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

- i. Full name;
- ii. Date of birth;
- iii. Permanent residential address;
- iv. Place of birth;
- v. Nationality; and
- vi. Identity number.

To complete the required customer identification and verification process, the Company asks its customers to upload a copy of valid identification documents (passport, identity card, driver's license or an equivalent document). This request is sent to the customer's registered email address. 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. Documents issued by the government that lack a photograph can be used to confirm the customer's current address, provided the address is included in the document. The Company accepts as proof of permanent residential address copy of utility bill (e.g. electricity, water, gas, telephone landline)² or bank statements, as long as they are not older than 6 months at the time they are received.

4.2.2. Identification and Verification of the Beneficial Owner

The Company is legally obligated to identify and verify the beneficial owner by confirming that customers are registering accounts to play and transact solely on their own behalf. This requirement is explicitly outlined in the terms and conditions on our website, which players must accept during the registration process. Furthermore, players must declare that they are not acting on behalf of any third parties.

The Company will not solely rely on this declaration. We are committed to actively monitoring player activity to detect any instances where a player may be using the account to play on behalf of others. This

¹ Financial transactions refer specifically to deposits and withdrawals, excluding bonuses. Wagered amounts and winnings fall under gambling transactions, which are not classified as financial transactions. To determine when a player reaches the monetary equivalent of NAf. 4,000 for CDD purposes, the Company will consider not only individual transactions but also any series, combination, or pattern of transactions that exceed this threshold. This calculation will be performed daily and will include all deposits and withdrawals made by the player, as well as any peer-to-peer transfers.

² Bills issued for mobile phone services are not acceptable, as they are generally not tied to a fixed location.

ongoing vigilance is essential to maintaining the integrity of our operations and ensuring compliance with AML-TF regulations.

To effectively manage this responsibility, the Company has implemented the following safeguards designed to prevent access to our services by individuals deemed suspicious. These safeguards include:

- Payment Method Verification: Ensuring that the payment method used for deposits is in the name to the player, insofar as possible.
- Denial of Service: Preventing transactions for players attempting to use payment methods not in their own name.
- Withdrawal Identity Verification: Confirming the identity of players before processing withdrawals.

4.2.3. Understanding the Purpose of the Business Relationship

While the primary purpose of a gaming account is clear, as part of our CDD measures, the Company must still collect relevant information to develop a customer risk profile. This involves:

- Establishing Source of Wealth: Understanding how a customer generates their net worth is crucial. Casinos must assess whether this source justifies the projected and actual level of account activity.
 - 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.
 - 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.

The extent of information collected must align with the risk rating identified during the CRA. For Low- and Medium-Risk customers the following measures may be applied risk-based:

- Information from open sources, including social media, can be a supplementary source for understanding a customer's profile.
- Obtaining a declaration from the customer detailing their nature of employment or business, along with their usual annual salary.

For High-Risk customers the following measures must be taken:

- Information provided by the customer must be substantiated by independent and reliable documentation. This could include tax returns, salary slips, or bank statements.
- The Company should collect comprehensive details about the sources of wealth to understand the financial background of high-risk customers.

To analyze and verify this information, the Company may take into account the average national income, average disposable income, and other relevant metrics to gauge expected wagering power based on jurisdiction, in consultation with the risk-based approach, whereby the extent of the mitigation will be based on the identified risks. The customer risk profile developed through this process serves as the foundation for the ongoing monitoring of player activity.

4.2.4. Timeline for Compliance and Non-Compliant Documents

If the customer cannot provide compliant documents within 30 days from the moment the NAf. 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

During the CDD process, customers may continue to access their accounts while the Company gathers the necessary information. However, if a deposit reaches the NAF. 4,000 threshold, 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 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.

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.

4.3. Enhanced Due Diligence (EDD)

The Company shall implement Enhanced Due Diligence (EDD) measures for customers identified as higher risk, with actions tailored to the specific risks identified during the assessment process. These measures aim to intensify monitoring of the business relationship to detect any unusual or suspicious transactions or activities. EDD is required in situations where the risk of ML, TF or PF is heightened.

In any case, the following scenarios are subject to EDD:

- *Products or transactions* that allow for a higher degree of anonymity, potentially facilitating illicit activities.
- *New products and new business practices*, including new delivery mechanism, and the use of new or developing technologies, or delivery mechanisms that may present unforeseen risks.

The measures applied during EDD must align with the identified risks and may include, but are not limited to:

- *Additional Customer Information:* Collect comprehensive information about the customer, including occupation, previous addresses, and relevant data from public databases and online resources.
- *Clarification of Business Relationship Intent:* Obtain further information regarding the intended nature of the business relationship to better understand the customer's gaming habits and expectations.
- *Source of Funds and Wealth:* Gather detailed information on the source of funds or wealth for the player. Examples include:
 - Personal savings
 - Employment income
 - Pension releases
 - Share sales and dividends
 - Property sales
 - Gambling winnings
 - Inheritances and gifts
 - Compensation from legal rulings

In higher-risk situations, the Company will periodically request SOF information, even if there has been no change in the customer's activity pattern. This ongoing diligence is essential for proactively addressing any potential concerns.

- *Transaction Purpose:* Ask for information regarding the reasons for intended or performed transactions to ascertain their legitimacy and ensure they align with the customer's profile.
- *Senior Management Approval:* Require approval from senior management before commencing or continuing the business relationship with higher-risk customers.
- *Enhanced Monitoring:* Implement increased scrutiny of the business relationship, which may involve more frequent reviews of transactions and account activities.
- *Account Verification for Initial Payments:* Require that the initial payment is made through an account in the customer's name with a bank that adheres to similar CDD standards.

4.4. Targeted Financial Sanctions

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 The Company's legal obligations. 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 ongoing 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 and confirmed, the Company must immediately proceed with freezing the funds of the particular customer(s), in accordance with the Sanctions Ordinance, and must 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, or otherwise, in light of tipping off considerations, follow instructions from the supervisory authority.

4.5. Politically Exposed Persons (PEPs)

A PEP is an individual who is entrusted with a prominent public function, other than middle ranking or more junior officials, including but not limited to the following individuals:

- heads of state, heads of government, ministers and deputy or assistant ministers,
- members of parliament or of similar legislative bodies,
- members of the governing bodies of political parties,
- members of supreme courts, constitutional courts or other high-level judicial bodies whose decisions are not subject to further appeal, except in exceptional circumstances,
- members of courts of auditors or of the boards of central banks,
- ambassadors, chargés d'affaires and high-ranking officers in the armed forces,
- members of the administrative, management or supervisory bodies of state-owned enterprises

- directors, deputy directors and members of the board or equivalent function of an international organization.

The following individuals are also regarded as PEPs by virtue of their relationship or association with the individuals listed above:

- family members of the individuals listed above, including spouse, partner, children and their spouses or partners, and parents
- known close associates of the individuals listed above, including individuals with whom joint beneficial ownership of a legal entity or legal arrangement is held, with whom there are close business relations, or who is a sole beneficial owner of a legal entity or arrangement set up for the benefit of the PEP.

4.5.1. CDD Measures Specific to PEPs

The Company implements appropriate risk management systems to identify whether a customer or beneficial owner is a PEP, or a relative or close associate of one. This includes, at first instance, conducting comprehensive screening against reliable databases and lists to determine the PEP status of new customers during the onboarding process.

No business relationship shall be established or continued with a PEP before obtaining senior management³ approval to service the PEP. This applies to new customers, ongoing relationships, and any occasional transactions.

In addition, the Company takes reasonable measures to ascertain the source of wealth and source of funds of the PEP. This involves:

- Requesting a statement from the PEP regarding their Source of Wealth.
- Verifying the statement through independent and reliable sources. Public sources will be consulted first, and if insufficient, additional documentation may be requested from the customer.

Additionally, the Company shall conduct enhanced ongoing monitoring of the business relationship, including analysis of the PEP's spending patterns to ensure they align with their declared legal sources of funds and the information on file.

In accordance with the risk-based approach that the Company employs, measures are tailored to the risk of the PEP, where the following are taken into consideration:

- the type of public function of the PEP;
- the country from which the PEP originates;
- the transactions that the PEP carries out.

PEP status screening will be conducted regularly throughout the business relationship. If a player who was not identified as a PEP at onboarding later becomes one, the Company is required to implement the enhanced due diligence measures outlined above within a thirty-day window of this determination. Failure to implement the required measures for newly identified PEPs within the specified timeframe will result in the termination of the relationship with that customer.

³ Senior management refers to individuals responsible for day-to-day operations or their immediate subordinates. Approval may also be sought from the Compliance Department manager.

4.6. 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, 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, CTF and CPF policies and procedures, proof of pertinent licensing or certification. The Compliance Officer will review these documents for their accuracy and completeness prior to entering into any agreements. See [Appendix II](#) for the form with the required information and due diligence documentation that might be requested from the potential third party to verify the legitimacy and suitability of the party.

4.7. Reliance on Third Parties to Perform CDD

The Company may engage third parties to fulfil certain elements of the CDD measures outlined in this Policy, excluding ongoing monitoring. The Company retains responsibility for monitoring the third party's compliance with CDD requirements and will maintain records of all outsourced CDD activities.

Before engaging a third party for CDD activities, the Company will conduct a thorough risk assessment of the third party. This assessment will include:

- Reviewing the third party's regulatory status and compliance history.
- Evaluating the third party's expertise and reputation in conducting CDD.
- Assessing the third party's internal controls and risk management measures.

The Company must ensure that the following criteria are met when engaging third parties for CDD activities:

- Information Acquisition: Obtain immediate access to CDD information (identification, purpose, risk assessment) from the third party.
- Documentation Agreement: Maintain an agreement allowing the Company to request identification data and relevant documentation.
- Regulatory Compliance: Verify that the third party is regulated and has effective AML/CTF compliance measures in place.
- Geographical Risk Assessment: Consider the country risk of the third party's jurisdiction.

The Company shall maintain comprehensive records of all CDD activities conducted by third parties, including:

- Copies of agreements with third parties.
- Documentation relating to the information provided by third parties.
- Records of any assessments or reports generated by the third parties.

4.8. Ongoing Monitoring

4.8.1. Ongoing Customer Profile Monitoring

During the periodic review of a customer, 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.

4.8.2. 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.

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).

5. Reporting Unusual Transactions

5.1. 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. See [Appendix III](#) for the Report form.

Employees are required to report any unusual activity to the Compliance Officer immediately using the Internal Unusual Activity Report form. The Compliance Officer will conduct a preliminary review of the reported activity within 24 hours to assess whether it requires further investigation.

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.

5.2. 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.

In accordance with the 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 Company fails to report internally identified transactions to the 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 pays 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 NAf. 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 NAf. 5,000.00 or more.
 - 2. Accepting or releasing a deposit in the amount of NAf. 5,000.00 or more at the request of the customer;
 - 3. Sale to a customer of chips in the amount of NAf. 5,000.00 or more. "Chips" include but is not limited to tokens and credits.
 - 4. A cash out in the amount of NAf. 5,000.00 or more;
- d. Transactions where there is cause to presume that they can be related to money laundering or terrorist financing.

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 NAf. 5,000.00 resets per game day of the user.

5.3. 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 FIU 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.

5.4. Record Keeping

The Company 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 ordered to do so by any enactment, rule of law or court order, the Company shall provide documents, 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.

6. Anti-Money Laundering Compliance Program

6.1. Appointment of a Compliance Officer

A senior compliance officer will be designated, independent from game operations, responsible for overseeing the AML program and ensuring compliance with regulations. The Compliance Officer will have timely access to customer identification data, CDD information, transaction records, and other relevant information.

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 prospect employees prior to their hiring for such roles, as well as 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.

Regular updates and re-evaluations are essential for maintaining an effective compliance program against ML, TF and PF. 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.

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.

6.2.2. 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.

6.3. Independent Audit Function

The AML program of the Company must be audited by a qualified independent party on a regular basis but at least once per year. The findings thereof must be documented and at a minimum must include an assessment of:

- 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.

6.4. Examination by the Gaming Control Board

The Company shall provide information and documentation regarding its money laundering and terrorist financing policies and procedures to examiners of the GCB 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.

7. Appendix I: Country Risk List

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.

High-risk countries include:

1. Afghanistan
2. Algeria
3. Angola
4. Belarus
5. Bosnia & Herzegovina
6. Bulgaria
7. Burkina Faso
8. Burma (Myanmar)
9. Burundi
10. Cameroon
11. Central African Republic
12. China
13. Côte d'Ivoire
14. Croatia
15. Cuba
16. Democratic People's Republic of Korea
17. Democratic Republic of the Congo
18. Guinea-Bissau
19. Haiti
20. Iran
21. Iraq
22. Kenya
23. Lebanon
24. Libya
25. Mali
26. Monaco
27. Mozambique
28. Namibia
29. Nicaragua
30. Nigeria
31. Pakistan
32. Panama
33. Philippines
34. Russia
35. Somalia
36. South Africa
37. South Sudan
38. Sudan
39. Syria

40. Tanzania
41. Trinidad and Tobago
42. Türkiye
43. Uganda
44. Ukraine (Crimea, Donetsk, Lugansk)
45. United Arab Emirates
46. Vanuatu
47. Venezuela
48. Vietnam
49. Yemen
50. Zimbabwe

Low-risk countries include:

1. Andorra
2. Armenia
3. Bhutan
4. Botswana
5. Czech Republic
6. Denmark
7. Estonia
8. Georgia
9. Grenada
10. Hungary
11. Luxembourg
12. Malta
13. Mauritius
14. New Zealand
15. Norway
16. Poland
17. Rwanda
18. Slovakia
19. Sweden
20. Uruguay

Excluded markets include, but are not limited to:

1. Afghanistan
2. Algeria
3. Aruba
4. Australia

5. Austria
6. Bahrain
7. Bangladesh
8. Belgium
9. Bonaire
10. Brunei Darussalam
11. Cambodia
12. China
13. Cuba
14. Curaçao
15. Czech Republic
16. Eritrea
17. France
18. Germany
19. Greece
20. Iran
21. Iraq
22. Israel
23. Jordan
24. Kuwait
25. Laos
26. Lebanon
27. Lithuania
28. Malaysia
29. Maldives
30. North Korea
31. Oman
32. Pakistan
33. Qatar
34. Saba
35. Saudi Arabia
36. Singapore
37. Sint Eustatius
38. Sint Maarten
39. Spain
40. Syria
41. the Netherlands
42. Turkey
43. United Arab Emirates
44. United Kingdom
45. United States of America
46. Vietnam

8. Appendix II: Business Affiliate and Supplier Due Diligence

Company information:

Registered name and legal form	
Registration number	
Date of incorporation	
Registered address	
Status	
Ultimate Beneficiary Owner (UBO)	
Persons with significant control (directors, members of supervisory board)	
Company website	

The documents below must be duly certified (where applicable) and, if they are not in the English language, provided with a legalized translation into a language understandable by the Company:

Document	Remarks
Memorandum & Articles of Association	
Certificate of Incumbency	
Excerpt from the Chamber of Commerce	
Company Structure	
Shareholders Register OR Declaration of Beneficial Ownership	
Copy passport of UBO(s) and director(s)	
Proof of address of the UBO(s) no older than 3 months	
Proof of Licensing	
AML/CFT/CFP Policy	
PCI DSS Attestation of Compliance	

Once the form is completed, please provide it, along with the relevant supporting documents and a copy of the pertinent agreement or contract, to the Compliance Officer for review.

9. Appendix III: Internal Unusual Activity Report

Internal Unusual Activity Report		
Date of report:		
Client ID:		
Date of account registration:		
Account status (Active/Suspended/Blocked):		
Risk rating:		
Account balance:		
Client details:	Full name:	
	E-mail:	
	Phone number:	
	Brand registration:	
	Date of birth:	
	Nationality/Country of registration:	
	Address:	
	CDD documents held:	< include document number and expiration date where available, provide copy of supporting documents to the CO >
Reason for reporting: If necessary, please use the additional information section:		< explain what activity / transaction gave rise to the report >
Date of unusual activity/transaction:		
Provide details (e.g. dates and amounts) of any known intended or pending transactions:		
Name (reporting employee):	Signature:	Date:
Upon completion, forward the form to the Compliance Officer as soon as possible.		