



Licensed and regulated by the Curaçao Gaming Authority

Licence Number OGL/2023/115/0092

**Preventions of Money Laundering & Terrorist Financing Policy
and Sanctions Policy
(collectively the “AML Policy”)**

Version 2.2.

December 2025

Revision Date	Version Number	Description	Approved Date by Management on:	Submitted to CGA on:
14.02.2024	1	Initial Drafting	14.02.2024	14.02.2024
09.07.2025	2	Comprehensive update, incorporating enhanced measures, detailed procedures, and regulatory requirements to ensure alignment with current best practices and compliance standards.	30.07.2024	30.07.2024
25.09.2025	2.1	Updating relevant legislative framework, expanding definitions section, alignment of UTR requirements, including employee screening and training, independent audit function, CGA supervision		
09.12.2025	2.2	Updates following CGA feedback		

Reviewed and Approved


 Guardian Corporation Curacao BV
 Type text here
 Corporate Director

TABLE OF CONTENTS

1.	POLICY STATEMENT	5
2.	PURPOSE	5
3.	AUDIENCE	7
4.	GENERAL DEFINITIONS	7
5.	POLICY IMPLEMENTATION	9
5.1.	Business Risk Assessment	10
5.2.	Customer Risk Assessment	10
5.3.	Customer Acceptance Policy	13
5.4.	Customer Due Diligence	14
5.5.	Ongoing Monitoring	27
5.6.	Reliance on third parties to perform due diligence	28
5.7.	Reporting of unusual transactions	29
5.8.	Anti-Money Laundering Compliance Program	32
5.9.	Employee Screening and Training Programs	33
5.10.	Independent Audit Function	34
5.11.	Examination by the Curaçao Gaming Authority	35
5.12.	Account Blocking Procedure	35
6.	COMPLIANCE AND CONSEQUENCES OF NON-COMPLIANCE	36
6.1.	Compliance Expectations	36
6.2.	Consequences of Non-Compliance	36
6.3.	Responsibility and Accountability	37
7.	RELATED INFORMATION	37
8.	CRYPTO USAGE RISK POLICY (THE “CRYPTO POLICY”)	37

8.1.	Purpose	37
8.2.	Scope	37
8.3.	Policies Principles	37
8.4.	Roles and Responsibilities	38
9.	CONTACT INFORMATION	39

x

1. POLICY STATEMENT

Medial N.V. (hereinafter referred to as the “**Company**”), is a limited company incorporated in Curaçao, offering its services as authorised and licensed by Curaçao Gaming Authority (the “**CGA**”). As a licensed entity, the Company is required by the CGA to issue in writing an “Anti-Money Laundering Policy” regarding its procedures on prevention of money laundering, terrorist financing and financing of proliferation of weapons of mass destruction.. The policies and procedures detailed in the Policy ensure the compliance of all the employees of the Company and other relevant persons with the obligations of the CGA.

AML processes are designed to identify in advance all risks to the Company relating to money laundering and terrorist financing and to respond to these risks effectively. The Company’s main risks in relation to money laundering and terrorist financing arise from the establishment of business relationships with its clients and accepting their funds. The assessment and control of risk begins before acceptance of a client or an engagement and continues throughout its duration.

The Company and its employees are fully committed to implementing measures to prevent Money Laundering, Combat Terrorism Financing and Proliferation Financing. The Company is dedicated to its social responsibility in preventing its systems from being used as a tool for criminal activities. The Company strive to stay updated with developments in prevention measures to protect the organization, its operations, and reputation.

2. PURPOSE

The purpose of this Policy is to ensure that the Company adheres to the obligations and requirements outlined by Curaçao legislation, regulations, and rules concerning the prevention, identification, and reporting of money laundering or terrorist financing, that applies to all of its domains. This includes ensuring that adequate systems and controls are in place to mitigate risks posed to the Company and its Players, including the verification of, and due diligence checks on Players and their transactions. This Policy provides guidance for its employees to ensure that their knowledge and understanding of financial crime regulations are exemplary and outlines the expectations and their responsibilities under the regulations and objectives.

The Policy is developed and periodically updated by the Money Laundering Compliance Officer (hereinafter the “**MLCO**”) based on the general principles set up by the Company’s Board in relation to the prevention of Money Laundering and Terrorist Financing.

The Policy shall be communicated by the MLCO to all the employees of the Company that manage, monitor, or control in any way the Clients’ transactions and have the responsibility for the application of the practices, measures, procedures, and controls that have been determined herein.

The Policy has been prepared to comply with the provisions of the CGA.

To prevent financial crime and money laundering within our organization, the Company aims to meet the following objectives:

- (a) Establish and maintain policies, controls, and procedures to mitigate and effectively manage the risks of money laundering and terrorist financing;
 - (b) Train all staff to remain vigilant for the signs of money laundering;
 - (c) Follow due diligence and client identification procedures by all staff;
 - (d) Maintain controls and procedures to detect and report any unusual transaction;
 - (e) Conduct frequent risk assessments of all AML and terrorist financing controls and systems;
 - (f) Review and maintain Client verification and due diligence procedures;
 - (g) Implement procedures to enable the reporting of suspicions of money laundering;
- Abide by the Acts, legislation, regulations, and supervisory authority guidance for preventing financial crime, terrorist financing, and money laundering.

This Policy is designed to be compliant with the following Curaçao Ordinances and Decrees (the “Acts”):

- Code of Criminal Law (Penal Code) (N.G. 2011, no. 48);
- The National Ordinance on the amendment of the Penal Code (penalization of terrorism, terrorist financing, and money laundering) (N.G. 2008, no. 46).
- National Ordinance on the Reporting of Unusual Transactions (NORUT) (N.G. 2017, no. 99), last update June 2024;
- National Ordinance on Identification of Customers when Rendering Services (NOIS) (N.G. 2017, no. 92), last update June 2024.
- The National Decree containing general measures on the execution of articles 22a, paragraph 2, and 22b, paragraph 2, of the National Ordinance on the Reporting of Unusual Transactions (National Decree penalties and administrative fines for reporters of unusual transactions (N.G. 2010 no. 70)).
- 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 May 21, 2010, laying down the indicators, as mentioned in article 10 of the National Ordinance on the Reporting of Unusual Transactions (Decree Indicators Unusual Transactions) (N.G. 2010, no. 27).
- Sanctions National Ordinance (N.G. 2014, no. 55);
- Kingdom Sanction Act (N.G. 2016, no. 54);
- National Decree entering into force of Kingdom Sanction Law (N.G. 2017, no. 2);

- National Ordinance extension of validity sanction decrees 2018 (N.G. 2018, no. 34);
- National Ordinance of the 20th of December 2024 Containing Rules concerning Games of Chance (National Ordinance on Games of Chance) (PB 2024, no. 157);
- Curaçao Gaming Control Board Regulations for the combating of Money Laundering, the Financing of Terrorism and Proliferation of weapons of mass destruction, last update January 2025.

3. AUDIENCE

This Policy applies to all Employees, contractors, partners, and stakeholders involved in the acceptance, processing within the Company.

4. GENERAL DEFINITIONS

For the purposes of this Preventions of Money Laundering, Terrorist Financing & Proliferation Financing and Sanctions Policy (the “**Policy**”), unless the context shall prescribe otherwise:

“**Beneficial Owner**” means the natural person or natural persons, who ultimately own or control the Client and/or the natural person on whose behalf a transaction or activity is being conducted. The Beneficial Owner shall at least include in the case of legal entities, (i) the natural person or natural persons, who ultimately own or control a legal entity through direct or indirect ownership or control of a sufficient percentage of the shares or voting rights in that legal entity, including through bearer share holdings, a percentage of 25% plus one share be deemed sufficient to meet this criterion and; (ii) the natural person or natural persons, who otherwise exercise control over the management of a legal entity.

“**Brand(s) / “Domain(s)”** means the websites and associated platforms owned and operated by the Company, which have been duly approved by the Curaçao Gaming Authority These Domains are subject to Company’s oversight and adhere to the regulatory requirements and standards set forth by the CGA.

“**Business Relationship**” means a business, professional or commercial relationship which is connected with the professional activities of the Company, and which was expected, at the time when the contact was established, to have an element of duration.

“**Client(s) or “Player(s)”** means any physical person(s) aiming to conclude a Business Relationship or conduct a single transaction with the Company.

“**CGA**” means the Curaçao Gaming Authority.

“**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.

“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” is the provision of funds for the manufacture, acquisition, possession, development, export, trans-shipment, brokering, transport, transfer, stockpiling or use of nuclear, chemical or biological weapons and their means of delivery and related materials.

“FIU” means the Financial Intelligence Unit Curaçao, referred to in art. 2 of the NORUT.

“Money Laundering” 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 traveler'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.

“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” 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” is transaction that is considered as such on the basis of certain indicators, pursuant to Article 10 of the NORUT.

5. POLICY IMPLEMENTATION

The Company shall apply appropriate measures and procedures, by adopting a risk-based approach, so as to focus its effort on those areas where the risk of Money Laundering and Terrorist Financing appears to be comparatively higher.

Further, the MLCO shall monitor and evaluate, on an on-going basis, the effectiveness of the measures and procedures of this Policy.

The adopted risk-based approach that is followed by the Company, and described in the Policy, has the following general characteristics:

- recognises that the money laundering or terrorist financing threat varies across Clients, countries, services, and financial instruments;
- allows the Board to differentiate between Clients of the Company in a way that matches the risk of their particular business;
- allows the Board to apply its own approach in the formulation of policies, procedures, and controls in response to the Company’s particular circumstances and characteristics
- helps to produce a more cost-effective system;

The risk-based approach adopted by the Company, and described in the Policy, involves specific measures and procedures in assessing the most cost effective and appropriate way to identify and manage the Money Laundering and Terrorist Financing risks faced by the Company.

Such measures include:

- identifying and assessing the Money Laundering and Terrorist Financing risks emanating from particular Clients or types of Clients, financial instruments, services, and geographical areas of operation of its Clients;
- managing and mitigating the assessed risks by the application of appropriate and effective measures, procedures, and controls;
- continuous monitoring and improvements in the effective operation of the policies, procedures, and controls.

The application of appropriate measures and the nature and extent of the procedures on a risk-based approach depends on different indicators. Such indicators include the following:

1. geographical spread of the services and Clients
2. the nature (e.g. non face-to-face) and economic profile of Clients
3. the volume and size of transactions
4. the degree of risk associated with each area of services
5. the country of origin and destination of Clients' funds
6. deviations from the anticipated level of transactions
7. the nature of business transactions.

The MLCO shall be responsible for the development of the policies, procedures, and controls on a risk-based approach. Further, the MLCO shall also be responsible for the implementation of the policies, procedures, and controls on a risk-based approach.

5.1. Business Risk Assessment

The risk-based approach adopted by the Company involves the identification, recording and evaluation of the risks that have to be managed. The Company shall assess and evaluate the risks it faces, for the purpose of Money Laundering or Terrorist Financing. The particular circumstances of the Company determine suitable procedures and measures that need to be applied to counter and manage risk.

In the cases where the services that the Company provides are relatively simple, involving relatively few Clients or Clients with similar characteristics, then the Company shall apply such procedures which are able to focus on those Clients who fall outside the "norm".

The Company shall be, at all times, in a position to demonstrate to Regulator that the extent of measures and control procedures it applies are proportionate to the risk it faces for the purpose of Money Laundering and Terrorist Financing.

5.2. Technological Developments Risk Assessment

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

- The development of a new product;

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

When conducting a Technological Risk Assessment, the following must be addressed:

- Anonymity Risk: Does the new technology increase the ability for customers to remain anonymous?
- Cross-Border Exposure: Does it facilitate international payments, P2P transfers, or multi-jurisdiction access?
- Licensing/Regulation: Are third-party providers (e.g., e-wallets) regulated in reputable jurisdictions?
- Transaction Traceability: Can the Company maintain a clear audit trail for every transaction?
- Volume and Velocity Risk: Can the product allow rapid/frequent transactions that might facilitate layering?
- Integration with Monitoring: Can the existing AML software capture and analyse transactions from the new channel?
- Contingency & Response: If misuse is detected, can the product be paused or suspended immediately?
- Periodic Re-assessment: Review the risk at launch + ninety (90) days, and annually thereafter

5.3. Customer Risk Assessment

The following, *inter alia*, are sources of risks which the Company faces with respect to Money Laundering and Terrorist Financing:

(a) Risks based on the Client's nature:

- Age of the Clients such as minors (less than 18 years old), students or retired
- Clients engaged in transactions which involves significant amounts of cash
- Clients from high-risk countries or countries known for high level of corruption or organised crime or drug trafficking

(b) Risks based on the Client's behaviour:

- Client transactions where there is no apparent legal financial/commercial rationale
- Situations where the origin of wealth and/or source of funds cannot be easily verified
- Unwillingness of Clients to provide requested information
- Client with no or insufficient, control over his gambling behaviour

(c) Risks based on the Client's initial communication with the Company:

- non-face-to-face Clients
- Clients introduced by a third person.

5.3.1. Design and Implementation of Measures and Procedures to Manage and Mitigate the Risks

Taking into consideration the assessed risks, the Company shall determine the type and extent of measures it will adopt in order to manage and mitigate the identified risks in a cost-effective manner. These measures and procedures include:

- adaption of the Client Due Diligence Procedures in respect of Clients in line with their assessed Money Laundering and Terrorist Financing risk
- requiring the quality and extent of required identification data for each type of Client to be of a certain standard (e.g. documents from independent and reliable sources, third person information, documentary evidence)
- obtaining additional data and information from the Clients, where this is appropriate for the proper and complete understanding of their activities and source of wealth and for the effective management of any increased risk emanating from the particular Business Relationship
- ongoing monitoring of high-risk Clients' transactions and activities, as and when applicable.

In this respect, it is the duty of the MLCO to develop and constantly monitor and adjust the Company's policies and procedures with respect to the Client Acceptance Policy and Client Due Diligence and Identification Procedures of Sections 5.3. and 5.4. of the Policy, respectively, as well as via a random sampling exercise as regards existing Clients. These actions shall be duly documented and provided to the Regulator upon request.

5.3.2. Relevant International Organisations

For the development and implementation of appropriate measures and procedures on a risk-based approach, and for the implementation of Client Identification and Due Diligence Procedures, the MLCO and the Head of the Back-Office Department shall consult data, information and reports [e.g. Clients from countries which inadequately apply Financial Action Task Force's (hereinafter "**FATF**"), country assessment reports] that are published in the following relevant international organisations

- FATF – www.fatf-gafi.org
- The Council of Europe Select Committee of Experts on the Evaluation of Anti-Money Laundering Measures (hereinafter "MONEYVAL") – <https://www.coe.int/en/web/portal/home>
- The EU Common Foreign & Security Policy (CFSP)- https://commission.europa.eu/index_en
- The UN Security Council Sanctions Committees - <https://main.un.org/securitycouncil/en>

5.4. Customer Acceptance Policy

The Client Acceptance Policy (hereinafter the “**CAP**”), following the principles and guidelines described in this Policy defines the criteria for accepting new Clients and defines the Client categorisation criteria which shall be followed by the Company and especially by the employees who shall be involved in the Client account opening process.

The MLCO shall be responsible for applying all the provisions of the CAP. In this respect, the Head of the Customer Support Department shall also be assisting the MLCO with the implementation of the CAP, as applicable.

5.4.1. General principles of the CAP

The General Principles of the CAP are the following:

- (a) the Company shall classify Clients into various risk categories and based on the risk perception, decide on the acceptance criteria for each category of Client;
- (b) where the Client wish to proceed with withdrawal actions, they can proceed only after the relevant pre-account opening due diligence and identification measures and procedures have been conducted, according to the principles and procedures of the Policy.
- (c) all documents and data described in Section 5.4.11. of the Policy must be collected before accepting a withdrawal request.
- (d) no account shall be opened in anonymous or fictitious name(s)

5.4.2. Not Acceptable Clients

The following list predetermines the type of Clients who are not acceptable for establishing a Business Relationship with the Company:

- (a) Clients who fail or refuse to submit, the requisite data and information for the verification of their identity and the creation of their economic profile, without adequate justification;
- (b) Clients who are residents or linked to blacklisted jurisdictions from the FATF or other equivalent lists;
- (c) Clients who are linked or presented to Sanctions list as those periodically updated from time to time;

(d) **Vulnerable Clients:**

- i. Clients under the age of 18 cannot register with the Company.
- ii. Known problem gamblers that previously been excluded from any respective Domain. Records will be maintained by the Company's Customer Support Department of all current, attempted and past registrations.
- iii. Clients who have no, or insufficient control over their gambling behaviour because of which they are or threatens to become addicted to one or more Games of Chance and as a result may cause harm to themselves or to other people.
- iv. Clients that have been banned from playing any Game of Chance either by force or at their own request
- v. Client that has been declared bankrupt.
- vi. FATF list nationals

5.5. Customer Due Diligence

5.5.1. Application of Client Due Diligence and Identification Procedures

The Company shall duly apply Client identification procedures and Client due diligence measures in the following cases:

- (a) when establishing a Business Relationship and/or before the acceptance of withdrawal request.
- (b) when there is a suspicion of money laundering or terrorist financing, regardless of the amount of the transaction
- (c) when there are doubts about the veracity or adequacy of previously Client identification data.

In this respect, it is the duty of the MLCO to apply all the relevant Client Due Diligence Identification Procedures described in the Policy for the cases mentioned above. Furthermore, the Head of Customer Support Department shall also be responsible to collect and file the relevant Client identification documents.

Further, the MLCO shall be responsible to maintain at all times and use during the application of Client due diligence and identification procedures template-checklists with respect to required documents and data from potential Clients.

5.5.2. Transactions that Favour Anonymity

In the case of Clients' transactions where the Client is not present so as to verify the authenticity of his signature or that he is the real owner of the account or that he has been properly

authorised to operate the account, the Company applies reliable methods, procedures and control mechanisms over the access to the electronic means, so as to ensure that it deals with the true owner or the authorised signatory of the account.

5.5.3. Failure or Refusal to submit information for the verification of Clients' identity

Failure or refusal by a Client to submit, before the establishment of a Business Relationship the requisite data and information for the verification of his identity without adequate justification, constitutes elements that may lead to the creation of a suspicion that the Client is involved in money laundering or terrorist financing activities. In such an event, the Company shall not proceed with the continuation of the Business Relationship.

If, during the Business Relationship, a Client fails or refuses to submit, within a reasonable timeframe, the required verification data and information according to Section 5.4.11. of the Policy, the Company shall terminate the Business Relationship and closes the account of the Client while at the same time examines whether it is justified under the circumstances to submit a report to Unit, according to Section 5.1. of the Policy.

5.5.4. Time of application of the Due Diligence

With respect to the timing of the application of the Due Diligence and Client Identification Procedures, the MLCO shall be responsible for the application of the following provisions:

1. The verification of the identity of the Client shall be performed before the establishment of a Business Relationship.
2. By way of derogation from point (1) above, the verification of the identity of the Client shall be completed during the establishment of a Business Relationship if this is necessary not to interrupt the normal conduct of business and where the risk of money laundering or terrorist financing occurring is low. In such situations these procedures shall be completed as soon as possible after the initial contact and before any transactions are conducted.
3. Without prejudice of what is stated in paragraph (2) by way of derogation from paragraph (1), the verification of the identity of the Client may be completed during the establishment of a business relationship if this is necessary not to interrupt the normal conduct of business and where there is little risk of money laundering or terrorist financing occurring. It is understood that in such situations these procedures shall be completed as soon as practicable after the initial contact.

4. When commencing the establishment of a business relationship with a Client whose identity has not been yet verified, the risk may be assessed as low when, as a minimum, the following, among others, are taken into consideration:
 - If the verification of the Client's identity has not been completed, the cumulative amount of deposited/withdrawal funds should not exceed NAF 4,000 (approximately EUR 2,000)
 - The cumulative time in which the verification of the identity of a Client is completed, must not exceed 30 days from initial contact.
 - Within the timeframe of 30 days from initial contact, the regulated entity takes all reasonable measures to ensure that the percentage of Clients that have not complied with the request to submit verification documents, is considerably low (e.g. the regulated entity issues requests/reminders to the Client/beneficial owner informing them of their obligation to submit the requested documents for the verification of their identity).
 - Where the verification of the Client/beneficial owner's identity has not been completed during the designated timeframe of 30 days, the commencement of a business relationship must be terminated on the date of the deadline's expiry and all deposited funds must be returned automatically to the Client, in the same bank account from which they originated: the return of funds must occur immediately, regardless of whether the Client has requested the return of their funds or not. The returned funds (deposits) include any profits the Client has gained during their transactions and exclude any losses incurred.
5. In cases where the Company is unable to comply with Section 5.4.1.4. of the Policy, the Company shall not carry out any transaction through a bank account, establish a Business Relationship.
6. Identification procedures and Client due diligence requirements shall be applied not only to all new Clients but also to existing Clients at appropriate times, depending on the level of risk of being involved in money laundering or terrorist financing.

5.5.5. Linked Transactions Aggregation Requirement

In accordance with Sections III.1 and III.3 of the CGA Regulations, the Company shall aggregate all "linked transactions" to determine whether the ANG 4,000 (approx. EUR 2,000) threshold has been met for triggering mandatory CDD.

Transactions are considered linked when:

- they occur within a 24-hour period from the same Client;
- they are structured into smaller amounts to avoid CDD;
- they involve multiple wallets/accounts controlled by the same Client;
- they involve a series of deposits and withdrawals connected to a single gaming session.

Where aggregated transactions reach or exceed ANG 4,000, the Company shall:

- immediately perform full CDD on the Client (if not already completed);
- temporarily restrict withdrawals until CDD is completed;
- escalate any structuring indicators to the MLCO as potential unusual transactions.

The MLCO shall ensure that automated transaction monitoring systems include rules for detecting and aggregating linked transactions.

5.5.6. Construction of Economic Profile and General Client Identification and Due Diligence Principles

The construction of the Client's economic profile needs to include/follow the principles below:

- (a) the Company shall be satisfied that it's dealing with a real person, and, for this reason, the Company shall obtain sufficient evidence of identity to verify that the person is who he claims to be.
- (b) the verification of the Clients' identification shall be based on reliable data and information issued or obtained from independent and reliable sources, meaning those data, and information that are the most difficult to be amended or obtained illicitly
- (c) a person's residential and business address will be an essential part of his identity
- (d) the data and information that are collected during the Business Relationship, with the aim of constructing the Client's economic profile and, as a minimum, shall include the following:
 - the purpose and the reason for requesting the establishment of a Business Relationship
 - the anticipated account turnover, the nature of the transactions, the expected origin of incoming funds to be credited in the account and the expected destination of outgoing transfers/payments
 - the Client's size of wealth and annual income and the clear description of the main business/professional activities/operations
- (e) Client transactions transmitted for execution, shall be compared, and evaluated against the anticipated account's turnover, the usual turnover of the activities/operations of the Client and the data and information kept for the Client's economic profile. Significant deviations are investigated, and the findings are recorded in the respective Client's file. Transactions that are not justified by the available information on the Client, are thoroughly examined so as to determine whether suspicions over money laundering or terrorist financing arise for the purposes of submitting an internal report to the MLCO.

- 5.5.7. The said data and information are recorded in a separate form designed for this purpose which is retained in the Client's file along with all other documents as well as all internal records of meetings with the respective Client. The said form is updated regularly or whenever new information emerges that needs to be added to the economic profile of the Client or alters existing information that makes up the economic profile of the Client.
- 5.5.8. The Company shall apply each of the Client due diligence measures and identification procedures set out above but may determine the extent of such measures on a risk-sensitive basis depending on the type of Client. The Company shall be able to demonstrate to the authorities, upon request, that the extent of the measures is appropriate for the purposes of Money Laundering and Terrorist Financing.
- 5.5.9. For the purposes of the provisions relating to identification procedures and Client due diligence requirements, proof of identity is satisfactory if it is reasonably possible to establish that the Client is the person he claims to be.

5.5.10. Further Obligations for Client Identifications and Due Diligence Procedures

In addition to the principles described in above, the Company, and specifically the MLCO shall:

- (a) ensure that the Client identification records remain completely updated with all relevant identification data and information throughout the Business Relationship
- (b) examine and check, on a regular basis, the validity and adequacy of the Client identification data and information that he maintains, especially those concerning high risk Clients.

The procedures and controls stated in this Policy, also determine the timeframe during which the regular review, examination and update of the Client identification is conducted. The outcome of the said review shall be recorded in a separate note/form which shall be kept in the respective Client file.

Despite the obligation described above and while taking into consideration the level of risk, if at any time during the Business Relationship, the Company becomes aware that reliable or adequate data and information are missing from the identity and the economic profile of the Client, then the Company takes all necessary action, by applying the Client identification and due diligence procedures according to the Policy, to collect the missing data and information, the soonest possible, so as to identify the Client and update and complete the Client's economic profile.

In addition to the obligations above, the Company shall check the adequacy of the data and information of the Client's identity and economic profile, whenever an important transaction takes

place which appears to be unusual and/or significant compared to the normal pattern of transactions and the economic profile of the Client;

5.5.11. Source of Funds / Source of Wealth

The Company applies an additional due diligence measure in regard to deposits above NAF 4,000 (or equivalent to any currency). For the Company it is of major importance how the client acquired the monies he deposits. This reflects the Company's commitment to maintain the highest possible standards of business practice and to counter money laundering and the financing of terrorism. The Legal & Compliance Department shall examine the case and the client's profile and if considers that further information and clarifications are needed in regard to a particular deposit, will liaise with Client Support requesting from the client to:

1. Request proof as to the source of funds/wealth of the money deposited;
2. The relevant proof includes but not limited to documents like the below:
 - bank account statements in order to see his wealth
 - proof of dividends/profits if he has his own company,
 - payslips showing amounts that can justify so high deposits
 - or any other supporting documentation deemed necessary

5.5.12. Client Identification and Due Diligence Procedures:

With respect to the provisions of the Law, for Low-Risk Clients the Simplified Client Identification and Due Diligence Procedures shall apply. The Company may not apply the measures described in Section 5.4. of the Policy in the cases where the Client is categorised as a low-risk Client. Furthermore, where the Client is categorised as a low-risk Client, the verification of the identity of the Client may be completed during the establishment of a Business Relationship if this is necessary not to interrupt the normal conduct of business and where the risk of money laundering or terrorist financing occurring is low. In such situations these procedures shall be completed as soon as possible after the initial contact and before any transactions are conducted. The following documents shall be collected:

Physical Person

1. **Copy of a valid International Passport front and back side or**
 - (a) Copy of a valid ID or
 - (b) Copy of a driving license or

In case the residential address can't be verified with any of the above identification document, other documents must be requests such as:

2. Copy of a Utility Bill up to three (3) months' old

- (a) water / gas / electricity / telecommunications bills
- (b) bank statement
- (c) tax statement or local authority tax bill
- (d) governmental issued proof of address
- (e) rental agreement

3. Residence / Work Permit / Certificate of Registration

In case an EU client lives or works in another EU country, Residence/Work Permit is NOT required. In case an EU client lives or works in another country outside EU, we request a Residence/Work Permit or Visa from the country which the client is a resident. In case of a non-EU client who works or lives in an EU country or another non-EU country, we request a Residence/Work Permit or Visa from the country which the client is a resident.

Important: In cases where the Visa has been issued in other language except English, Client Support has to translate the relevant document and all documentation must be stored in English.

4. Extra documentation that can be requested (upon discretion)

- (a) Photo holding the Identification Document
- (b) Requiring the first payment from an account in a reputable jurisdiction
- (c) Using systems with codes returned via a verified phone

5.5.13. Identification and Verification of Beneficial Owners of Legal Persons

Where the customer is a legal person, the Company shall identify and verify the natural persons who ultimately own or control the entity. In accordance with NOIS and the CGA Regulations, the Company shall identify all natural persons who directly or indirectly hold 25% or more of the ownership or voting rights, or who otherwise exercise ultimate effective control over the legal person.

The Company shall obtain and verify the following information and documents:

- Certificate of Incorporation or equivalent;

- Register of shareholders or official corporate registry extract;
- Identification documents (ID + proof of address) for each natural person owning or controlling $\geq 25\%$;
- Identification documents for directors and authorized representatives;
- Documentation evidencing the authority of any person acting on behalf of the legal person.

Where no natural person can be identified as owning or controlling $\geq 25\%$, the Company shall identify and verify the senior managing official as the UBO.

Enhanced verification measures shall apply where the structure involves:

- Multi-layered or opaque ownership;
- Offshore or high-risk jurisdictions;
- Trusts, foundations, or nominee arrangements.

5.5.14. Enhanced Client Identification and Due Diligence Procedures

The Company when dealing with the High-Risk Clients shall apply the Enhanced Due Diligence and Monitoring procedures.

With respect to transactions or Business Relationships with people within the above category, the Company shall:

- have appropriate risk-based procedures to determine whether the Client falls under this category
- take adequate measures to establish the source of wealth and source of funds that are involved in the Business Relationship or transaction
- conduct enhanced ongoing monitoring of the Business Relationship.

Below are described due diligence, identification and enhanced monitoring procedures with respect to high-risk Clients:

5.5.15. Enhanced Account Monitoring

The Company has implemented an internal procedure whereby the Accounts of High-risk clients are reviewed in depth once every three months. The review is done jointly by the Client Support Department and the Compliance Officer.

The main aim of the review is to closely monitor the below 5 categories of clients and observe any deficiencies or discrepancies in their accounts:

- FATF list nationals
- High Deposit Clients (clients who deposit €2.000+)
- Politically Exposed Persons

- Clients marked as “Sensitive”
 - Unemployed
 - Students
 - Retired with Deposits more than €20.000 per year.

5.5.16. Enhanced Monitoring Procedure

The categories of clients are tagged (hereinafter the “**High risk clients**”) accordingly by the Customer Support Department in the Company’s CRM, so as to segregate their accounts from Medium or Low Risk clients. Based on the tags in CRM the following review of the four categories is done:

- A. Check the documents of all clients with the relevant tag
 1. If personal documents of the Clients are expired/missing/better copy is needed – the client is contacted to provide new documents.
 2. Unlike the UBs provided by Medium or Low Risk clients which have a validity period of 24 months as of the issue date, the UBs of High-Risk Clients have a validity period of 3 months after their issue date.
 3. The ongoing monitoring review is done again by the Company for the clients which is then reviewed
 4. Review the financial background of the clients in comparison to the total period deposits to see whether there is any unusual activity in the account comparing it to the economic profile of the client.
- B. When the above review is finished, a note with a short summary in the client’s profile in CRM is added in order to have a record of the reviews done on the client profile throughout his trading activity with the Company.

The note should be in the following form:

Regular check done:

Personal document – OK
 UB – OK
 World Check Report– OK
 Financial activities – OK

5.5.17. “Client accounts” in the name of a third person

The Company does not allow “client accounts” (e.g. omnibus accounts) in the name of a third person.

5.5.18. “Politically Exposed Persons” accounts

The Company does not allow Politically Exposed Persons accounts to be opened. Comprehensive screening against reliable databases will be conducted during the onboarding and periodically to determine PEP status.

(a) **PEP Identification**

Politically exposed person means a natural person both domestic and international who is or who has been entrusted with prominent public functions and includes the following:

1. Heads of State, heads of government, ministers and deputy or assistant ministers;
2. Members of parliament or of similar legislative bodies;
3. Members of the governing bodies of political parties;
4. Members of supreme courts, of constitutional courts or of other high-level judicial bodies, the decisions of which are not subject to further appeal, except in exceptional circumstances;
5. Members of courts of auditors or of the boards of central banks;
6. Ambassadors, chargés d'affaires and high-ranking officers in the armed forces;
7. Members of the administrative, management or supervisory bodies of state-owned enterprises;
8. Directors, deputy directors and members of the board or equivalent function of an international organization;

No public function referred to in points above shall be understood as covering middle-ranking or more junior officials. Individuals closely related to a PEP, for instance immediate family members and close associates, are also considered PEPs. PEPs are classified as a ML risk since they may be exposed to property that has been generated by corruption and bribery because of their position.

1. **Family members include the following:**

- a) the spouse, or a person considered to be equivalent to a spouse, of a politically exposed person;
- b) the children and their spouses, or persons considered to be equivalent to a spouse, of a politically exposed person;
- c) the parents of a politically exposed person.

2. **"Persons known to be close associates" includes the following:**

- b) any natural person who is known to have joint Beneficial Ownership of legal entities or legal arrangements, or any other close business relations, with a person referred to in point (1) above
- c) any natural person who has sole Beneficial Ownership of a legal entity or legal arrangement which is known to have been set up for the benefit de facto of the person referred to in point (1) above.

Establishing or continuing a Business Relationship with a PEP requires explicit, documented approval from Senior Management. The Company shall obtain credible and documented evidence of the Client's Source of Wealth and Source of Funds, including income

documentation, business ownership records, tax filings, or other independent verification. PEP relationships shall be formally reassessed at least annually or sooner if new risk factors arise.

The MLCO shall apply increased frequency and depth of monitoring, including:

- close review of transaction patterns,
- periodic updates of identification information,
- regular re-screening in the sanctions and PEP databases.

5.5.19. Clients from countries which inadequately apply FATF's recommendations

- a) The FATF 40+9 Recommendations constitute the primary internationally recognised standards for the prevention and detection of Money Laundering and Terrorist Financing.
- b) The Company does not accept Clients who are residents of countries which falls under the FATF list.
- c) The Company accepts Clients who are nationals of countries which falls under the FATF list BUT undertake the following measures:
 - i. exercise additional monitoring procedures and pay special attention to Business Relationships and transactions with persons, including companies and financial institutions, from countries which do not apply or apply inadequately the aforesaid recommendations
 - ii. transactions with persons from the said countries, for which there is no apparent economic or visible lawful purpose, are further examined for the establishment of their economic, business or investment background and purpose. If the Company cannot be fully satisfied as to the legitimacy of a transaction, then a unusual transaction report is filed to the Unit, according to Section 5.10 of the Policy.
 - iii. with the aim of implementing the above, the Head of the Back-Office Department and the MLCO shall consult the country assessment reports prepared by the FATF (<http://www.fatf-gafi.org>), the other regional bodies that have been established and work on the principles of FATF [e.g. Moneyval Committee of the Council of Europe (www.coe.int/moneyval)] and the International Monetary Fund (www.imf.org). Based on the said reports, the MLCO assesses the risk from transactions and Business Relationships with persons from various countries and decides of the countries that inadequately apply the FATF's recommendations. According to the aforesaid decision of the MLCO, the Company applies, when deemed necessary, enhanced due diligence measures for identifying and monitoring transactions of persons originating

from countries with significant shortcomings in their legal and administrative systems for the prevention of Money Laundering and Terrorist Financing.

A politically exposed person will cease to be deemed as having political exposure depending on an analysis by the MLCO.

5.5.25. Negative Media:

Negative media shall be deemed as information or intelligence, whether proven factual or alleged, related to serious financial crime, terrorism, fraud, narcotics, or any crime that has an element of or could lead to ML/FT. Negative Media screening is to be conducted when establishing a business relationship with a client. Instances where a client is connected to Negative Media, will be evaluated prior to granting a business relationship;

When analyzing Negative Media hits, the Company is looking at individuals that are both convicted and not fully convicted, meaning; allegations, cases under investigation pending the legal procedure, wanted individuals and any intelligence which gives rise to knowledge or suspicion that the client is involved with ML/TF;

Negative Media hits showing predicate offences of ML such as mafia, forgery, drug trafficking and fraud and terrorism amongst many others, shall be reported due to the sensitivity of the crime and the involvement of financial crime. Should any predicate offence raise concerns, they shall be raised with the MLCO accordingly.

Negative Media is categorized as follows:

- a) **Financial crimes:** financial crime covers a wide range of activities, including ML and the FT. It may also include fraud, bribery, or insider trading. Financial crime is a broad and complex criminal field that may be covered in both traditional and emerging media;
- b) **Violence:** violence involving Clients directly, or carried out on their behalf, may generate significant different types of adverse media, especially when part of a criminal enterprise. Violent crimes may be associated with political and workforce disputes, or wider patterns of human rights abuse;
- c) **Terrorism:** the financing of terrorism, any terror-related activities are liable to generate significant adverse media across a range of media outlets. Terror-related types of adverse media may range from the distribution of terrorist literature and encouragement to radicalization, to the direct perpetration of terrorist acts;

- d) **Fraud:** fraud can be perpetrated in numerous ways and includes fraudulent letters, telephone calls, emails, and websites. Fraud can be both a civil and criminal offence and, while the majority of cases involve improper financial gain, it may also involve property or immigration;
- e) **Narcotics:** narcotics crimes involve not only the use or sale of drugs but also drug production and trafficking. Narcotics offenses and associated news stories are often related to financial crimes, including ML and FT;
- f) **Cybercrime:** any criminal activity involving a computer or networked device like a phone or tablet may be considered cybercrime and reported as such. Cybercrime is an umbrella-term describing activities used to facilitate other offenses like digital financial crime, ML, fraud, and terrorism;
- g) **Regulatory crimes:** regulatory misconduct or non-compliance may constitute a crime in itself, or be an indication that clients are involved in other types of criminal activity. The types of adverse media stories relating to regulatory offenses frequently cross-over with financial crime;
- h) **Property crimes:** adverse media stories on property may involve activities such as burglary, theft, larceny, and arson, and constitute both civil or criminal misconduct. Property offenses may vary greatly in scope and be reported in a wide variety of news media formats;
- i) **Human Trafficking:** trafficking involves the transport of humans for the purposes of forced labour or sexual exploitation. A serious criminal offense, trafficking is often related to other offenses, including terrorism and various financial crimes;
- j) **Sexual crimes:** sexual crimes include a wide range of activity, from violence, abuse, and rape to the transmission or possession of illegal imagery. Sexual crimes are often in proximity to other offenses, including ML and cybercrime.

Any of the offences indicated above, whether convicted or alleged, shall be evaluated and terminated accordingly if the media is deemed to be a positive match.

5.5.26. Financial Sanctions & Sanctioned Individuals

The Company shall implement mechanisms to screen all Clients—at onboarding and on a daily ongoing basis—against all applicable sanctions lists, including those issued by the United Nations Security Council, the European Union, the Kingdom of the Netherlands, and any additional sanctions lists published by the Curaçao Gaming Authority.

The Company shall ensure that no funds or economic resources are made available, directly or indirectly, to or for the benefit of any designated person or entity.

If a Player is listed under any sanction, or Players who are directly or indirectly involved or the provenance of funds is from ownership, involvement or controlled by an individual seeking a business relationship with the Company, the following actions shall be conducted:

- a) All funds are to be frozen without delay and without prior notice, including financial assets and economic resources, whether owned directly or indirectly by a person or an entity, in line with the Process for the freezing of resources (Proces bevroezing van middelen);
- b) All those assets being financial or economic resources, are not to be made available to or for the benefit of the designated persons or entities;
- c) Any transactions in progress, whether incoming or outgoing, shall be immediately cancelled and blocked, ensuring that no further movement of funds can occur;
- d) If one suspects that a transaction, whether completed or attempted, is related to FT, he/she should immediately inform the MLCO by following internal reporting procedures;

If the MLCO knows, rather than suspects, that a transaction is related to property owned or controlled by or on behalf of a terrorist or a terrorist group, he/she should not complete the transaction and report it to the FIU Curaçao immediately.

The MLCO shall be responsible for the ongoing monitoring of sanctions lists and shall ensure that internal systems are updated immediately upon any amendments published by the CGA. No staff member shall notify or warn the affected Client of any freezing measure or the filing of an FIU report.

5.6. Ongoing Monitoring

5.6.1. General

The constant monitoring of the Clients' accounts and transactions is an imperative element in the effective controlling of the risk of Money Laundering and Terrorist Financing. In this respect, the MLCO shall be responsible for maintaining as well as developing the on-going monitoring process of the Company. The External Auditors shall review the Company's procedures with respect to the on-going monitoring process, at least annually.

5.6.2. Procedures

The procedures and intensity of monitoring Clients' accounts and examining transactions on the Client's level of risk shall include the following:

- (a) the identification of:
 - transactions which, as of their nature, may be associated with money laundering or terrorist financing

- unusual transactions that are inconsistent with the economic profile of the Client for the purposes of further investigation.
 - in case of any unusual transactions, the head of the department providing the relevant investment and/or ancillary service as well as the Head of the BackOffice Department shall be responsible to communicate with the MLCO
- (b) further to point (a) above, the investigation of unusual transactions by the MLCO. The results of the investigations are recorded in a separate memo and kept in the file of the Clients concerned
- (c) the ascertainment of the source and origin of the funds credited to accounts
- (d) the use of appropriate IT systems.
- (e) following the approval of a Physical Client and for the duration of the account operation, the Customer Support Department shall request from the Client new International Passport in case the existing identification documents become expired. In case the Client does not have International Passport, the national Identity Card with MRZ code together with the Driving License shall be accepted. If the Client does not have a Driving License, the Identity Card shall be accepted as the only identification document only if it has MRZ code. In case the Client does not respond within 4 weeks, a second email shall be sent as reminder including a warning of account “blocked” if another 2 weeks pass. In case the total of 6 weeks pass with no result, the account shall be “blocked” until the Client sends the required documents. Additionally, once every few months, depending on the Client categorisation, from the date of account opening, a new Utility Bill shall be requested from the Client.
- (f) following the approval of a Corporate Client and for the duration of the account operation, the Customer Support Department shall request once a year from the day of the account opening, Certificate of Good Standing or up to 3 months Bank Statement and a Board of Directors’ Resolution that the organizational structure of the Client did not change since the day of the account opening. In case the Client does not respond within 4 weeks, a second email shall be sent as reminder. If the Client does not respond, a third email shall be sent as reminder, but it shall include a warning of account “blocked” if another 4 weeks pass. In case the total of 12 weeks pass with no result, the account shall be “blocked” until the Client sends the required documents.

5.7. Reliance on third parties to perform due diligence

The Company may rely on third party providers for the implementation of Client identification and due diligence procedures, provided that:

- (a) The third party must be subject to AML/CFT supervision equivalent to Curaçao standards, including entities located within FATF-compliant jurisdictions
- (b) the third party provider makes immediately available all data and information, which must be certified true copies of the originals, that were collected in the course of applying Client identification and due diligence procedures

- (c) the Company applies the appropriate due diligence measures on the third party provider with respect to the procedures and measures applied from the third party provider for the prevention of Money Laundering and Terrorist Financing.

For the purposes of this Section of the Policy, third party providers refer to external entities or service providers engaged by the Company to assist with Client identification and due diligence procedures. These providers are relied upon to perform functions such as identity verification, screening against sanctions, PEP lists, and adverse media, and ensuring compliance with regulatory requirements.

The Company ensures that such providers are reputable, compliant with applicable data protection and AML regulations, and employ robust systems to conduct these procedures. While third-party providers are relied upon to perform these functions, the ultimate responsibility for compliance with AML obligations remains with the Company.

The MLCO or the appointed person shall assess and evaluate, the systems and procedures applied by the third-party provider for the prevention of Money Laundering and Terrorist Financing, as applicable

- (a) as a result of the assessment, the MLCO must be satisfied that the third-party provider implements Client identification and due diligence systems and procedures which are in line with the requirements of the applicable Laws.
- (b) the MLCO shall maintain a separate file for every third-party provider, where it stores the assessment report of point (a) and other relevant information
- (c) the commencement of the cooperation with the third-party provider and the acceptance of Client identification data verified by the third-party provider is subject to approval by the MLCO.

5.8. Reporting of unusual transactions

The Company takes any form of illicit activity very seriously. Predicate offences and illicit activity, including acts of money laundering (ML) and financing of terrorism (FT), as determined at the Company's sole discretion is strictly prohibited.

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 Cg. 5,000.00 or more, regardless of whether this transaction is carried out in cash, via a check or another payment instrument or electronically or in any other non-physical manner. This includes but is not limited to:
 - a A cashless transaction in the amount of Cg. 5,000.00 or more.
 - b Accepting or releasing a deposit in the amount of Cg. 5,000.00 or more at the request of the customer;
 - c Sale to a customer of chips in the amount of Cg. 5,000.00 or more. "Chips" include but is not limited to tokens and credits.
 - d A cash out in the amount of Cg. 5,000.00 or more;
- d) Transactions where there is cause to presume that they can be related to money laundering or terrorist financing.

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

Additionally, linked transactions that cumulatively reach or exceed Cg. 5,000 within a 24-hour period are considered for unusual transaction reporting in accordance with the Ministerial Decree on Indicators for Unusual Transactions (2015, no. 73).

Fraudulent activity that could give rise to a subjective report may include, but is not limited to:

- a) Stolen or black-listed wallets;
- b) Forgery of documentation;
- c) Collusion (for which such is not possible at the current stage of operation);
- d) The use of impermissible software tools to render the client anonymous;
- e) The provision of false registration data or other requested information;

- f) Any red flag identified above.

Where there is suspicion, knowledge or reasonable grounds to suspect that Clients are involved in fraudulent activity, money laundering, financial crimes or funding of terrorism will be reported to the appropriate authorities within the stipulated time frame, which is IMMEDIATELY UPON THE SUSPICION BEING RAISED via the Unusual Transaction Report (UTR). All personnel must have direct access to the MLCO.

Once a Unusual Transaction Report (UTR) has been escalated, it will be included in a UTR central repository within the Company. The Company shall at all times retain any UTR as follows:

- a) Reports raised to the FIU and;
- b) Reports not raised also hold information on why the report was not raised.

The Company may occasionally receive requests for information or notifications from regulatory authorities or law enforcement bodies regarding an investigation of a criminal, civil or regulatory nature. When such requests for information are received, these are to be forwarded in their entirety to the MLCO. The MLCO will handle and process these requests in line with the following process; the MLCO will:

- a) Record the receipt of such a request;
- b) Verify the legitimacy of the requesting organisation and individual making this request;
- c) Verify the legal basis under which such a request is made;
- d) Identify the Client (or Clients) accounts relevant to the request;
- e) Analyse the Client's information, including, amongst others, due diligence, transactions and ongoing monitoring information;
- f) Re-consider the Client's risk status considering the received request and take appropriate action depending on the case;
- g) Identify information that is relevant to the request and following a due assessment of the information, prepare and provide the information to the requestor; and
- h) Update the Company records in respect of such a request and where appropriate, notify the relevant regulators or authorities with follow-up actions as per relevant regulatory obligations.
- i) Reporting of unusual transaction or transactions and requests for information shall be done via the GOAML system by the MLCO.

Employees are required to report any unusual activity to the MLCO immediately, but no later than twenty-four (24) hours after the transaction has been executed, using the internal UTR form. If a more in-depth investigation is necessary, the Compliance Officer will complete this within ten (10)

business days. During this time, the MLCO may request additional information from relevant departments.

If the MLCO concludes that the activity is unusual, a report shall be submitted to the FIU Curaçao regarding any unusual monetary operations or transactions within forty-eight (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 forty-eight (48) hours after the transaction has been executed.

The MLCO can assign the reporting function to a Money Laundering Reporting Officer (MLRO), while retaining oversight over the quality of reported transactions and final approval of subjective reports.

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.

The MLCO will ensure that the following minimums are met concerning the information disclosed in any reports:

- a) Full details of the people involved.
- b) Full details of the nature of their/your involvement.
- c) The types of money laundering activity involved.
- d) The dates of such activities.
- e) Whether the transactions have occurred, are ongoing, or are imminent.
- f) Where they took place.
- g) How they were undertaken.
- h) The approximate and/or exact amount/s of money/assets involved.
- i) What has given rise to the suspicion.

5.9. Anti-Money Laundering Compliance Program

In accordance with Chapter V of the CGA Regulations, the Company's AML/CFT/CPF Program, including this Policy, shall be:

- approved by the Board of Directors,
- reviewed at least annually,
- updated whenever material changes occur, including regulatory amendments, business model changes, or new products or technologies.

The MLCO shall prepare an annual AML Report summarizing the effectiveness of internal controls, risk assessments, monitoring outcomes, and training activities. The Board shall review this report and ensure that any identified deficiencies are remediated in a timely manner.

The approved version of the Policy and all subsequent amendments shall be documented and retained for regulatory inspection.

The Company maintains a comprehensive Anti-Money Laundering (AML) Compliance Program that is risk-based and tailored to mitigate the risks associated with money laundering and terrorist financing. The program is designed to ensure that the Company's operations remain in full compliance with all applicable laws and regulatory requirements of Curaçao.

The AML Compliance Program includes the following core components:

- **Risk-Based Approach:** Identification and assessment of risks across clients, services, jurisdictions, and transactions to prioritize resources and apply appropriate levels of due diligence.
- **Policies and Procedures:** Implementation of formal, written policies that define roles, responsibilities, and controls to detect and prevent money laundering and terrorism financing.
- **Client Due Diligence (CDD):** Robust procedures for identifying and verifying clients, including enhanced due diligence for high-risk categories and ongoing monitoring of client activity.
- **Monitoring and Reporting:** Continuous monitoring of transactions and accounts to identify unusual patterns or anomalies. All employees are required to escalate unusual activity to the MLCO in accordance with internal reporting procedures.
- **Training and Awareness:** Ongoing AML/CTF training programs to ensure that all relevant employees are aware of the risks, obligations, and procedures.
- **Recordkeeping:** Maintenance of client identification and transaction records for a minimum of five (5) years in accordance with regulatory requirements.

5.10. Employee Screening and Training Programs

5.10.1. 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.

Any employee whose position may enable them to facilitate ML or TF must undergo screening. This requirement applies to prospective employees prior to their hiring for such roles, as well as current employees from time to time. Regular updates and re-evaluations are essential for maintaining an effective compliance program against ML, TF and PF.

To screen both current and potential employees, The Company will:

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

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.

5.10.2. Training

The Company provides AML, CTF, and CPF training based on each employee's role and responsibilities. Training covers what staff need to know and do to meet legal and policy requirements. We keep records of all training

- 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.

Training is updated regularly to reflect changes in laws, regulations, or company policies. Extra training will be given when:

- New rules are introduced
- New products or services change our risk exposure
- A breach happens due to lack of knowledge

5.11. **Independent Audit Function**

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

- Reviewing the Company's AML, CTF and CPF manual.
- Examining customer files.

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

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

5.12. 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.

5.13. Account Blocking Procedure

As part of the AML Compliance Program, the Company has established internal procedures for the immediate blocking of accounts under suspicion of involvement in money laundering or terrorist financing activities. If the MLCO, upon investigation or internal reporting, determines that there are reasonable grounds to suspect illicit activity, the following actions are taken:

- The account is promptly blocked to prevent further transactions;
- A Unusual Transaction Report (UTR) is prepared and submitted to the appropriate regulatory or law enforcement authority;
- Funds may be frozen in accordance with applicable laws and sanctions requirements;
- The business relationship may be terminated following internal escalation and legal review.

These actions are taken to ensure regulatory compliance and to protect the Company from legal, financial, and reputational harm.

6. COMPLIANCE AND CONSEQUENCES OF NON-COMPLIANCE

Medial N.V. is committed to maintaining full compliance with all applicable AML, CTF, and sanctions-related laws and regulations. Strict adherence to this AML Policy is mandatory for all employees, contractors, partners, and stakeholders. Non-compliance with the provisions outlined in this Policy poses significant legal, operational, and reputational risks to the Company.

6.1. Compliance Expectations

All employees and associated persons are expected to:

- Understand and comply with the AML Policy, procedures, and internal controls.
- Participate in ongoing AML training and awareness programs.
- Immediately report any unusual activities or breaches to the Money Laundering Compliance Officer (MLCO).
- Cooperate fully with internal investigations and any requests from regulatory authorities.

6.2. Consequences of Non-Compliance

Failure to comply with this AML Policy may result in severe consequences, which may include but are not limited to:

a) Internal Disciplinary Action:

- Verbal or written warnings;
- Suspension or reassignment of duties;
- Termination of employment or contract.

b) Legal and Regulatory Sanctions:

- Civil or criminal penalties including substantial fines and imprisonment;
- Regulatory sanctions or disciplinary measures imposed by the Curaçao Gaming Authority (CGA);
- Suspension or revocation of the Company's license.

c) Business and Reputational Risks:

- Loss of customer trust and confidence;
- Damage to the Company's brand and public image;
- Financial losses due to regulatory fines or terminated business relationships.

The Company maintains a zero-tolerance approach to intentional non-compliance. Any employee found to have knowingly facilitated, engaged in, or concealed illicit activities will be subject to immediate dismissal and referred to the appropriate legal authorities.

6.3. Responsibility and Accountability

All employees share the responsibility for compliance. The ultimate accountability for ensuring adherence lies with senior management and the MLCO. Supervisors are expected to foster a culture of compliance and proactively address any risks or violations.

7. RELATED INFORMATION

Additional documentation supporting the implementation of this Policy, including internal procedures, forms, guidelines, and references to relevant legal and regulatory frameworks, are available upon request.

To access these materials, please contact the Money Laundering Compliance Officer (MLCO). Availability of documents is subject to internal access control measures to ensure the confidentiality and integrity of sensitive compliance materials.

8. CRYPTO USAGE RISK POLICY (the “Crypto Policy”)

8.1. Purpose

This Crypto Policy establishes a framework for managing risks associated with the use of cryptocurrencies in Company’s operations, ensuring compliance with applicable laws and regulations, safeguarding company assets, and promoting responsible practices in the online gambling sector.

8.2. Scope

This policy applies to all Employees, contractors, partners, and stakeholders involved in the acceptance, processing, and management of cryptocurrencies within the Company.

8.3. Policies Principles

8.3.1. Risk Assessment

The Company shall conduct regular risk assessments to identify and mitigate risks related to cryptocurrency use, including financial, operational, and reputational risks. Also, the Company shall review risks associated with specific cryptocurrencies accepted by the Company.

8.3.2. AML / KYC Controls

Implement robust KYC procedures for Clients using cryptocurrencies, including identity verification and risk profiling.

Monitor transactions for unusual transaction and promptly report such activity to the appropriate authorities, in compliance with reporting obligations.

Utilize blockchain analytics tools to trace the origin and destination of funds.

8.3.3. Client and Transaction Monitoring

Set transaction thresholds and require enhanced due diligence for transactions exceeding predefined limits.

Maintain real-time monitoring of cryptocurrency transactions to detect anomalies or unusual activities.

8.3.4. Acceptance of Cryptocurrencies

Accept only pre-approved cryptocurrencies deemed secure and widely recognized.

Use secure wallets and custody solutions to manage company-held cryptocurrencies.

Convert received cryptocurrency to fiat currency promptly to minimize exposure to price volatility.

8.3.5. Data Security and Privacy

Secure all wallets and private keys using industry-standard encryption and multi-signature authentication.

Ensure the confidentiality of Client data in compliance with data protection regulations.

8.3.6. Employee Training

The Company shall train its Employees on cryptocurrency-specific risks, AML/CTF compliance, and the responsible use of cryptocurrencies in operations.

8.3.7. Third-Party Due Diligence

Vet and conduct due diligence on cryptocurrency payment processors, wallet providers, and other third-party service providers.

Require third parties to comply with this Crypto Policy and relevant regulations.

8.4. Roles and Responsibilities

8.4.1. Compliance Officer

Ensure adherence to this Crypto Policy and oversee cryptocurrency-related compliance efforts.

Act as the liaison with regulatory authorities for cryptocurrency matters.

8.4.2. Risk Management Department

Conduct risk assessments and implement mitigation measures.

Monitor and evaluate the effectiveness of cryptocurrency risk controls.

8.4.3. Employees

The Employees of the Company should read, acknowledge and comply with this Crypto Policy.

8.4.4. Incident Reporting and Response

Cryptocurrency-related security incidents, fraud, or AML violations should be reported to the MLCO by the Employee that identified such. MLCO should investigate the incidents promptly and take corrective actions if deemed necessary.

8.4.5. Recordkeeping

The Company shall maintain detailed records of cryptocurrency transactions, Client information, and risk assessments for at least five (5) years, which is calculated after the execution of the transactions or the termination of the Business Relationship.

9. CONTACT INFORMATION

For any questions regarding this Policy, please contact legal@medialnv.com

Appendix 1

Internal Unusual Report For Money Laundering and Terrorist Financing

INTERNAL UNUSUAL REPORT FOR MONEY LAUNDERING AND TERRORIST FINANCING

INFORMER'S DETAILS

Name:
Department:
Position:

CLIENT'S DETAILS

Name:
Address:
Date of Birth:
Tel: Occupation:.....
Passport No.: Nationality:
ID Card No.: Other ID Details:
Other information:

INFORMATION/SUSPICION

Brief description of activities/transaction:
.....

Reason(s) for suspicion:

.....
.....

Employee's / Informer's Signature

Date

.....

.....

FOR MLCO USE

Date Received:

Time Received:

Ref.

MLCO DECISION

.....
.....
.....
.....
.....

FILE NUMBER

Reported to the Unit: Yes/No

Date Reported:

Ref

MLCO SIGNATURE

DATE

.....

.....

Appendix 2

EXAMPLES OF SUSPICIOUS TRANSACTIONS/ACTIVITIES RELATED TO MONEY LAUNDERING AND TERRORIST FINANCING

A. MONEY LAUNDERING

1. Transactions with no discernible purpose or are unnecessarily complex.
2. Use of foreign accounts of companies or group of companies with complicated ownership structure which is not justified based on the needs and economic profile of the Client.
3. The transactions or the size of the transactions requested by the Client do not comply with his usual practice and business activity.
4. Large volume of transactions and/or money deposited or credited into, an account when the nature of the Client's business activities would not appear to justify such activity.
5. The Business Relationship involves only one transaction or it has a short duration.
6. There is no visible justification for a Client using the services of a particular financial organisation. For example the Client is situated far away from the particular financial organisation and in a place where he could be provided services by another financial organisation.
7. There are frequent transactions in the same financial instrument without obvious reason and in conditions that appear unusual (churning).
8. There are frequent small purchases of a particular financial instrument by a Client who settles in cash, and then the total number of the financial instrument is sold in one transaction with settlement in cash or with the proceeds being transferred, with the Client's instructions, in an account other than his usual account.
9. Any transaction the nature, size or frequency appear to be unusual, e.g. cancellation of an order, particularly after the deposit of the consideration.
10. Transactions which are not in line with the conditions prevailing in the market, in relation, particularly, with the size of the order and the frequency.
11. The settlement of any transaction but mainly large transactions, in cash.
12. Settlement of the transaction by a third person which is different than the Client which gave the order.
13. Instructions of payment to a third person that does not seem to be related with the instructor.
14. Transfer of funds to and from countries or geographical areas which do not apply or they apply inadequately FATF's recommendations on Money Laundering and Terrorist Financing.

15. A Client is reluctant to provide complete information when establishes a Business Relationship about the nature and purpose of its business activities, anticipated account activity, prior relationships with financial organisations, names of its officers and directors, or information on its business location. The Client usually provides minimum or misleading information that is difficult or expensive for the financial organisation to verify.
16. A Client provides unusual identification documents that cannot be readily verified.
17. A Client's home/business telephone is disconnected.
18. A Client that makes frequent or large transactions and has no record of past or present employment experience.
19. Difficulties or delays on the submission of the financial statements or other identification documents, of a Client/legal person.
20. A Client who has been introduced by a foreign financial organisation, or by a third person whose countries or geographical areas of origin do not apply or they apply inadequately FATF's recommendations on Money Laundering and Terrorist Financing.
21. Shared address for individuals involved in cash transactions, particularly when the address is also a business location and/or does not seem to correspond to the stated occupation (e.g. student, unemployed, self-employed, etc).
22. The stated occupation of the Client is not commensurate with the level or size of the executed transactions.
23. Financial transactions from non-profit or charitable organisations for which there appears to be no logical economic purpose or in which there appears to be no link between the stated activity of the organisation and the other parties in the transaction.
24. Unexplained inconsistencies arising during the process of identifying and verifying the Client (e.g. previous or current country of residence, country of issue of the passport, countries visited according to the passport, documents furnished to confirm name, address and date of birth etc).
25. Complex trust or nominee network.
26. Transactions or company structures established or working with an unneeded commercial way. e.g. companies with bearer shares or bearer financial instruments or use of a postal box.
27. Use of general nominee documents in a way that restricts the control exercised by the company's board of directors.
28. Changes in the lifestyle of employees of the financial organisation, e.g. luxurious way of life or avoiding being out of office due to holidays.
29. Changes the performance and the behaviour of the employees of the financial organisation.

B. TERRORIST FINANCING

1. Sources and methods

The funding of terrorist organisations is made from both legal and illegal revenue generating activities. Criminal activities generating such proceeds include kidnappings (requiring ransom), extortion (demanding “protection” money), smuggling, thefts, robbery and narcotics trafficking. Legal fund raising methods used by terrorist groups include:

- i. collection of membership dues and/or subscriptions
- ii. sale of books and other publications
- iii. cultural and social events
- iv. donations
- v. community solicitations and fund raising appeals.

Funds obtained from illegal sources are laundered by terrorist groups by the same methods used by criminal groups. These include cash smuggling by couriers or bulk cash shipments, structured deposits to or withdrawals from bank accounts, purchases of financial instruments, wire transfers by using “straw men”, false identities, front and shell companies as well as nominees from among their close family members, friends and associates.

2. Non-profit organisations

Non-profit and charitable organisations are also used by terrorist groups as a means of raising funds and/or serving as cover for transferring funds in support of terrorist acts. The potential misuse of non-profit and charitable organisations can be made in the following ways:

- i. Establishing a non-profit organisation with a specific charitable purpose but which actually exists only to channel funds to a terrorist organisation.
- ii. A non-profit organisation with a legitimate humanitarian or charitable purpose is infiltrated by terrorists who divert funds collected for an ostensibly legitimate charitable purpose for the support of a terrorist group.
- iii. The non-profit organisation serves as an intermediary or cover for the movement of funds on an international basis.
- iv. The non-profit organisation provides administrative support to the terrorist movement.

Unusual characteristics of non-profit organisations indicating that they may be used for an unlawful purpose are the following:

- i. Inconsistencies between the apparent sources and amount of funds raised or moved.
- ii. A mismatch between the type and size of financial transactions and the stated purpose and activity of the non-profit organisation.
- iii. A sudden increase in the frequency and amounts of financial transactions for the account of a non-profit organisation.
- iv. Large and unexplained cash transactions by non-profit organisations.
- v. The absence of contributions from donors located within the country of origin of the non-profit organisation.