

[Handwritten signature]
[Faint blue stamp]

Registered Address:
Media Entertainment N.V.
Emancipatie Boulevard 29 New Haven e-Zone, Curacao

Anti-Money Laundering Policy



Document Revision History
Author: Petar Mitkovski
Approving Official(s): Board of Directors

Version	Issue Date	Key Revisions
1.0	14 th May 2019	Initial Version Release
1.1	01 th Aug 2021	Update version due to 6th AMLD
1.2	11 th July 2024	Update version due to CGA
1.3	01 st April 2025	Update version due to New National Ordinance of game of chance and amended legislation

Approval	Board of Directors
Responsible Office	Compliance Officer
Review	Annually
Audience	All Employees, Contractors, and Third Parties
Effective Date	April 10, 2025
Next Review Date	May 30, 2026

Approved:

Table of Contents

1.	INTRODUCTION & STATEMENT	4
2.	OBJECTIVES	5
3.	COMMONLY USED TERMS AND DEFINITIONS	8
4.	POLICY IMPLEMENTATION	12
4.1.	RESPONSIBILITY OF THE SENIOR MANAGEMENT	12
4.2.	AML POLICY CHANGES AND IMPLEMENTATION REQUIREMENTS:	12
4.3.	COMPLIANCE OFFICER & MONEY LAUNDERING REPORTING OFFICER (MLRO)	12
5.	RISK BASED APPROACH	15
6.		17
6.1.	SERVICE RISK	17
6.2.	TRANSACTION RISK	17
6.3.	INTERFACE RISK	17
6.4.	GEOGRAPHICAL RISK	18
6.5.	CUSTOMER RISK	18
6.6.	CUSTOMER ACCEPTANCE POLICY	19
7.	CUSTOMER DUE DILIGENCE (CDD)	21
8.	ONGOING MONITORING	31
9.	RECORD KEEPING	33
10.	REPORTING OF UNUSUAL TRANSACTIONS	34
11.		36
11.1.	EMPLOYEE DUE DILIGENCE	36
11.2.	COMPLIANCE DEPARTMENT TRAINING	36
11.3.	TRAINING	36
11.4.	INDEPENDENT AML AUDIT	37
11.5.	EXAMINATION BY THE GAMING CONTROL BOARD	37
12.	COMPLIANCE AND CONSEQUENCES OF NON-COMPLIANCE	39
13.	CONTACT INFORMATION:	40
14.	RISK CLASSIFICATION	41
	AML COMPLIANCE PROGRAM	36
	BUSINESS AND CUSTOMER RISK ASSESSMENT	17

Anti Money Laundering Policy

1. INTRODUCTION & STATEMENT

Media Entertainment N.V. ("Media Entertainment") is a leading B2C Licensee under the Curaçao Gaming Authority (CGA) supplier of sports betting and casino games for online gambling industry. Media Entertainment N.V. (also referred as the "Company" or "we", "Licensee", "Operator", "Offside Gaming") is committed, a legal entity registered with company registration number 108625, and registered address at: Emancipatie Boulevard 29 New Haven e-Zone, Curaçao, to a comprehensive anti-money laundering (AML) program. It is the policy of the Company to prohibit and actively prevent money laundering and any activity that facilitates money laundering or the funding of terrorist or criminal activities by complying fully and completely with all applicable requirements under the various Bills and Regulations such as: Financial Action Task Force (FATF), Kingdom Sanction Act (The National Ordinance – Rijkssanctiewet), National Ordinance on Identification of Clients (NOIS), National Ordinance of Curaçao, The Caribbean Action Taskforce (CFATF) (NORUT) of Curaçao, Sanction National Ordinance of Curaçao, The Caribbean Action Taskforce (CFATF) recommendations and the international anti-money laundering and combating the financing of terrorism as well with financing proliferation of weapons and proliferation (AML/CFT) standards and frames of regulation and preventing the criminal activities of money laundering, financing of terrorism, using and involving money and funds from illegal and criminal activity into business and the life and economy.

Media Entertainment NV's AML policies, procedures and internal controls are designed to ensure compliance with all applicable FATF regulations and AML/CFT regimes and will be reviewed every year and updated on a regular basis to ensure appropriate policies, procedures and internal controls are in place to account for both changes in applicable law and changes in our business.

The Company is committed to the highest national and international AML and CFT standards when providing its Services and requires management and employees on all the Company's branches to follow these standards.

2. OBJECTIVES

Media Entertainment NV is committed to ensuring that complying fully and completely with all applicable requirements under the various Bills and Regulations such as: Financial Action Task Force (FATF), Kingdom Sanction Act (The National Ordinance – Rijkssanciewet), National Ordinance on Identification of Clients (NOIS), National Ordinance on the reporting of unusual transactions (NORUT) of Curacao, Sanction National Ordinance of Curacao, The Caribbean Action Taskforce (CFATF) compliance with anti-money laundering and counter terrorism financing legislation and good practice is embedded in all aspects of its business and operations.

The purpose of this policy is to establish the general framework of our Company for the fight against money laundering and terrorism financing throughout its business. We are committed to high standards of AML compliance and requires management and employees to adhere to these standards in preventing the use of its products and services for money laundering or terrorism financing purposes.

Accordingly, this policy sets the processes according to which Media Entertainment NV collects information about potential new business partners, end users' customers, how such information is assessed and reviewed and conclusions are made based on such assessment and review. It also provides for handling any AML concerns that may arise during the business relationship with any such third party, as well as record keeping and reporting issues.

The review of this Policy will be conducted on an annual basis by the Compliance Officer and will be approved by the board of directors.

It is the policy of Media Entertainment NV that all members of staff shall actively participate in preventing the services of the Company from being exploited by criminals and terrorists for money laundering purposes or used to fund a terrorist, or for any other illegal and or criminal action(s), activity whatsoever, stated and covered by Criminal Code activity through screening funds as being winnings obtained through betting on the company's website(s).

We seek to offer the highest security to all of our users/players and customers/partners/vendors/providers on our website(s) for that an account verification is done in order to insure the identity of our customers. The reason behind this is to prove that the details of the person registered are correct and the deposit methods used are not stolen or being used by someone else, which is to create the general framework for the fight against money laundering as well financing the terrorism and or any other illegal or criminal activity at all. We also take into account that depending on the nationality and origin, the way of payment and for withdrawing different safety measurements must be taken to mitigate and minimize the risk of illegal actions and potential breach of legislation which might occur malicious consequences.

Media Entertainment N.V. also puts reasonable measures in place to control and limit ML risk, including dedicating the appropriate means. Media Entertainment N.V. is committed to high standards of anti-money laundering (AML) according to the Curacao, but not limitedly, taking into consideration worldwide and the globalism itself, the complexity of migration and a flexible legal framework - a consequence of international legal relations and business relations between citizens and legal entities (companies and corporations) and not only, as well as international unions and associations such as EU/EEA guidelines, compliance and requires management & employees to enforce these standards in preventing the use of its services for any illegal and money laundering purposes.

The AML program of **our company** is designed to be compliant with:

• 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);

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

• Curacao 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 Recommendations of the Financial Action Taskforce on money laundering (FATF);

• Any other applicable law due to international market and country of origin;

This participation has as its objectives:

- ensuring Media Entertainment NV's compliance with all applicable laws, statutory instruments of regulation, and requirements of the relevant supervisory body
- protecting the company and all its staff as individuals from the risks associated with breaches of the law, regulations, and supervisory requirements and most important not being involved into illegal activities
- preserving the good name of Media Entertainment against the risk of reputational damage presented by implication in money laundering and terrorist financing activities
- making a positive contribution to the fight against crime and terrorism.
- prevent players/customers/users/partners/vendors/providers from being involved and or participate into illegal activity which might occur also to ML and FT.

To achieve these objectives, it is the policy of the Company that:

- every member of staff shall meet their personal obligations as appropriate to their role and position within the company
- commercial considerations shall never be permitted to take precedence over Media Entertainment's anti-money laundering (AML) commitments
- the company has appointed a Compliance Officer, and a designate employee to ensure continuation during his / her absence, and they shall be afforded every assistance and cooperation by all members of staff in carrying out the duties of their appointments. Any reference to Compliance Officer in this document, will include that of the designate employee should the Compliance Officer be temporarily absent.

3. COMMONLY USED TERMS AND DEFINITIONS

Money laundering

Money laundering is the common term for the process by which a person seeks to conceal the proceeds of crime by exchanging criminal property for so-called clean money. Activities associated with money laundering include:

- acquiring, using, or possessing criminal property;
- handling the proceeds of crimes such as theft, fraud and tax evasion;
- being knowingly involved in any way with criminal or terrorist property;
- investing the proceeds of crimes in other financial products or through the acquisition of property or assets;
- transferring criminal property; and financing of terrorist activities

The proceeds of crime or "criminal property" means any property which constitutes or comes to represent a person's benefit from criminal conduct. Criminal property (which also includes "terrorist property") can take any form: e.g. money, securities, tangible and intangible property, and money, whether or not it is "clean" money, which is used to fund terrorism.

Money laundering is (i) the use, conversion or transfer of property, knowing or suspecting that such property is derived from criminal activity or from an act of participation in such activity, including for the purpose of concealing or disguising the illicit origin of the property or for assisting any person who is involved in the commission of such an activity to evade the legal consequences of that person's actions; (ii) the concealment or disguise of the true nature, source, location, disposition, movement and/or rights with respect to, or ownership of, property, knowing or suspecting that such property is derived from criminal activity or from an act of participation in such an activity; (iii) the acquisition, possession or use of property, knowing or suspecting that such property was derived from criminal activity or from an act of participation in such an activity; (iv) participation in, association to commit, attempts to commit and aiding, abetting, facilitating and counselling the commission of any of the above.

Generally, money laundering occurs in three stages:

Placement: Cash generated from criminal activities is "placed" in the financial system or the retail economy, often by converting the cash into monetary instruments, such as money orders or travellers' checks, or deposited into accounts at financial institutions. To disguise the placement of unlawful funds, money launderers will often use a technique called "Structuring" or "Smurfing". Structuring involves the breaking up of a transaction that would normally have to be recorded or reported into smaller transactions which are below the recording/reporting thresholds.

Layering: Funds are transferred or moved into other financial institutions to further separate the money from its criminal origin. In this stage the money launderer is trying to disguise the trail leading to him/ to the crime by creating complex layers of financial transactions

Integration: Funds are reintroduced into the financial system and then integrated into the economy by purchasing legitimate assets or funding legal businesses.

Anti Money Laundering Offences

The phrase "money laundering" covers all procedures aimed to conceal the origins of criminal proceeds so that they appear to have originated from a legitimate source. This gives rise to three features common to persons engaged in criminal conduct, namely that they seek:

- to conceal the true ownership and origin of criminal proceeds;
- to maintain control over them; and

- to change their form.

Major AML offences include:

- Failing to report suspected money laundering;
- Tipping off about money laundering disclosures, a money laundering investigations and prejudicing money laundering investigations;
- Tipping-off is where an employee informs / gives a hint / warns somebody of being suspected / investigated in money laundering and therefore prejudicing an investigation. Tipping off is considered a serious crime as it can prevent investigations from running adequately, properly and to its full length;
- Concealing offence;
- Arranging offence;
- Acquisition, use or possession offence.

Businesses which are seen as likely targets for money launderers wishing to use them to channel the proceeds of crime include: solicitors; accountants; authorized Companies; money services businesses; high value dealers; and trust or company service providers.

There are number of obligations placed on these businesses, such as:

- a. the identification of customers;
- b. the appointment of a nominated individual to be responsible for reporting of suspicious persons and transactions;
- c. the implementation of systems and procedures to combat the use of their services by money launderers;
- d. ensuring that employees are aware of their obligations under the legislation.

Financing Terrorism

Terrorism financing is the act of providing financial support to terrorists or terrorist organizations to enable them to carry out terrorist acts or to benefit any terrorist or terrorist organization.

While funds may come from criminal activities, they may also be derived from legitimate sources, for example, through salaries, revenue from legitimate business or donations including through non-profit organizations.

Similar to money laundering, there are generally three stages in terrorism financing: raising, moving and using funds. Despite the different stages, the ways in which terrorism financing is done is similar and, in some cases, may be identical to the methods used to launder money. In both cases, the perpetrator seeks to misuse the financial or non-financial sectors for illegitimate purposes. is the provision or collection of funds and other assets by any means, directly or indirectly, with a view to, or in the knowledge that those means will be used in full or in part by a terrorist organization or by a terrorist acting alone, even without any connection to a particular act of terrorism. Unlike money laundering, terrorist financing is typically motivated by ideological, rather than profit-seeking concerns, and often may not involve the proceeds of criminal conduct, but an attempt to conceal either the origin of the funds or their intended use. Money laundering is frequently an important component of terrorist financing, and the methods used are often similar or identical to those used by money launderers.

Large sums are not necessarily involved, and terrorists rely on both legitimate and illegitimate sources of funding for operational, organisational, and administrative purposes. They can obtain funding through cultural and social events, different sponsors, corporate contributions, collection of memberships, donations as NGO and even legitimate business activities. Criminal activities generating such proceeds could include kidnappings, extortion, smuggling, thefts, robbery, and drug trafficking etc.

The goal of terrorist financing is to establish flexible sources of funding for the purchase of products and services that will be used to further or commit terrorist acts.

Financing of Proliferation of Weapons

Proliferation is defined by the Financial Action Task Force (FATF) as the illegal manufacture, acquisition, development, export, trans-shipment, brokering, transport, transfer, stockpiling or use of nuclear, chemical, or biological weapons and their means of delivery and related materials.

Proliferation financing is defined by the FATF as the provision of funds or financial services used for the manufacture, acquisition, development, export, trans-shipment, brokering, transport, transfer, stockpiling or use of nuclear, chemical, or biological weapons and their means of delivery and related materials (including both technologies and dual-use goods used for non-legitimate purposes), in contravention of national laws or, where applicable, international obligations.

Preventing proliferation financing is an important part of combating proliferation. It is essential to disrupt the financial flows available to proliferators and to obstruct and complicate the procurement of the illicit goods, services and technology needed for the development of weapons or mass destruction and their means of delivery. Financing of proliferation (FP) 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.

Politically Exposed Person (PEP) is a person in an influential and prominent political position operating within a domestic or foreign capacity. In their role as senior government officials, such people have access to resources and power that can influence government, policy, and people. The more senior the role person holds in government, the more exposure that person has to the people and resources that can influence or corrupt the laws that govern financial actions. Those that are politically exposed are more likely to have the opportunity to manipulate and misuse the financial system for illicit gain and personal advantage. A person that is a close family member of a PEP will also be considered a PEP

Targeted Financial Sanctions

The term targeted financial sanctions includes both asset freezing and prohibitions to prevent funds or other assets from being made available, directly, or indirectly, for the benefit of individuals, entities, groups, or organization who are sanctioned.

Sanctions are restrictive measures used to bring a change in another countries, corporations or individuals' activities, to protect international law, to prevent conflict, to maintain international peace or respond to emerging/current crises. Sanctions are also used to target terrorists and, for example, those involved in nuclear proliferation activities, weapons of mass destruction, arm trafficking etc.

These measures can apply to named individuals, entities or bodies, groups, sectors, or countries. Individuals and entities targeted by a sanction's regime are often referred to as "listed" or "designated."

The United Nations Security Council is the principal international sanctions-setting body. The European Union (EU) is an example of a regional sanctions setting body. Individual countries (such as Malta, UK, and others) also administer their own sanctions list, which again may target additional persons or entities.

Unusual Transaction Report (UTR) is a report, that can be internal, issued by an employee to the compliance department; or external – from the Compliance Officer to the applicable authorities: the Financial Intelligence Unit (FIU) Curacao), or any other and applicable authorities, all in accordance with the applicable legislation if that person has conclusion or intent that some illegal or criminal action has been taken and as a personal individual and responsive citizen decide to report to responsible authority.

4. POLICY IMPLEMENTATION

Our website(s) is/are operated by above mentioned company incorporated under the laws of Curaçao Media Entertainment N.V. has an application (OGL/2024/1110/0512) for a gaming license in progress with the Curaçao Gaming Authority. Until that process is concluded, based on a transitional arrangement outlined in the National Ordinance on Games of Chance (Landsverordening op de Kansspelen, P.B. 2024, no. 157), the company is permitted to continue its operations under this Certificate of Operation.

Policy implementation involves a risk-based approach to detect and mitigate ML/TF/FP risks. It includes Business Risk Assessment, Customer Risk Assessment, Customer Acceptance Policies, Due Diligence procedures, Ongoing Monitoring, and Reporting mechanisms. Detailed processes and responsible departments are outlined in the sub-sections below.

4.1. Responsibility of the Senior Management

The Senior Management is responsible for:

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

4.2. AML policy changes and implementation requirements:

Each major change of Media Entertainment NV AML policy is subject to approval by AML and Compliance Officer, approved internally by the general management of the Company and finally approved by CGA. The Company has appointed a Key Compliance Executive, Key Money Laundry Officer, experienced staff and employees, with proper education, knowledge and qualification which has on timely schedule participate into trainings and update of their qualifications and expertise.

4.3. Compliance Officer & Money Laundering Reporting Officer (MLRO)

Media Entertainment shall appoint a Compliance Officer who shall be in charge for the compliance with this policy and the overall adherence to the applicable AML legislation. The Compliance Officer and MLRO is to be knowledgeable of the applicable legislation and AML issues, risks and manners in which these are to be handled.

The Compliance Officer & MLRO shall be appointed by the CEO of Media Entertainment NV and shall report directly to him.

The Compliance Officer shall be provided with all resources required for the execution and implementation of its role in accordance with this policy.

The duties and responsibilities of the Compliance Officer include, but are not limited to, the following:

(i) **AML Program Development and Implementation:**

- Designing and implementing the AML program.
- Making necessary changes to the AML program.
- Ensuring compliance with Curacao laws and regulations regarding money laundering and terrorist financing.

(iii)

Policy and Procedure Oversight:

- Drafting and updating compliance policies and procedures to ensure alignment with legal and regulatory requirements.
- Overseeing and monitoring the implementation of compliance policies and procedures, and periodically reviewing their suitability, adequacy, and effectiveness, making changes as necessary.
- Reviewing adherence to the casino's policies and procedures.
- Designing internal procedures regarding the reporting of unusual transactions that may lead to blocking/freezing of user accounts.

(iiii)

Staff Training and Awareness:

- Organizing staff training sessions on compliance-related issues.
- Providing ongoing guidance, advice, and educational programs to improve staff understanding of compliance-related laws and regulatory requirements.
- Staying informed about local and international developments related to money laundering and terrorist financing and suggesting improvements to management.

(iv)

Transaction Monitoring and Reporting:

- Analyzing transactions and identifying those subject to reporting under the Ministerial Decree on Indicators for Unusual Transactions.
- Reviewing internally reported unusual transactions for completeness and accuracy.
- Maintaining records of both internally and externally reported unusual transactions.
- Conducting further investigations into unusual transactions if necessary.
- Preparing external reports on unusual transactions.

(v)

Reporting and Compliance Assessment:

- Preparing periodic reports on the casino's efforts against money laundering, terrorism financing, and proliferation financing.
- Liaising with applicable authorities in relevant jurisdictions to ensure compliance with regulations, including the filing of Unusual Transaction Reports (UTRs) as required.
- Reviewing, assessing, and overseeing new and existing employees in connection with AML issues to ensure compliance with AML policies.

(vi)

Strategic Direction:

- Providing strategic direction to management on compliance matters and suggesting improvements based on current regulatory trends.

Any change in the roles and/or identity of the Compliance Officer shall be promptly reported to the applicable authorities, but no later than 24 hours from such change occurring. The goal and main purpose of Media Entertainment N.V. is to prevent, protect and fully complying with the legislation and protect the law and mitigate risk of illegal actions which could bring to huge impact on economy and financial ground in the world. By violating the policies or disregarding money laundering will conclude to legal implications of all over the world or business risk in the future time being. This AML Policy and gardening it policies is to destroy and "work" as shield against criminal activities, which describes minimum standards of gardening

the own Media Entertainment's business and designated to comply with Curacao laws and regulations, but not only with and also international whereas applicable.

5. RISK BASED APPROACH

Media Entertainment NV implements a risk-based approach in its efforts to combat money laundering. Our diligence which is compatible with the risk level: the higher the risk, the broader due diligence is performed; the level of risk also affects the level and identity of the person / department handling and reaching resolutions in this matter. Following which, the Company collects the required information and documentation, analyses them and reaches a decision whether to enter into a business relationship with that third party.

The possibility to apply different measures on the basis of the particular ML/FT risks is a novel concept within the ambit of AML/CFT. The principle behind this is that resources should be directed proportionately in accordance with the extent of the ML/FT risks posed, so that the business, products and customers posing the highest risks receive the highest attention.

The risk-based approach is implemented following a risk assessment performed by Media Entertainment NV, intended to identify the various risks we face in the sphere of money laundering and terrorist financing, quantify the level of each risk and detail the various means in which these risks can be mitigated. This risk assessment, which is reviewed on an annual basis, is provided in a separate document.

We perform a due diligence process in respect of all its potential business partners. In addition, Media Entertainment NV performs a thorough due diligence process on its potential customers and, where applicable, Media Entertainment NV may perform such thorough due diligence on such other potential business partners as well, depending on the facts and circumstances, including, inter alia, the scope and nature of the transaction involved, the geographic location of such business partner and related people, the nature of intended activities of the business partner, information concerning the business partner and related people and certain attributes of the proposed transaction. The Company has preferred this approach over a rules-based approach that may lead to a 'tick box' approach with the focus being placed on meeting regulatory needs rather than on effectively combating money laundering. The application of a risk-based approach ensures that measures to prevent or mitigate money laundering are commensurate with the risks identified and that resources are allocated in the most efficient ways.

The steps that the Company will take to achieve this are to:

- identify the money laundering risks that are relevant to the Company;
- assess the risks presented by the Company's

- clients
- products
- delivery channels
- geographical areas of operation

- design and implementation controls to manage and mitigate these assessed risks; monitor and improve the effective operation of these controls; and record appropriately what has been done, and why

This risk based approach allows the senior management of the Company to apply its own approach to procedures, systems and controls, and arrangements that fit with the business of the Company and of its clients.

For identification purposes the levels of due diligence that will have to be undertaken will depend on the level of risk that Senior Management has assessed that the Company may be exposed to when dealing with or for a particular client.

From time to time the Compliance Officer may require additional information or actions be taken concerning clients or transactions that may not be set out in the published procedures, and Employees are expected to comply at all times with any such requirements.

6. BUSINESS AND CUSTOMER RISK ASSESSMENT

Media Entertainment N.V. adopts a risk-based approach, thereby focusing the company's efforts where they are most needed, and will have the most impact both in the short and long term. This approach allows for flexibility and significant discretion to be exercised by Media Entertainment N.V., but also entails significant responsibility. In this regard this policy lays out the specific steps which Media Entertainment N.V. will adopt so as to ensure that its conduct is in line with the Risk Based Approach in respect of considering and identifying those risks that directly impinge on money laundering and funding or terrorism. Please refer to the Risk Classification section for overview.

Media Entertainment N.V.'s business risk assessment, which is to be approved by the Board of Directors, takes the following factors into consideration:

6.1. Service Risk

Some services/transactions are more vulnerable to criminal exploitation than others. These include, for instance, services that allow the customer to influence the outcome of a game, be it one player alone or in collusion with others. During 21st century and development of IT and high technologies thus should be identified as risk as well of potential scam, fraud or illegal possibilities of disability.

6.2. Transaction Risk

Depending on the funding methods made use of, low/medium/high risk will be identified. The more transparency the funding method allows for, the lower the risk that will be identified. Conversely, for instance, the use of pre-paid cards will allow the player to make use of Media Entertainment N.V.'s service with a degree of or complete anonymity, and therefore the risk in that case is high. On the other hand, just by way of example, where customer transfers funds from a bank account or a card linked to a bank account held in his name with an institution established in a reputable jurisdiction, the risk of money laundering decreases. Some methods of payment/deposit/withdrawal used are higher risk than others, and being used more often for crime than others. Such as Credit/Debit cards, Media Entertainment N.V. is a Licensee and as such do not accept, and provide or support cash or physical payment methods. Another transaction risk is: anonymous and secured payment methods which hide the owner's personal data and transaction detailing for example pre-paid cards, virtual assets, vouchers.

6.3. Interface Risk

This refers to the channel through which Media Entertainment N.V. establishes a business relationship and/or through which transactions are carried out. Non-face-to-face interactions, such as in respect of Media Entertainment N.V.'s business interface, are no longer considered as automatically high risk, as long as technological measures, and controls to address the heightened risk of identity fraud or impersonation are adopted. Media Entertainment N.V. will make sure to adopt a good mix of verification methods, so as to counter the mentioned risks. Provision of additional identification documents will provide further proof that Media Entertainment N.V. was justified in considering that the customer is actually the person he alleges to be. As part of its risk-based approach, Media Entertainment N.V. has conducted an AML "Enterprise-wide risk assessment" to identify and understand risks specific to our brands and its business lines. The AML risk policy is determined after identifying and documenting the risks inherent to its business lines such as the services the website offers. The Users to whom services are offered, transactions performed by these Users, delivery channels used by the bank, the geographic locations of the bank's operations, customers and transactions and

other qualitative and emerging risks. The identification of AML risk categories is based on our understanding of regulatory requirements, regulatory expectations and industry guidance. Additional safety measures are taken to take care of the additional risks the world wide web brings with it. The "Enterprise-wide risk assessment is yearly reassessed. As Licensee – Operator Media Entertainment N.V. is providing only a online business to its customers and partners, vendors and business relationships. Thus, establishes a relationship through which transactions and funds are carried mostly online. Whereas such business impact to none-Tet-a-Tet basis and automatically being risk, apropos involving third parties, sometimes might identify fraud, or scam etc. which apparently is a risk considered to business. On daily basis where an involving of another (3rd) party between the customer and Media Entertainment N.V. is also identified as a risk.

6.4. Geographical Risk

This is the risk posed to Media Entertainment N.V. by the geographical location of the customers, however also the geographical locations of its suppliers and service providers. The element to be considered in respect of this anti-money laundering procedure is primarily that attributable to the customers and the source of funds of the said customers. The nationality, residence and place of birth of a customer should be taken into account as these might be indicative of a heightened geographical risk. Countries that have a weak anti-money laundering and counterfeited terrorism system, countries known to suffer from a significant level of corruption, and countries subject to international sanctions in connection with terrorism or the proliferation of weapons of mass destruction will be considered as high risk. Countries such as sanction by OFAC, FATF list, well-known non-governmental, non-approved and accepted by variety of Countries and jurisdictions as legitimate Constitutional Country with Government body, countries under increased monitoring, or Public stated countries by CFATF officially, countries identified as territory of concerns by US Department of State (CIA, FBI etc.), geo-locations on the EU Commission's list, countries identified by official sources for funding and supporting a terrorism, supporting guns and activities with such, corrupted countries. The opposite is also true and hence may be considered as presenting a medium or low risk.

6.5. Customer Risk

This relates to the type of customer being provided with the service. The assessment of the risk posed by a natural person is generally based on the person's economic activity and/or source of wealth. In identifying the level of risk inherent in a relationship, Media Entertainment N.V. will be assessing what would be the likelihood that a customer would be able to launder proceeds of crime through Media Entertainment N.V.'s service. A high earning customer who spends a fourth of his monthly wage in betting is not likely to constitute a high risk, even if the amount being bet is large. On the other hand, a minimum wage earner who spends his only wage on betting will more likely constitute a high risk. Furthermore, the individual will be screened so as to determine whether he is a politically exposed person (PEP), or in any way associated to a PEP. PEPs will not be accepted as players on Media Entertainment N.V.'s platform. Checks will also be carried out to ensure that the individual is not subject to any sanctions or other statutory measures. In order to determine whether the individual is a PEP or subjected to sanctions, Media Entertainment N.V. will make use of reliable electronic databases, and consult different trustworthy sources such as the sanctions list of the Financial Action Task Force (FATF) and the Office of Foreign Assets Control (OFAC). Another customer risk is funds arising from maintaining different sources of wealth, locations to the given person usually such as (business, entrepreneurship, regular employment jobs of a very few employers etc.) and direct correlation and his/her economy standard and way of living, including geographical location with relation to country of living standard of life and his own family and

siblings/relatives involved into household. Customers with multiple source of income are regular high risk, depend on source and case by case. Customers such as with irregular incomes also involved with geo-location and not only but limitedly whom doesn't have minimum 6 months period of income fall under the customer risk assessment observation. All high-level spenders fall into customer risk approach, Disproportional and illogical spenders as well in correlation to all facts, figures such as (age, country of living and origin, family members, age, etc.) which forward the conclusion of risk approaching and concluding to potential low-medium-high risk level of the case & it's customer. Under this framework are customers – tourists long term travellers and local players. Unknown and unidentified customers in very beginning with large amount of funds deposits/playing spending. Those remarks are the main triggers of identifying a customer risk as terms and general framework.

Risk assessments are 'works in progress.' Such assessments are to be constantly re-evaluated as new risks emerge. Risks may emerge due to changes in technology, which may render money laundering or the funding of terrorism attempts easier to carry out. Other examples include the widening of the customer-base or the addition of games and payment methods which present a different risk profile from those already offered, which will thus require a revision of the business risk assessment. In the absence of any such changes, Media Entertainment N.V. will re-assess its business risk assessment at least once a year, so as to evaluate whether any changes thereto are necessary. In determining the level of risk posed by a customer, the accumulation of all of the relevant indicators will be taken into consideration. These together, determine the player's risk profile contributing to the totality of a player's risk profile.

6.6. Customer Acceptance Policy

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. In alignment with our commitment to maintaining the integrity of our operations, the Company adopts a zero-tolerance stance towards financial crime and any illegal activities. We will not onboard customers who are engaged, directly or indirectly, in any form of illegal conduct. To uphold this standard, the Company implements various levels of due diligence to ensure all customers are reputable and compliant with applicable laws.

Prior to account creation, it is mandatory to conduct due diligence of potential customers to ensure they are not associated with financial criminal activities or barred from participation in the gaming industry. The Company will consider all relevant factors pertaining to the applicant's activities before granting access to our services.

Screening for Politically Exposed Persons (PEPs), and sanction checks is conducted at registration. Accounts in obviously fake or fictitious names will not be accepted.

the Company will accept customers only if they meet the following criteria:

- The applicant is a natural person, the Company does not accept companies or other legal entities.
- The applicant has read and agreed to the latest applicable terms and conditions, including privacy policies and other relevant policies.
- The applicant consistently complies with the terms and conditions.
- The applicant registers and transacts on any the Company platform on their own behalf.
- The applicant uses payment methods for which they are the legal and beneficial owner.
- The applicant is over 18 years of age.
- The applicant resides in a jurisdiction that is not prohibited.
- The applicant is satisfactorily identified and verified under the Company's AML compliance program and AML policy.

- The applicant meets due diligence requirements, including source of wealth and source of funds checks, where applicable.
- The applicant provides all requested information and documentation as per the Company's AML compliance program.
- The applicant is not:
 - Listed on any sanctions list from recognized authorities, including the UN, EU and OFAC.
 - Linked to jurisdictions subject to comprehensive sanctions.
 - Identified with a risk profile that exceeds the Company's risk tolerance.
 - Customers who refuse to comply with documentation requests or fail to provide required information within the prescribed timelines in this Policy.
 - Customers who submit false or forged documentation, including fictitious identities.
 - Customers of unknown identity or those whose identity cannot be verified.
 - Individuals attempting to create multiple accounts to evade due diligence requirements.
 - Customers with any suspicion of involvement in money laundering or terrorism financing.
 - Self-excluded customers who are barred from our websites or included in any national self-exclusion registers as stipulated by licensing conditions.

7. CUSTOMER DUE DILIGENCE (CDD)

The formal identification of customers on entry into commercial relations is a vital element, both for the regulations relating to money laundering and for the KYC policy. Customer due diligence/know your customer verification process and steps must be complete as soon as possible and if we identify and or suspect ML/FT actions, adequacy of obtain and collected personal data for identification of personal individual – player, and or if a player engage into financial transaction including and or but not limited to (deposit, wager, withdrawal, win, play etc.), and the threshold is reached out by player itself in the amount of and or over - **4000** (four thousand) Caribbean Guilders (Cg.) and or equal to this amount into any other currency whatsoever the Customer due diligence/KYC verification will be completed in reasonable timely manner. Additionally, to that Casino will conduct a PEP sanction screening on the player case by case.

Prior reaching the threshold of 4000 Cg. the player will be allowed to use his/her account, once reached the player will be asked for supportive documents to verify and identify himself and during this period of time he/she provides documents account will be put on hold till CDD process has been completed. If we do not receive in 30 days requested documents for proper CDD we are going to close account and forfeit money. If a suspicion of money laundering exists, an internal report will be submitted to the Compliance Officer for further assessment and potential FIU reporting.

This identification relies on the following fundamental principles:

A copy of the customer's passport, ID card or driving license, sometimes alongside a handwritten note mentioning six random generated numbers, and or if case by case scenario, also, a second picture with the face of the user/customer is required. The user/customer may blur out every information, besides date of birth, nationality, gender, first name, last name and the picture to secure their privacy. Please note that all four corners of the ID/Passport have to be visible in the same image and all details have to be clearly readable besides the name above. We might ask for all details if necessary. An employee may do additional checks, if necessary, based on the situation.

Proof of Address:

Proof of address will be done via different checks, which use two different databases. If an electronic test fails, the user/customer has the option to make a manual proof. A recent utility bill sent to your registered address, issued within the last 6 months or an official document made by the government that proves your state of residence and not older than 6 months. To make the approval process as speedy as possible, please make sure the document is sent with a clear resolution where all four corners of the document are visible, and all text is readable. For example: An electricity bill, water bill, bank statement or any governmental post addressed to you. An employee may do additional checks, if necessary, based on the situation.

Source of funds

thousand euro there is a process of understandings the source of wealth (SOW) Examples of SOW are:

- Ownership of business, source of business and funds
- Employment
- Inheritance
- Investment
- Family

It is critical that the origin and legitimacy of that wealth is clearly understood. If this is not possible an employee may ask for an additional document or prove. The account will be frozen if the same user deposits either this amount in one go or multiple transactions which amount to this. An email will be sent to them manually to go through the above and information on the website itself.

We also asks for a bank wire/credit card to further insure the identity of the user/customer. It also gives additional information about the financial situation of the user/customer.

Basic document for step one:

The basic document will be accessible via the setting page on our website. Every user must fill out the following information:

- First name
- Second name
- Nationality
- Gender
- Date of Birth

The document will be saved and created by an AI, an employee may do additional checks if necessary based on the situation.

Additional measurements.

In addition, an AI which is overseen by the AML Compliance Officer will look for any unusual behavior and report it right away to an employee of Media Entertainment N.V.

According to a risk based few and general experience the human employees will recheck all checks which are done before by the AI or other employees and may redo or do additional checks according to the situation.

In addition, a data Scientist supported by modern, electronic, analytic systems will look for unusual behavior like: Depositing and withdrawing without longer Betting sessions. Attempts to use a different Bank account for Deposit and Withdrawal, nationality changes, currency changes, behavior, and activity changes as well as checks, if an account is used by its original owner.

Also, a User has to use the same method for Withdrawal as he/she used for Deposit, for the amount of the initial Deposit to prevent any Money Laundering.

Enterprise-wide risk assessment

As part of its risk-based approach, **the Company** has conducted an AML "Enterprise-wide risk assessment" (EWRA) to identify and understand risks specific to and its business lines. The AML risk policy is determined after identifying the risks inherent to its business lines such as the services the website offers. The Users to whom services are offered, transactions performed by these Users, delivery channels used by the bank, the geographic locations of the bank's operations, customers and transactions and other qualitative and emerging risks.

The identification of AML risk categories is based on our understanding of regulatory requirements, regulatory expectations, and industry guidance. Additional safety measures are taken to take care of the additional risks the world wide web brings with it.

The EWRA is yearly reassessed.

Ongoing transaction monitoring

AML-Compliance ensures that an "ongoing transaction monitoring" is conducted to detect transactions which are unusual or suspicious compared to the customer profile.

This transaction monitoring is conducted on two levels:

- **The first Line of Control:** Media Entertainment works solely with trusted Payment Service Providers, Banks etc., who all have effective AML policies in place to prevent the large majority of suspicious deposits onto our site(s) from taking place without proper execution of KYC procedures onto the potential customer.

- **The second Line of Control:** We make its network aware so that any contact with the customer or player or authorized representative must give rise to the exercise of due diligence on transactions on the account concerned. In particular these include:
 1. Requests for the execution of financial transactions on the account;
 2. Requests in relation to means of payment or services on the account;

Also, all transactions must be overseen by employees over-watched by the AML Compliance Officer who is over-watched by the general management.

The specific transactions submitted to the customer support manager, possibly through their Compliance Manager must also be subject to due diligence.

Determination of the unusual nature of one or more transactions essentially depends on a subjective assessment, in relation to the knowledge of the customer (KYC), their financial behavior and the transaction counter party. These checks will be done by an automated System, while an Employee cross checks them for additional security.

The transactions observed on customer accounts for which it is difficult to gain a proper understanding of the lawful activities and origin of funds must therefore rapidly be considered atypical (as they are not directly justifiable). Any Media's staff members must inform the AML division of any atypical transactions which they observe and cannot attribute to a lawful activity or source of income known to the customer.

- **The third line of control:** As a last line of defence against AML, *Media Entertainment* will do manual checks on all suspicious and higher risk users in order to fully prevent money laundering. If fraud or Money Laundering is found the authorities will be informed. Reporting of Suspicious transactions on site. In its internal procedures, we describes in precise terms, for the attention of its staff members, when it is necessary to report and how to proceed with such reporting. Reports of atypical transactions are analyzed within the AML team in accordance with the precise methodology fully described in the internal procedures. Depending on the result of this examination and on the basis of the information gathered, the AML team: will decide whether it is necessary or not to send a report to the FIU, in accordance with the legal obligations provided in the Law; will decide whether or not it is necessary to terminate the business relations with the customer.

(1) Type of Engagement stage:

Assessment of the nature of the engagement. Media Entertainment N.V. shall focus on the engaging party whether it is a potential customer or a third-party provider of any kind (supplier).

Not all engagements will require the Company to perform full due diligence; e.g., where Media Entertainment is engaged with a simple and limited subscription-based service provider such as a domain name registrar or simple email or live chat services provider, we will not perform due diligence.

On the other hand, the below types of engagements require due diligence prior to signing any agreement:

- (a) Any content provider where software is customer facing (games/sports etc.);
- (b) Any third-party provider (customer verification service, hosting services etc.);
- (c) Any financial services arrangement or payment service provider engagement;
- (d) Any engagement with potential customer;
- (e) Any engagement with a Electronic money institution (EMI) wallet;
- (f) Any crypto wallet;
- (g) Any engagement with a Affiliation;
- (h) Any external (advocate, tax, financial etc.) advisors;

The above list is not exhaustive and if there is any doubt as to whether to require due diligence to be supplied, the Compliance Officer is to be consulted.

(2) Identification stage:

After the type of engagement is determined, the next stage (identification) is required.

In order to fully identify and verify the potential partner legal entity, the Business Unit ("BU"), shall collect necessary data and documents and ensure that all information and documentation provided is accurate and truthful. A client is any person (including individuals, incorporated entities, partnerships, trusts etc.) to whom the Company provides, intends to provide, or has in the past provided/receive a service in the course of carrying on its regulated business. A client for these purposes also includes a potential client.

Before acting for any client the Company must carry out a process of Customer Due Diligence (CDD), CDD involves:

The BU shall collect and receive at least the following information:

- The identifying the beneficial owner where relevant and verifying his or her identity, and obtaining information on the purpose and intended nature of the business

- relationship;
- Certificate of incorporation of the third party intended to contract with Media Entertainment;
- Office address of the third party;
- Shareholders/UBOs' and directors registry, as well as passport copies and proof of residence of all shareholders;
- Directors' registry, as well as passport copies and proof of residence of all directors;
- Organizational chart of the group of companies of which the third party is a part;
- Copies of all regulatory licenses held by the third party.
- Check and online verification for PEP, check official sources and or online for negative articles, feedback, or reputation on the third party(s).
- Proof of addresses on the involved parties (Directors, Shareholders, UBO, and parties with control in the third party).
- Source of wealth.
- Bank reference Letter
- Professional Reference Letter issued from such as (Advocate, Notary, Tax advisor etc.).

CDD must also be carried out whenever the Company suspects money laundering or has cause to be suspicious about or believes that any documents or other information that has been supplied is out of date or inaccurate. Full CDD must be accomplished in case of - any player transaction(s) equal and or above of 4,000 Cg.. Any transactions above the monetary equivalent of Cg. 4,000. Any other doubts on behalf of Media Entertainment's staff, employees Business Unit which forward to conclusion of clarification and verification of customer's personal data and to avoid further misleading and misunderstandings for illegal or any kind of unusual transactions whatsoever actions which could be breaching of the legislations. Any business relationship with a client will be subject to periodic review which may result in Employees being asked to conduct CDD or seek additional information from a client at any time.

The verification of the identity of the customer and the beneficial owner 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. In such situations these procedures shall be completed as soon as practicable after the initial contact. Media Entertainment N.V. is prohibited and do not accept/collect anonymous accounts whatsoever on behalf of personal individuals – players and or business companies – partners, vendors, providers etc. on the business, which can't be identified the UBO/Major shareholder and legit board of management by laws.

CDD: external players, individuals, advisors' expertise etc.

In each case of a customer engagement, the Company must obtain the individual's:

- full name;
- residential address;
- date of birth and place of birth.
- Nationality and ID number

This information must then be verified

Documents that could be used to meet this requirement are listed below:

Documents that identify the individual:

- current signed passport

- residence permit issued by home office on sight of own country passport
- current photo card driving license

Documents that verify the individual's address:

- Signed record of home visit
- recent (within the last 6 months) utility bill that has been posted to the individual's home address
- local authority utility bill (valid for the current year)
- bank, building society statement or passport

Identification Records

All evidence establishing the identity of a client must be recorded or copied as appropriate and kept on the client electronic file together with details of all transactions undertaken with or for the client (this may be kept electronically but must be in a printable form). This information must be kept for a minimum period of 5 years and or 10 years after closing business relationship and or account closure of a player(s).

(3) Review and Assessment stage:

At this stage, all information and documentation collected during the previous stages are assessed. It is the responsibility of the BU to ensure that all information and documentation are accurate, truthful and properly provided.

The purpose of this stage is, in accordance with Media Entertainment's risk-based approach, to identify whether potential business partners, and potential suppliers / customers of the Company, require thorough or limited due diligence, depending on the existence of high or medium risk factors.

Where the potential business partner is a third-party provider as per options (a) and (b) in stage 1 above, the BU shall collect all required documentation and assess the risk involved. If the risk found is moderate to severe, the BU shall notify the compliance department of the existence of these risk factors and send all relevant information and documentation to the compliance department to decide if Media Entertainment NV can contract with the supplier or not.

The BU must not communicate with the third party prior to obtaining the instructions of the compliance department, and any following communication will be solely in accordance with the instructions of the compliance department.

To the extent that the BU identifies no risk factors or only insignificant to minor risk factors, then it has the discretion to proceed with contracting with the third party, and approve the transaction, subject to all other policies of Media Entertainment. In any case of doubt, the BU must consult with the compliance department.

The BU may decide to move the transaction for further review according to the next stages, even where it believes the transaction contains only insignificant to minor risk factors.

When the transaction assessed is with an operator, payment processor or a potential licensee as per options (a) and (b) in stage 1 above, the BU shall collect all required information and documentation and send them to the compliance department for review. If the compliance department finds moderate to severe risk factors associated with this transaction, an approval from the Compliance Officer is required.

In order to evaluate the risks associated, the BU shall perform a research concerning the third party, its ultimate beneficial owners, shareholders and directors and collect information that pertains to potential moderate to severe risk factors, as well as check the names of the above mentioned vis-à-vis the following sanctions lists - OFAC ([Sanctions List Search \(treas.gov\)](https://sanctionslistsearch.treas.gov)), and the UN ([Sanctions | United Nations Security Council](https://scsanctions.un.org/inuhen-all.html)), United Nations Sanction List <https://main.un.org/securitycouncil/en/content/un-sc-consolidated-list> , UN Sanctions List <http://www.sanctionsmap.eu/#/main> ;

For PEP status screening casinos can rely on internet search or consult reports and databases on corruption risk, like the Transparency International Corruption Perceptions Index, or on www.knowyourcountry.com

All documents to be provided by the third party must be no older than 6 months from the date in which they were provided to the BU. In case in which the process of obtaining the information and documentation is lagging, the BU may request to be provided with updated documents.

In addition, the BU will analyse the following information, in order to examine whether any severe, major or moderate risk factors exist in respect of that third party:

- Jurisdiction – whether the third party is incorporated in or has an office address in a jurisdiction which (i) is perceived as a high-risk jurisdiction for corruption and/or financial crime, or (ii) known to have high levels of bank secrecy and facilitating illicit financial flows. The same shall be verified vis-à-vis the citizenship and residency of the ultimate beneficial owners, shareholders, and directors of the third party. For this purpose, the classification as high-risk jurisdictions is made on the basis of the recommendations of FATF ([Documents - Financial Action Task Force \(FATF\) \(fatf-gafi.org\)](https://www.fatf-gafi.org)).
- Background and identity of the potential business partner – a third party will be considered as including moderate/major/severe risk factors, if (i) an online and news search reveals significant problems relating to the integrity of the third party, or any of its ultimate beneficial owners, shareholders or directors, or (ii) the third party, or any of its ultimate beneficial owners, shareholders or directors (a) was subject to regulatory action or legal proceedings related to regulatory related activities, (b) appears on a denied parties/persons list in consequence of national or international sanctions or as a result of past misconduct, or (iii) the third party, its ultimate beneficial owners, shareholders or directors have little or no experience in the sphere of sports betting or are unknown to Media Entertainment N.V. Additional considerations are (iv) the date in which the potential business partner was incorporated (new corporate entities suggest higher risk), (v) corporate structure, especially if it is complex and involves several levels and/or trusts.
- Connection with PEP – major to severe risk factors include ownership, directly or indirectly, of the potential business partner by a PEP, or that business partner has direct or indirect links with a PEP,

- previous or current close relationship with PEPs, including, but not limited to, a situation in which a shareholder, ultimate beneficial owner or director is a PEP (now or in the previous 12 months).
- Financial transactions – a major or to severe risk factors will be considered if the third-party requests to receive payments by unusual means (e.g., deviating from standard practice, to multiple accounts, upfront payments, split into small amounts, using cryptocurrencies).
- Current activities – is the website of the proposed business partner compliant and provides the required legal structure and documents (to the extent required), as well as holds the required licenses; is there any adverse media in respect of such website.

The Compliance Officer may decide at any stage to override the initially imposed risk assessment, however any information/details being a ground for such change should be appropriately documented.

Media Entailment determined 5 categories of risks:

Severe – for example entities and/or legal representatives mentioned in sanctions lists, associated with illegal activities, dissolved entities or in the course of liquidation;

Major - for example entities that support crypto currency transfers; involved with PEP, incorporated in high-risk jurisdictions, newly setup incorporations with low turnover, no presence in the gambling industry, adverse media presence;

Moderate – for example, entities incorporated in a medium-risk jurisdiction; operating and/or licensed less than a year;

Minor – for example, the legal entity has been incorporated in a low-risk jurisdiction; operates under a license issued by a reputable jurisdiction more than a year.

Insignificant – minimal harm to the organization.

The above are just examples and by no means to be considered a closed list.

Without derogating from the above, the compliance department will perform routine reviews of the processes and decisions performed and taken by the BL in respect of third parties identified as insignificant or minor risk, in order to determine whether such processes and decisions were performed and taken in a proper manner. To the extent the compliance department identifies any shortcomings, it is authorized to launch a thorough due diligence and perform the activities according to the next stages in respect of any third party, as well as, to the extent so determined by the Compliance Officer, terminate the agreement with such third party.

Upon receiving the information and documentation from the BL, the compliance department will review, verify, and validate them. This will include ensuring that there are no internal inconsistencies and/or incompatibilities, as well as validate them vis-à-vis other sources of information.

The compliance department will evaluate the information and documentation provided and determine whether there are any red flags in the entire information and documentation provided to it, and whether the transaction with the third party can proceed. Red flags refer to circumstances suggesting a strong money laundering risk that should be properly identified and mitigated through adequate safeguards. There is no closed list of red flags, as such depend on the nature of the transaction and the applicable facts and circumstances. Having said that, examples of red flags include (on top of the matters discussed above):

- The third party appears to lack sufficient capability or staff qualifications to be part of the proposed transaction;
- The third party wants to work on the basis of a vague contract;
- The third party has family or business ties with PEPs;

- The commercials of the transaction appear to be unreasonable or not in line with the customary or arms-length amount;
- Unusual upfront or excessive payments have been requested by the third party;
- Indirect or unusual payment or billing procedures are being requested.

The existence of red flags does not necessarily require the rejection of the proposed transaction, but does require mitigating and resolving them, to proceed with the transaction. Any decision to proceed with a proposed transaction that has red flags requires the approval of the Compliance Officer, and – at the discretion of the Compliance Officer – the approval of the CEO as well.

(4) Approval Stage

In respect of any third party that seeks to become a supplier of Media Entertainment, as well as in respect of any third party that seeks to enter a contractual relationship with Media Entertainment, which was identified to have certain moderate to severe risk factors / red flags, the compliance department will require the following additional information and documentation:

- To the extent not provided previously – certified certificate of incorporation; certified shareholders' registry, as well as certified passports and certified proof of residence of all shareholders, UBOs and directors; organizational chart of the group of companies of which the third party is a part;
- For each director, shareholder, and ultimate beneficial owner – a bank / accountant / lawyer reference letter;
- The third party's memorandum and articles of association;
- A letter of good standing from the Companies Registrar of the jurisdiction of incorporation of the third party;
- Confirmation from a financial institution as to the ownership of the bank account to be used by the third party in connection with contracting with Media Entertainment N.V.;
- Source of funds declaration executed by a shareholder or director of the third party and confirmed by an accountant or a lawyer.

For the avoidance of doubt, the above-mentioned list of information and documentation may be extended if needed, in respect of any specific third party or in general, at the sole and absolute discretion of the Compliance Officer.

Any change in the identity of the party to contract with us will require a clear written explanation by the third party as to the reason of such change, as well as performance of a thorough due diligence in respect of the information and documentation affected by such change. In case of in case the obligations arising from the customer due diligence cannot be met and completed properly by Media Entertainment N.V., the casino cannot establish the business relation or perform the transaction and is obliged to terminate the business relationship with the customer/partner/vendor/provider. Media Entertainment N.V. also keep a record of all the attempts made to get the necessary information and documentation. Media Entertainment N.V. reserve the right to decide to either close the account or to keep it blocked and suspended in its entirety.

In the event that the customer makes the requested information and/or documentation available to the Company following the closure or the suspension and blocking of the gaming account, the Company must consider whether the delay in providing the requested CDD documentation and/or information affects the risk of ML/FT associated with the given business relationship. Any decision will be send in written to customer.

The reluctance of the customer to provide CDD on its own should not be automatically equated to a suspicion of ML/TF/FP. Media Entertainment N.V. is considering together all factors and information it has at his disposal to decide whether there are grounds to suspect ML/TF/FP. If, however the presumption of ML/TF/FP exists the Company will submit an unusual transaction report to the FIU with regard to this particular case and issue.

Where there is no reason for the retention of funds, the funds are to be remitted back to the player. This has to be done through the same channels used to receive the funds.

The above mentioned stages can be performed in parallel to the commercial negotiations and contractual drafting vis-à-vis the third party, provided that no contract and/or agreement is executed with any third party prior to approval if the transaction in accordance with this process.

8. ONGOING MONITORING

The BU is responsible to monitor, on an ongoing basis, the relationship with the third party with which Media Entertainment contracted. Any instance in which there is any suspicion of money laundering or terrorist financing, and/or any change in any of the facts and circumstances, information and documentation provided by that third party during the AML process, must be communicated immediately to the Compliance Officer, which will review the matter and decide how to proceed with it.

Any third party with which Media Entertainment contracted with, which had any red flags during the approval process by the compliance department and/or identified with moderate to severe risk factors, will be required to submit the information and documentation every two years. Other third parties will be derogate from the third party's obligation to promptly provide (and the BU's obligation to demand and receive) any information and documentation following any changes in the information and documentation formerly provided by the third party.

The Company implements and monitors all activity of clients and/or staff, to ensure that all activity whether it be transactional or instructional, be consistent and given the required attention for the detection of possible money laundering or terrorist financing.

8.1. Ongoing Customer Profile Monitoring

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

The periodic 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.

8.2. Ongoing Transaction Monitoring

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

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

- Requests to transfer gambling accounts or winnings to third parties (such transfers are also prohibited).

9. RECORD KEEPING

All information and documentation received, obtained and/or created in connection with this policy, including, but not limited to, any reviews, analysis, monitoring, reports, training, communications with applicable authorities, internal communications as well as the decisions taken and the rationales for such decisions (all together – the "Records") must be properly recorded and transferred to the compliance department. Online reviews and searches will be documented by screenshots / printing.

All Records in respect of a potential business transaction shall be held, subject to applicable legislation, for at least seven years after the later of the decision not to enter into such business transaction or the termination of that business relationship. Any other Records shall be held, subject to applicable legislation, for at least five years.

The Compliance Officer will keep a detailed record of:

(a) all steps taken to establish the identity of applicants for business or reasons as to why steps have been taken in a particular case;

(b) the full name, postal address, and date of birth of each person with whom the Company does business;

(c) the form and source of funds and/or securities used by the applicant for business;

(d) the form and destination of funds paid or delivered to the applicant for business or another person on his behalf;

(e) financial transactions carried out by the Company with or for each client or counterparty of the Company.

No Records will be erased without the written approval of the Compliance Officer.

10. REPORTING OF UNUSUAL TRANSACTIONS

Definition: Unusual transaction - it is a transaction, financial flow or movement of money and or other sources of funds (FIAT, crypto) which has been identified as inconsistent, illogical, with player's account history, and activity, could be indicator or factors for suspicious due to some action being taken and identified by our employees due to case by case, information granted to Company which is consisting criminal and or reported to relative authorities such as Police, Precrurritment office, Court etc., a transaction of amount equal and or higher than 4000 (ANG) has to be observed and identified prior taking a conclusion to identify it as unusual or not. Following transactions deemed as unusual: such as are in connections of money laundering, or funding terrorism, reported to Police or to the Department of Justice, on behalf of personal individual or legal company or corporate entities, group etc., who is in the list of sanctions, transaction of amount of transaction made by cash, by personal id check or anonymous form of payment method higher amount of deposit above 4,000 ANG.

The Company is committed to identifying and reporting any unusual activities and transactions, including attempted transactions, to ensure compliance with Anti-Money Laundering (AML) regulations. This section outlines the procedures and responsibilities for recognizing, reporting, and investigating unusual transactions. Employees must report any unusual activity to the Compliance Officer immediately, but no later than 24 hours after the transaction has been executed. This includes any transactions that raise suspicion or deviate from normal behavior.

Employees must submit an Internal Unusual Transaction Report (IUTR) to the Compliance Officer, in a format approved by Management. All additional documents available, such as copies of identification documents, cash out slips, and other records must be also submitted as supplements. If a more in-depth investigation is required, the Compliance Officer may request additional information from relevant departments. This investigation must be completed within ten (10) business days. The Compliance Officer will assess the information available to determine if it is sufficient to warrant filing an Unusual Transaction Report (UTR) with the FIU Curacao. If the Compliance Officer concludes that the activity is unusual, a report shall be submitted to the FIU regarding any unusual monetary operations or transactions within 48 hours.

10.1. Indicators Of Unusual Transactions

The Company observes both objective and subjective indicators to assess whether a customer's transaction is deemed unusual. The following transactions or intended transactions are considered unusual:

1. A transaction reported to law enforcement or judicial authorities in connection with money laundering or terrorism financing.
2. An intended transaction carried out by or for the benefit of any individual, legal entity, or group identified on a sanctions list.
3. A transaction amounting to NAF. 5,000.00 or more, regardless of the payment method, which includes:

- A cashless transaction in the amount of NAF. 5,000.00 or more.
 - Accepting or releasing a deposit of NAF. 5,000.00 or more at the customer's request.
 - Sale of chips to a customer amounting to NAF. 5,000.00 or more.
 - A cash-out transaction of NAF. 5,000.00 or more.
4. Transactions that may reasonably be presumed to relate to money laundering or terrorist financing.

10.2. Prohibition Of Disclosure

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

10.3. Protection For Reporting Employees

The Company has implemented measures to safeguard employees and representatives who report suspicions of money laundering, terrorist financing, and/or financing of proliferation to the FIU. Employees reporting such suspicions are protected from threats or hostile actions by other employees, management, or customers, as well as from adverse or discriminatory employment actions.

11. AML COMPLIANCE PROGRAM

11.1. 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 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.

11.2. Compliance Department Training

The compliance department is in charge first and foremost of:

- Safeguarding Company's compliance across all activities, employees, procedures, regulations, and policies;
- Providing due diligence and KYC for potential customers, vendors and senior management; Review agreements, notifications, letters, writing drafts, preparing and advising legally in all matters;
- the company and management itself;
- Participating with regulatory audits.
- Any other related work;

Therefore, all new compliance employees are provided with the most current and correlating laws, regulations, adopted policies and procedures by their managers.

The main objective of the mandatory trainings is to provide the employees with a general overview and understanding of money laundering/terrorist financing and to raise awareness of the warning signs of problematic gambling and gambling addictions.

11.3. Training

All employees of the Media Entertainment N.V. that are in contact with third party business partners and/or once a year and prior to commencing their employment. The scope of the training will be determined by the Compliance Officer, tailored to the employees' responsibilities, provided that such training will include the following issues:

- (i) Introduction to AML and main definitions;
- (ii) AML and terrorist financing offences;
- (iii) The provisions, roles, and responsibilities according to this policy;
- (iv) Collection of information and documentation relating to AML;
- (v) SAR;
- (vi) Risk factors and red flags;
- (vii) AML assessment and decision making;
- (viii) Reporting obligations;
- (ix) Record keeping;
- (x) Disciplinary measures (including termination) to be taken for breaching the provisions of this policy and/or abusing the processes according to this policy.

The training of the members of the compliance department includes all of the above, but is more in-depth and consists of ongoing training on the job, including case studies and updates about any regulatory and compliance developments.

11.4. Independent AML Audit

Periodically, the efficacy of the organization's AML/CFT program is assessed to ascertain that it remains pertinent and in accordance with industry standards, best practices, business operations, and regulatory advancements. The Company demonstrates compliance with all relevant legal and regulatory obligations in the jurisdictions where it conducts business. 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.

11.5. Examination by the Gaming Control Board

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

- The written and approved AML Compliance Program addressing ML/TF/PF.

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

12.COMPLIANCE AND CONSEQUENCES OF NON-COMPLIANCE

The Company is fully committed to adhering to all applicable laws and regulations related to Anti-Money Laundering (AML), Counter-Terrorism Financing (CTF), and sanctions enforcement as established by the jurisdiction of Curacao, aligning with international best practices, including the FATF Recommendations. Compliance with the AML/CTF Policy is mandatory for all employees, officers, agents, and third-party service providers. Non-compliance may expose the organization and individuals to significant legal, regulatory, and reputational risks, including fines or penalties imposed by Curacao's authorities, revocation or suspension of the Casino's gaming license, and potential criminal prosecution for willful violations. Additionally, non-compliance can lead to reputational damage, resulting in loss of customer trust, negative media exposure, and strained relationships with financial partners. Operational disruptions may also occur, such as freezing of funds, loss of access to financial systems, and increased scrutiny from regulators. Employees who violate the AML/CTF Policy may face disciplinary actions, including formal warnings, suspension, or termination for serious or repeated breaches, as well as potential referral to law enforcement. Third-party providers may have their agreements terminated if found non-compliant. All employees must understand and comply with the AML/CTF Policy, participate in mandatory training, and report any unusual behavior or breaches to the Compliance Officer, who will ensure that whistleblower protections are in place.

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

13. CONTACT INFORMATION:

For questions, related topics, reporting with regards to this policy, please contact:
Petar Mitkovski – Compliance Officer,

phone number: +359 898581590

email: p.mitkovski@offsidegaming.com

14. RISK CLASSIFICATION

Risk rating allocated for each risk

The below table describes the risk rating allocated for each risk:

Risk Factor	Risk Rating	Details	Mitigating Factor/s
Service Risk	Low	The players are not directly able to influence the outcome of the game/event, in respect of the casino games, since these are entirely RNG based results. In respect of Sports betting there may be a possibility of players colluding together, however Media Entertainment monitors bets placed very closely including which	- Media Entertainment monitors all transactions, and anything suspicious will be investigated further detail, however as explained this is not being regarded as any major risk.
Transaction Risk	Low Medium	players are placing bets. Furthermore, even IP addresses are closely monitored thus making it easier to identify possible collusion or the use of multiple accounts by a single player. In addition there are various checks and controls in place with respect of monitoring of financial transactions being placed. At this stage Media Entertainment N.V. feel confident that players are closely monitored to reduce such a risk to an acceptable low level. Bank transfers (with EEA or equivalent safeguards) Visa/Mastercard	- All the financial institutions which Media Entertainment N.V. engages with are established in reputable jurisdictions and subject to strict AML regulations Such institutions are themselves

Medium	EEA-licensed payment service providers (Wirecard, Neteller, Skrill, ecoPayz)	obliged to monitor the bank accounts or debit / credit card activities on an on-going basis, as part of their due diligence (DD) obligations
High	Pre-paid cards/vouchers (AstroPay Card and PaysafeCard etc.)	Media Entertainment N.V. adopts a strict policy of remitting withdrawals to the same account from where the funds originated. It is only in exceptional circumstances and where there is no additional option, that withdrawals will be processed to a different source, such as the case with the use of Mastercard. In such circumstances, Media Entertainment will obtain corroborating documents to ensure that the account belongs to the same individual player. Once that is confirmed Media Entertainment will allow the player to receive the funds in the different account

Media Entertainment N.V. verifies the ownership of the bank account / credit card etc. It adopts this measure to help it ensure that the account belongs to the registered player. Furthermore, Media Entertainment traces the source from where the funds were received. Well trained payment and anti-fraud team, with on-going training provided as and when required and also when there are new developments within the industry Identification of patterns within deposits made by players – a thorough analysis of all the transactions made by the player will then be conducted Identification of players who always seem to just miss the due diligence verification requirements – full KYC procedures will anyway be applied, and in extreme cases the Enhanced Due Diligence (EDD) documents will be requested, to further ensure no specific wrongdoing Identification of players who always process deposits from different sources / different accounts – conducting full due diligence, including corroborating that all accounts / Cards used to process deposits are owned by the same person. If there are any further outstanding suspicions after such checks – the source of wealth would also need to be investigated to ensure that it is not a case of a problem gambler using different sources to fund the habit.			
---	--	--	--

Effective technological tools in
place to monitor and detect
suspicious activities

Geographical Risk	Low	EEA Member States, and other reputable jurisdictions.	Accepting players only from reputable jurisdictions, as also
Interface Risk	Low	Media Entertainment adopts a remote and automated registration process. The registration happens on Media Entertainment's database without any third party intervention. The AML measures adopted ensure that the high risk brought about by the non-face-to-face interactions are mitigated through the various controls related to KYC and the due diligence process, as well as via the on-going monitoring. This allows Media Entertainment N.V. to categorise such risk as a low-level risk.	Strict KYC and AML measures are adopted as per this policy and the KYC procedure. This secures the effectiveness of our onboarding procedures, and the control techniques used for monitoring of player activity Customer support also play an important role in the risk mitigation of the interface risk. Even though it is a non-face-to-face relationship, customer support communicates with players via e-mail, but more importantly via telephone communication, and that helps in the creation of a personal, albeit not face-to-face relationship. Adherence to applicable laws and Curacao Gaming Board regulations, and effective supervision by the relevant local authorities

	High	Non-reputable jurisdictions (for instance, those known to have a weak AML/CFT system, and countries known to suffer from a significant level of corruption) and countries subject to international sanctions in connection with terrorism or the proliferation of weapons of mass destruction, as well as countries which are known to have terrorist organisations operating within them, are to be considered as high risk.	Indicated in the Players' Terms & Conditions and as including in the Customer Acceptance Policy within this document. Ongoing monitoring and verification which ensures that information provided by player is true, and up-to-date. Strict KYC and AML measures are adopted as per the company's policies and procedures. Monitoring of IP addresses, as a general this allows us to identify that the player is logging in from the same country where he claims to be resident. There are exceptions to this rule such as when a player uses a proxy server, or
--	------	--	---

Customer Risk	Low to High	Identification of risk generally depends on person's economic activity and/or source of wealth.	- Ongoing monitoring and verification which ensures that information provided by player is true, and up-to-date. Strict AML measures are adopted as per this policy - Adherence to applicable laws and CIL regulations, and effective supervision by the relevant local authorities - PEPs are automatically considered as a high risk and hence will not be accepted as players as per the Customer Acceptance Policy.
			- Adherence to applicable laws and CGA regulations, and effective supervision by the relevant local authorities - when a player is abroad, away from his country of residence, however such cases would be the exception and not the rule and hence such scenarios would be investigated further to identify why the mismatch

