

Anti-Money Laundering, Counter-Terrorism
Financing, and Counter-Proliferation Financing
(AML/CTF/CPF) Policy
Media4 Curaçao N.V.

Table of Contents

1.	<i>Definitions.....</i>	5
2.	<i>Introduction</i>	7
2.1.	AML, CTF and CPF Compliance Statement	7
2.2.	Legislative Framework.....	7
2.3.	Purpose	8
2.4.	Document Maintenance and Review.....	8
3.	<i>Policy Implementation.....</i>	8
3.1.	Responsibilities of Senior Management.....	8
3.2.	Compliance Officer.....	9
3.3.	Employees.....	9
4.	<i>The Risk-Based Approach.....</i>	9
4.1.	Explanation of the Risk-Based Approach	9
4.2.	Business Risk Assessment	10
4.3.	Technology Risk Assessment	10
5.	<i>Customer Acceptance Policy.....</i>	11
5.1.	Customer Risk Assessment	11
5.1.1.	Customer Risk	11
5.1.2.	Product/Service Risk:	12
5.1.3.	Geographic Risk:	12
5.1.4.	Delivery Channel Risk:	13
5.1.5.	Assigning Customer Risk Score	13
5.2.	Prohibited Accounts	13
5.3.	Politically Exposed Persons	14
5.4.	Sanctions Screening.....	14
6.	<i>Customer Due Diligence (CDD) Measures</i>	14
6.1.	Customer Due Diligence (CDD).....	15
6.1.1.	Identification and Verification of the Player	15
6.1.2.	Identification and Verification of the Beneficial Owner	15
6.1.3.	Understanding the Purpose of the Business Relationship.....	16
6.1.4.	Timeline for Compliance and Non-Compliant Documents	16
6.2.	Simplified Customer Due Diligence (SDD).....	17
6.3.	Enhanced Due Diligence (EDD).....	17
6.4.	Business Affiliate and Supplier Diligence.....	18
6.5.	Reliance on Third Parties to Perform CDD	19
6.6.	Ongoing Monitoring	19
6.6.1.	Ongoing Customer Profile Monitoring.....	19
6.6.2.	Ongoing Transaction Monitoring	20

7.	<i>Reporting Unusual Transactions</i>	20
7.1.	Reporting Obligations	20
7.2.	Recognition of Unusual Transactions	20
7.3.	Prohibition of Disclosure	21
7.4.	Record Keeping	22
8.	<i>Termination of Business Relationship</i>	22
8.1.	Grounds for Termination	22
8.1.1.	Regulatory and AML/CFT/CPF Grounds	22
8.2.	Responsible Gaming and Player Protection	22
8.3.	Breach of Terms or Fraud	22
8.4.	Termination Procedure	23
8.4.1.	Internal Review and Approval	23
8.4.2.	Account Actions	23
8.4.3.	Regulatory Reporting	23
8.4.4.	Player Notification and Tipping-Off	23
8.5.	Record Keeping and Retention	23
8.6.	Business and Compliance Measures	23
9.	<i>Anti-Money Laundering Compliance Program</i>	23
9.1.	Appointment of a Compliance Officer	23
9.1.1.	Duties of the Compliance Officer	24
9.2.	Employee Screening and Training Programs	24
9.2.1.	Employee Due Diligence	24
9.2.2.	Training	25
9.3.	Independent Audit Function	25
9.4.	Examination by the Curaçao Gaming Authority	26
10.	<i>Compliance and Consequences of Non-Compliance</i>	26
10.1.	Employee and Third-Party Responsibilities	27
10.2.	Oversight and Enforcement	27

Document Information

Approval	Managing Director
Responsible Office	Compliance Officer
Review	Annually
Audience	All Employees, Contractors, and Third Parties
Effective Date	1 October 2025
Next Review Date	1 October 2026

Version History

Date	Ver.	Author	Summary Changes	Approved by Management
October 2024	1.0	Compliance Officer	Policy implementation	
January 2025	1.1	Compliance Officer	Policy revision to align with CGA AML Regulations	
September 2025	1.2	Compliance Officer	Policy alignment with CGA AML Policy template	

For any questions regarding this policy, please contact the Compliance Officer.

1. Definitions

"CGA"	Curaçao Gaming Authority
"CFATF"	means The Caribbean Financial Action Taskforce, an organization of twenty-four (24) states of the Caribbean Basin, Central and South America, which have agreed to implement common countermeasures to address money laundering.
The "Company"	means Media4 Curaçao N.V. (company number 164617, registered address Zuikertuintjeweg Z/N (Zuikertuin Tower), Willemstad, Curaçao) which is a holder of license number OGL/2024/1510/0839 from the CGA.
"Compliance Officer"	means a senior officer at management level and independent from the games' operations, responsible for the detection and deterrence of money laundering and terrorist financing.
"FATF"	means The Financial Action Task Force. An independent intergovernmental body, established in 1989 and mandated by its Member Jurisdictions to develop and promote policies to protect the global financial system against money laundering, terrorist financing and the financing of proliferation of weapons of mass destruction.
"FATF Recommendations"	means A framework of recommendations on policies and measures, issued by the FATF, to combat money laundering, terrorist financing and the financing of proliferation of weapons of mass destruction;
"Financial Transactions"	include the purchase or cashing in of casino chips or tokens, the opening of an account, wire transfers and currency exchanges. Financial transactions do not refer to gambling transactions that include only casino chips or tokens. Amounts wagered and winnings are considered as gambling transactions. Gambling transactions are not considered as financial transactions.
"Financing of proliferation (PF)"	is the provision of funds for the manufacture, acquisition, possession, development, export, trans-shipment, brokering, transport, transfer, stockpiling or use of nuclear, chemical or biological weapons and their means of delivery and related materials.
"FIU"	means the Financial Intelligence Unit Curaçao, referred to in art. 2 of the NORUT.
"Kingdom Sanctions Act"	means the National Ordinance also known as the "Rijkssanctiewet", published under N.G. 2016 no. 54.
"Money laundering (ML)"	is generally defined as engaging in acts designed to conceal or disguise the true origins of criminally derived proceeds so that the proceeds appear to have derived from legitimate origins or constitute legitimate assets. Money laundering may generally occur in three stages. Cash first enters the financial system at the 'placement' stage, where the cash generated from illegal or criminal activities is converted into monetary instruments, such as money orders or traveller's checks, or deposited into accounts at financial institutions. At the 'layering' stage, the funds are transferred or moved into other accounts or other financial institutions to further separate the money from its criminal origin. At the 'integration' stage, the funds are reintroduced into the economy and used to purchase legitimate assets or to fund other criminal activities or legitimate businesses.
"NOIS"	means National Ordinance on Identification of Clients when rendering Services (Landsverordening identificatie bij dienstverlening, N.G. 2017, no. 92).
"NORUT"	means National Ordinance on the Reporting of Unusual Transactions (Landsverordening Melding Ongebruikelijke Transacties, N.G. 2017, no. 99).

"Politically Exposed Persons (PEPs)"	means: Foreign PEPs are individuals who are or have been entrusted with prominent public functions by a foreign country and the direct family members or close associates of such persons. Examples are: Heads of State or of government, senior politicians, senior government, judicial or military officials, senior executives of state-owned corporations, important political party officials. Domestic PEPs are individuals who are or have been entrusted domestically with prominent public functions, for example Heads of State or of government, senior politicians, senior government, judicial or military officials, senior executives of state-owned corporations, important political party officials, and the direct family members or close associates of such persons. Persons who are or have been entrusted with a prominent function by an international organization refers to members of senior management, i.e. directors, deputy directors and members of the board or equivalent functions, and the direct family members or close associates of such persons.
"Sanctions National Ordinance"	means The National Ordinance also known as the "Sanctielandsverordening", published under N.G. 2014 no. 55.
"Source of Funds"	Refers to how the funds for a particular transaction were obtained by the player, like personal savings, pension release, property sales, share sales and dividends, gambling winnings, gifts, compensation from legal rulings.
"Source of Wealth"	is the origin of all the money a person has accumulated over their lifetime, like employment income, inheritances, investments, business ownership interests.
"Targeted financial sanctions"	are measures imposed by governments or international bodies to restrict the financial activities of specific individuals or entities linked to unlawful activities, such as terrorism or money laundering. These sanctions aim to prevent these parties from accessing the financial system. Unlike general sanctions that apply broadly to entire countries, targeted sanctions focus on specific individuals or entities. This approach minimizes the impact on the wider population while addressing particular risks. Targeted financial sanctions apply to individuals or entities listed on sanctions lists maintained by organizations like the United Nations or the European Union.
"Terrorism Financing (TF)"	refers to the provision of funds or financial support for terrorist acts, individuals, or organizations, and is characterized by the intent to intimidate populations or compel governments and international bodies to act or refrain from acting. Terrorist financing may not involve the proceeds of criminal conduct, but rather an attempt to conceal either the origin of the funds or their intended use, possibly for criminal purposes. Legitimate sources of funds are a key difference between terrorist financiers and traditional criminal organizations. In addition to charitable donations, legitimate sources include foreign government sponsors, business ownership and personal employment. Although the motivation differs between traditional money launderers and terrorist financiers, the actual methods used to fund terrorist operations can be the same as or similar to methods used by other criminals to launder funds. Funding for terrorist attacks does not always require large sums of money, such funding could be of cumulative nature over extended periods, and the associated transactions may not be complex.
"Unusual transaction"	A transaction that is considered as such on the basis of certain indicators, pursuant to Article 10 of the NORUT.
"(Ultimate) beneficial ownership (UBO)"	Refers to the natural person(s) who ultimately own(s) or control(s) a customer and/or the person on whose behalf a transaction is being conducted. It also incorporates those persons who exercise ultimate effective control over a legal person.

2. Introduction

2.1. 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.

2.2. Legislative Framework

The authorities in charge of the supervision of AML, CTF and CPF matters for the gaming sector are the Curaçao Gaming Authority (CGA) 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

2.3. Purpose

By implementing this Policy, the Company aims to ensure that all employees understand and fulfil their legal and regulatory obligations. The Company will apply a risk-based approach to customer due diligence, transaction monitoring, and the reporting of unusual activity. Additionally, this Policy seeks to foster a culture of compliance, transparency, and accountability across all levels of the organization.

From a business perspective, this Policy aims to protect the integrity of the Company's operations by preventing the platform from being exploited by criminal actors. It also seeks to safeguard the Company's reputation with customers, financial institutions, and regulatory authorities. Furthermore, maintaining eligibility for operating licenses and business partnerships is a key objective, as the Company demonstrates compliance with relevant regulations. Finally, this Policy is designed to ensure business continuity by mitigating the legal, financial, and operational risks associated with AML, CTF and CPF breaches.

2.4. Document Maintenance and Review

This Policy is designed to meet the legal requirements as outlined by the CGA 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.

3. Policy Implementation

The Company maintains internal controls consisting of structured policies and procedures designed to ensure efficient, compliant operations and to safeguard a secure and fair gambling environment for customers. With respect to money laundering and terrorist financing (ML/TF) risks, these controls are primarily implemented through the consistent application of the rules and procedures outlined in this Policy and in the applicable Regulations.

3.1. Responsibilities of Senior Management

Senior Management holds ultimate responsibility for the effectiveness of the Company's AML/CFT/CPF framework. Their duties include:

- Establishing and approving the core principles underpinning the prevention and mitigation of money laundering, terrorist financing, and proliferation financing.
- Appointing a Compliance Officer and communicating internal policies to them.
- Defining the Compliance Officer's duties and responsibilities.

- Ensuring that robust and adequate systems and controls are in place to achieve compliance with all relevant laws and regulations.
- Guaranteeing that the Compliance Officer has timely access to all data necessary for the effective execution of their role, including (but not limited to) customer identification data, transaction records, and other relevant information.
- Ensuring that all employees are informed of their obligation to report information relating to unusual transactions and are aware of the designated reporting line.
- Providing the Compliance Officer with sufficient resources, including qualified staff and appropriate technological tools.
- Reviewing and approving the annual compliance report, and ensuring that corrective action is taken to address any identified weaknesses or deficiencies.

3.2. Compliance Officer

The Compliance Officer must possess a thorough understanding of the Company's business model, associated risks, and the AML/CFT/CPF obligations established under the Regulations, as amended. Their primary responsibilities include:

- Monitoring the Company's ongoing compliance with AML/CFT/CPF requirements.
- Assessing internal and external risks relevant to the business.
- Overseeing AML/CFT/CPF-related employee communications and training.
- Reporting key findings, risks, and deficiencies in AML/CFT/CPF systems and procedures to the Company's management and senior executives.

3.3. Employees

The Company applies rigorous pre-employment and ongoing screening measures to ensure staff integrity and role suitability. These measures include identity verification, background and reference checks, and role-specific assessments where applicable. Enhanced screening procedures apply to employees in senior or sensitive positions.

The Company ensures that all employees receive AML training proportionate to their role and responsibilities. Training programs include:

- Induction training: mandatory for all new employees, covering AML/CFT/CPF principles, internal reporting procedures, and regulatory requirements.
- Annual refresher training: designed to maintain awareness and reinforce individual responsibilities.
- Ad hoc training: provided in response to regulatory changes, product updates, or identified compliance weaknesses.

The Compliance Officer is responsible for maintaining a training register documenting attendance, content delivered, and (where applicable) testing results.

4. The Risk-Based Approach

4.1. 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.

4.2. 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.

4.3. Technology Risk Assessment

As part of its risk-based approach, the Company shall conduct a Technological Developments Risk Assessment to identify and mitigate any risks of money laundering (ML), terrorist financing (TF), or proliferation financing (PF) associated with new technologies.

Whenever the Company introduces or considers implementing new technology, a Responsible Person will be appointed to complete the Technology Risk Assessment Form. This assessment must be undertaken when any of the following apply:

- The development or launch of a new product.
- The introduction of a new delivery mechanism.
- The adoption of a new business practice, particularly where money and technology interact in a novel way (e.g., new payment channels, new methods of transferring funds, or changes in the payment infrastructure enabled by technological advances).
- The use of new technology to deliver existing or new services.

The Risk Assessment must address, at a minimum, the following considerations:

- Anonymity Risk: Does the technology increase the potential for customer anonymity?

- Cross-Border Exposure: Does it enable international payments, peer-to-peer transfers, or access across multiple jurisdictions?
- Licensing and Regulation: Are third-party providers (such as e-wallets) subject to effective regulation in reputable jurisdictions?
- Transaction Traceability: Can the Company maintain a transparent and auditable trail for all transactions?
- Volume and Velocity Risk: Could the product enable rapid or frequent transactions that facilitate layering or other ML techniques?
- Integration with Monitoring: Can the Company's AML systems capture, monitor, and analyse transactions from the new channel?
- Contingency and Response: Can the product be paused, suspended, or otherwise restricted immediately if misuse is detected?
- Periodic Reassessment: The risk profile must be reviewed at launch, again after ninety (90) days, and subsequently on an annual basis.

5. Customer Acceptance Policy

5.1. 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:

5.1.1. 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).

5.1.2. 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.

5.1.3. 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.

5.1.4. 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.

5.1.5. Assigning Customer Risk Score

After the assessment, customers are categorized as low, medium, or high risk. The level of due diligence and ongoing monitoring applied corresponds to their risk classification:

- For customers assessed as low risk, a Simplified Due Diligence process will be applied, provided they do not exhibit any risk-enhancing characteristics and their transactions remain below the threshold of Cg. 4,000.
- Medium and high-risk customers will require additional information and documentation in accordance with the Company's policies.
- Accounts classified as high risk or displaying potentially suspicious behaviour will be reviewed by compliance personnel and reported to the Compliance Officer for further investigation.

This structured approach ensures that the Company effectively identifies and mitigates the risks associated with its customers, aligning with regulatory expectations and promoting a robust AML, CTF and CPF compliance program.

5.2. 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.

5.3. Politically Exposed Persons

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

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

5.4. Sanctions Screening

The Company is committed to complying with targeted financial sanctions, which require the freezing of funds and assets of individuals and entities identified by the UN and EU as involved in terrorism or proliferation activities.

- Ongoing Monitoring: The Company will perform ongoing sanctions screening at key points, including during registration, withdrawal requests, and any changes to personal details or payment methods.
- Action on True Matches: If a true match is discovered, the Company will immediately freeze the funds of the affected customer and file a report with the Financial Intelligence Unit (FIU). Services will be terminated upon confirmation of the true match by the supervisory authority, and frozen assets will be held until further instructions are received.

6. 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.

6.1. 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.

6.1.1. 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.

6.1.2. 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.

6.1.3. 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.

6.1.4. 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.

6.2. 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.

6.3. 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.

6.4. 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.

6.5. 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.

6.6. Ongoing Monitoring

6.6.1. 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.

6.6.2. 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).

7. Reporting Unusual Transactions

7.1. 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.

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.

7.2. 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.

7.3. 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.

7.4. 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.

8. Termination of Business Relationship

The Company may terminate a player relationship where continuation would breach applicable law, expose the business to unacceptable risk, or otherwise be necessary to protect the player or safeguard the integrity of the platform. Termination is carried out in accordance with Curaçao AML/CFT/CPF obligations, the Company's Player Complaints Policy, and its Responsible Gaming Policy.

8.1. Grounds for Termination

8.1.1. Regulatory and AML/CFT/CPF Grounds

Failure to complete, or unsuccessful outcome of, Customer Due Diligence (CDD) or Enhanced Due Diligence (EDD) in accordance with NOIS/NORUT.

Suspicion of money laundering, terrorist financing, or proliferation financing, supported by submission of an Unusual Transaction Report (UTR) to FIU Curaçao.

Match against sanctions lists under the Sanctions National Ordinance or Kingdom Sanctions Act.

8.2. Responsible Gaming and Player Protection

The player is identified as a minor or otherwise vulnerable person as defined under LOK Article 1.1(h).

Player activates self-exclusion or is subject to operator-initiated exclusion under the Responsible Gaming Policy.

Evidence of problematic gambling behaviour where continued access would pose a risk to the player or others.

8.3. Breach of Terms or Fraud

Evidence of fraud, collusion, bonus abuse, or use of a third party to access the account.

Violation of civil or criminal law or use of the account for unlawful purposes.

8.4. Termination Procedure

8.4.1. Internal Review and Approval

The Compliance Officer documents the grounds for termination and supporting evidence.

Closures involving high-risk or regulatory issues require management approval.

8.4.2. Account Actions

The account is suspended with immediate effect.

Player balances are refunded to the original payment method within two (2) business days, unless funds are frozen under AML laws or FIU Curaçao directives.

The player is removed from all marketing and promotional lists.

8.4.3. Regulatory Reporting

All AML-related closures involving suspicious or unusual activity are reported to FIU Curaçao via goAML.

The CGA is not notified of routine closures. Notification is only provided where the termination forms part of a reportable incident, a regulatory request, or a compliance audit disclosure, in line with the B2C License Conditions and the LOK.

8.4.4. Player Notification and Tipping-Off

Every termination is reviewed against the tipping-off prohibition under NORUT Article 12.

Decision-making process:

- The Compliance Officer assesses whether notifying the player could compromise an AML investigation or FIU report.
- If a tipping-off risk exists, notification is delayed or limited to operational wording (e.g., “account closed in accordance with terms”).
- The rationale is documented and retained in the compliance file.

8.5. Record Keeping and Retention

Termination records must include CDD/EDD documentation, the rationale for closure, supporting evidence, FIU reports (if applicable), and all internal approvals and communications. Records are retained for a minimum of five (5) years where termination relates to self-exclusion.

8.6. Business and Compliance Measures

All actions following account termination are executed in strict compliance with AML/CFT/CPF regulations and internal controls. Frozen funds are managed exclusively in accordance with FIU Curaçao instructions and applicable laws.

After closure, the Company actively monitors linked accounts, devices, and access points to prevent circumvention or unauthorized re-registration.

All account closures are aligned with the Player Complaints Policy and the Responsible Gaming Policy. Players retain the right to submit a complaint or escalate to Alternative Dispute Resolution (ADR) if they consider a termination unfair, unless restricted by tipping-off provisions under NORUT.

9. Anti-Money Laundering Compliance Program

9.1. 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.

9.1.1. 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.

9.2. Employee Screening and Training Programs

9.2.1. 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.

9.2.2. 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.

9.3. 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.

9.4. Examination by the Curaçao Gaming Authority

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

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

10. Compliance and Consequences of Non-Compliance

The Company is fully committed to complying with all applicable laws and regulations on anti-money laundering (AML), counter-terrorist financing (CTF), counter-proliferation financing (CPF), and sanctions enforcement as established under Curaçao law, in line with international best practices, including the FATF Recommendations.

Compliance with this Policy is mandatory for all employees, officers, agents, and third-party service providers. Non-compliance may expose both the Company and individuals to significant legal, regulatory, and reputational risks, including:

- Administrative fines or penalties imposed by Curaçao authorities.
- Suspension or revocation of the Company's gaming license.
- Criminal liability in cases of willful or negligent violations.

Beyond legal risks, non-compliance may also cause serious reputational and operational consequences, including loss of customer trust, negative media attention, strained banking and business relationships, freezing of funds, restricted access to financial systems, and heightened regulatory scrutiny.

10.1. Employee and Third-Party Responsibilities

Employees must understand and comply with this Policy, complete mandatory AML/CTF/CPF training, and report any unusual activity or suspected breaches to the Compliance Officer.

Employees who violate the Policy may face disciplinary measures, ranging from formal warnings to suspension or dismissal for serious or repeated breaches, with potential referral to law enforcement.

Third-party providers found to be non-compliant may have their contracts or agreements terminated.

The Compliance Officer ensures that whistleblower protections are in place for all staff who report concerns in good faith.

10.2. Oversight and Enforcement

The Compliance Officer and Senior Management are jointly responsible for investigating suspected violations, determining appropriate disciplinary measures, and reporting material breaches to the competent authorities.

All enforcement actions, including investigations and disciplinary outcomes, are documented and periodically reviewed to strengthen the Company's compliance framework.