

**The Prevention of Money Laundering and Funding of Terrorism
Policies and Procedures Manual**

March 2023

Preface

These policies and procedures have been approved by the Company and are considered to be binding upon such and also upon any persons engaged by the same. These policies and procedures are subject to periodic review in view of continuous developments in the industry, in an effort to maintain the policy of best practice. In fact, this AML Policies and Procedures Manual should be seen as a '*working document*', which is amended from time to time.

It is to be noted that the Company shall refer to the Laws of Curacao, guidelines issued by the Financial Intelligence Unit in Curacao, AML best practices and European directives and regulations whilst applying the principles and procedures contained herein.

The objective of this document is to establish and maintain policies, procedures and controls, which deter criminals from using our lawful facilities for money laundering and the funding of terrorism.

This document is for internal use only.

Abbreviations

CDD- Customer Due Diligence

EDD – Enhanced Customer Due Diligence

ID - Identity

FATF – Financial Action Task Force

FIU- Financial Intelligence Unit

M&As- Memorandum & Articles of Association

ML/FT- Money Laundering/Funding of Terrorism

MLRO- Money Laundering reporting Officer

PMLFTR – Prevention of Money Laundering and Funding of Terrorism Regulations

SDD – Simplified Customer Due Diligence

STR – Suspicious Transaction Report

Definitions:

For the purposes of the provisions of this manual:

“Player” means the natural or legal person, who can be acting either as principal or as agent, with whom deal with whom the Company deals, when embarking on a business relationship or occasional transaction;

“Funding of Terrorism” shall have the meaning ascribed to it under European Directives (AMLDs) and may be described generally as “the process by which terrorist organisations or individual terrorists are funded in order to be able to carry out acts of terrorism”¹;

“Money Laundering” shall have the meaning ascribed to it under Curacao Law and European Directives (AMLDs), and may be described generally as “the process by which the illegal nature of criminal proceeds is concealed or disguised in order to lend a legitimate appearance to such proceeds”²;

“PEP” (Politically Exposed Person) means a natural person who is or has been entrusted with prominent public functions and for a period of 12 months thereafter, including:

- (i) Heads of State, Heads of Government, Ministers and Deputy and Assistant Ministers and Parliamentary Secretaries;
- (ii) Members of Parliament;
- (iii) Members of the Courts or of other high-level judicial bodies whose decisions are not subject to further appeal, except in exceptional circumstances;
- (iv) Members of courts of auditors, Audit Committees or of the boards of central banks;
- (v) Ambassadors, charges d'affairs and other high ranking officers in the armed forces;
- (vi) Members of the administrative, management or boards of State-owned corporations;

and the immediate family members or persons known to be close associates of such persons³;

“Reputable Jurisdiction” means any country having appropriate legislative measures for the prevention of money laundering and the funding of terrorism, and which supervises natural and legal persons subject to such legislative measures for compliance therewith;

“Regulations” means the applicable anti money laundering and funding of terrorism regulations currently in force in Curacao, any issued AML guidelines and any European Directive applicable to the prevention of Money Laundering and Funding of Terrorism.

“Source of funds” means the activity, event, business, occupation or employment from which the funds used in a particular transaction are generated.

“Source of wealth” means the economic activity which generates the total net worth of the customer.

The Company means MSD Tech BV, a company registered in Curacao, licensed and operating in the field of remote gaming;

Scope:

This manual seeks to implement the provisions of the Regulations which require the Company (as a “subject person” in terms of the Regulations) to take appropriate measures to make employees aware of:

- Customer due diligence, record-keeping and internal reporting measures required to be applied and maintained by the Company;
- Policies and procedures, including internal control, risk assessment and management and communications, which are aimed at preventing the carrying out of operations that may be related to money laundering or the funding of terrorism; and
- The provisions of the Regulations.

Chapter 1: Policy document

ANTI-MONEY LAUNDERING POLICIES FOR THE COMPANY

1.1. Compliance statement

It is the policy of the Company to comply in all respects with any applicable AML legislation by ensuring that policies and procedures aid the compliance function.

1.2. Policy on money laundering

The Company is committed to following the requirements of the money laundering legislation and supporting authoritative guidance issued by relevant regulatory authorities. It is committed to promoting a culture of compliance throughout the organisation and practice. The Company confirms that the policy is:

- to ensure that prevention of money laundering is addressed appropriately in all player transactions.
- to ensure that commercial considerations never override the need to comply with the Regulations;
- to ensure sufficient resources are devoted to the development, documentation and training necessary to ensure compliance; and
- to ensure that, where necessary, they appoint, a suitable Money Laundering Reporting Officer to monitor compliance.

The current Compliance Officer also responsible for AML is Dr Michael Muscat LL.D

1.3. Policy and procedure on due diligence

It is the policy of the Company to undertake a risk assessment (using the due diligence measures), and ensure that evidence of identity is obtained and retained as appropriate to that risk assessment for all players. This evidence will be obtained before an account is opened.

Due diligence is undertaken on all players at different stages of the relationship depending on the risk profile of the Player.

Identity verification is always carried out prior to opening an account.

Further KYC is obtained at withdrawal.

Source of Funds is carried out on all transactions of two thousand Euro or More.

Source of wealth is requested from players once they deposit two thousand Euro or more.

Player gambling patterns and deposit patterns are continuously monitored by our platform technology.

1.4. Policy and procedure on reporting

It is the policy of The Company to report all suspicions identified by the MLRO or by any other practitioner appointed on behalf of The Company to the FIU and the gambling regulator.

All assistants, whenever and wherever appointed, will report suspicions to the MLRO as soon as the suspicion arises. The report will be made using internal reporting tools. This report will not be discussed with anyone apart from the Lawyers and the MLRO and at no stage must the player or third parties be given any details of the report, without the specific agreement of the MLRO.

On receipt of the report, the MLRO will consider the contents, request further information where required and determine what action should be taken. His decision will be recorded on the internal reporting tool and then where necessary a report will be submitted to the FIU.

At this stage the MLRO will inform the Lawyer and/or assistant of The Company and/or player relationship manager in charge, if any, of any action that he needs to take (for example, blocking balances, ceasing to take bets.).

The Company shall never carry out a transaction that is suspected or known to be related to ML/FT. Upon customers' requests for such transaction, the employee shall inform the MLRO immediately.

When an assistant or appointee of The Company has suspicions that ML/FT is occurring, all assistants or appointees, are prohibited from disclosing to the person under investigation or to third parties, that an investigation is being carried out, may be carried out, or that information has been or may be transmitted to FIU. Disclosure of such information would give rise to the offence of tipping off and may prejudice an investigation.

Suspicious should not be discussed with anyone other than the MLRO.

The Company, must however still retain the necessary contact with a customer and should enquire, in a tactful manner, about any transaction which is not consistent with the customer's normal pattern of activity.

1.5. Policy and procedure on record keeping

It is the intention and an inherent policy of The Company to maintain records of identification and consideration of money laundering issues for the entire relationship and for at least five years thereafter.

The customer due diligence measures will be completed for all new customers and updated at appropriate times. These measures, along with supporting documentation, will be filed in the corporate file of the respective customer.

At the end of the relationship, this information will be archived in the archive file with a date logged.

1.6. Policy and procedure on third party reliance

It is the policy of The Company not to rely on third parties for due diligence purposes.

1.7. Policy and procedure on internal control

It is the policy of The Company to facilitate adequate internal control to allow for compliance with the Regulations and other appropriate legislation.

As set above, The Company's Compliance Officer/MLRO will be given authority to implement the necessary changes in these procedures to ensure compliance. All assistants or appointees will be required to accept the changes necessary and service/partnership agreement, where applicable, that confer the necessary authority on the MLRO. Moreover, all assistants and appointees will be required to make the necessary internal reports using our internal reporting tool when they have a suspicion in respect of a player .

1.8. Policy and procedure on risk assessment and management

It is the policy of The Company to undertake AML risk assessments for players and retain the same on file for a period of 5 years.

1.9. Policy and procedure on compliance management

It is the policy of The Company to undertake a regular compliance review to ensure that the requirements of the Regulations are being followed.

1.10. Policy and procedure on communication

It is the policy of The Company to ensure that all assistants and appointees have access to adequate training to ensure that they have the necessary knowledge of the Regulations and of these policies and procedures.

All assistants will be required to undertake an update course on anti-money laundering

procedures and compliance, at least once every two (2) years. This should be provided by a reputable educational institution or institution of practitioners such as Society Education and/or the FIU and/or the 'Big Four' audit firms.

1.11. Other policies and procedures

Where players do not provide sufficient documentation to render compliance herewith, the Company shall not provide services to such players.

Moreover, any document which is in a language not understood by The Company should be translated in English. The translation should be signed, dated and certified by an independent person of proven competence, confirming that it is faithful translation of the original.

Chapter 2: Customer Due Diligence Measures

The Company must apply and maintain, **in all cases**, customer due diligence measures when forming a relationship or carrying out an occasional transaction. Enhanced Customer Due Diligence **must be applied** when the risk assessment of a relationship and/or an occasional transaction is considered as 'High-Risk'.

2.1. Purpose of Customer Due Diligence Measures:

These measures will assist The Company in:

- Determining if the player poses a high or low money laundering risk;
- Determining the business profile of the player, in order for The Company to be able to identify those transactions which may be deemed to be unusual for such player;
- Assisting the FIU by providing timely and precise information on Players and their transactions.

The Company may have a system in place, which detects whether a Player is subject to any financial sanctions issued by the UN Security Council or the EU in relation to persons known to be involved in terrorism:

- (i) Sanctions websites shall be consulted as soon as the identity of the Player is established
- (ii) Independent research should be carried out through world-check and other similar online commercial databases (for example; a Google search).

The Company should be alerted to the OECD Anti-Bribery Convention.

2.2. Enhanced Customer Due Diligence:

Enhanced Customer Due Diligence is to be applied and maintained in relation to all Players considered to be on a high risk-sensitive basis.

In addition to the three specific instances mentioned above, The Company must conduct EDD in relation to a business relationship or a transaction connected to a jurisdiction listed under the public documents issued by the FATF, which is contained in Appendix II. Moreover, The Company must inform the FIAU of any business relationships or transactions with persons, companies and undertakings, including those carrying out relevant financial business or a relevant activity from a non-reputable jurisdiction⁴.

Generally, the Company will refrain from conducting business with persons from non-reputable jurisdictions and/or jurisdictions on any FATF lists.

2.2.1. The identification of the Player and the verification of his identity⁵:

The Company must first identify the player and in a separate procedure verify such identity.

2.2.1.1. Natural Person:

Identification:

All of the following should be obtained:

- (a) Full name and surname;
- (b) Place and date of birth;
- (c) Permanent residential address;
- (d) Identity reference number (I.D./Passport number); and
- (e) Nationality.

i. Verification:

When the applicant for business is **present for verification purposes**, the verification of the person's identity shall be made by reference to **any one** of the following containing photographic evidence of identity:

- (a) Valid, unexpired passport (original);
- (b) Valid, unexpired government-issued ID card (original); or
- (c) Valid unexpired driving license (original).

Verification of the person's residential address shall be made by reference to **any one** of the following which must be **not more than 6 months old**:

- (a) A recent statement from a recognised bank (original);
- (b) A recent utility bill (original);
- (c) A correspondence from a local or central government entity (original);
- (d) Any government-issued document listed in (Aii) above, where a clear indication of residential address is provided

The verification of the person's identity shall be made by applying **one or more** of the following measures:

- (a) Use identity verification software and video conferencing together with document scanning software to establish authenticity and confirm identity.
- (b) Require certified confirmation of the documentation supplied by a person carrying out relevant financial business.
- (c) Ensure that the first payment or transaction into the account is carried out through an account held by the applicant for business in his name with a credit institution holding a license in a reputable jurisdiction.

2.2..2 Legal Persons

The Company shall generally have no relationships with companies in that its customers shall only be natural persons. When dealing with suppliers, mostly technology companies will be dealt with as software providers and similar. In this case, a request of the share register of the

supplier, its certificate of registration, its memorandum and articles together with a confirmation of beneficial owner will be requested. The same checks as carried out above for Players will be carried out for beneficial owners of suppliers in order to ensure that the Company does not do business with sanctioned and/or questionable persons.

2.2.3. When the applicant for business is a PEP

The Company will refuse business from PEPs as a general policy.

Chapter 3: Understanding the nature and profile of the business relationship

3.1. Information on the purpose and intended nature of the business relationship

The Company must obtain all the following information in order to establish the business and the risk profile of the application for business:

- Identity, Age, Place of Residence, Nationality.
- The nature and details of the business/ occupation/ employment of the applicant for business;
- The source(s) of wealth;
- The expected source and origin of the funds to be used in the business relationship;
- The anticipated level and nature of the activity that is to be undertaken through the relationship;

3.2. On-going monitoring of the business relationship

Once the business profile of the customer has been established, The Company must continue monitoring the activities on an on-going basis in order to identify any unusual transactions which may involve ML/FT. On-going monitoring of a business relationship includes:

- The scrutiny of transactions undertaken throughout the course of the relationship to ensure that the transactions being undertaken are consistent with the subject person's knowledge of the customer, his business and risk profile, including where necessary, the source of funds. The Company must ensure that the customer's business corresponds to the information disclosed by the customer at the beginning of the business relationship and that the business patterns of the customer are consistent with the risk profile established by the subject person.
- Ensuring that the documents, data or information held by the subject person are kept up to date. The Company must ensure that any expired documentation are replaced by the latest documents within 2 months of the expired date.

The Company should pay special attention to any large complex transactions, including patterns of transactions that have no apparent or visible economic or lawful purpose and business relationships and transactions with persons from non-reputable jurisdiction. A list of countries associated with non-reputable jurisdiction is found in Appendix II. These are generally not accepted by the Company.

3.3. Monitoring complex or large transactions

The Company must examine complex or large transactions with special attention to the following transactions:

- the background and purpose of any complex or large transactions,
- unusual patterns of transactions,
- complex or/and large transactions which have no apparent economic or visible lawful purpose and
- transactions which are particularly likely, by their nature, to be related to ML/FT.

Where it is revealed that the customer's business and risk profiles have significantly diverged from the established patterns or for no apparent economic or lawful purpose, the employee or appointee must immediately report to The Company by submitting an internal report found in appendix 1.

3.4. Source of wealth and source of funds

The Company is obliged to identify the source of wealth at the beginning of the business relationship. The customer must provide detailed explanation together with documents to substantiate such explanations such as contracts.

The Company must also obtain information on the source of funds. The Company shall not, to the extent possible, be satisfied with a generic description when questioning the customer about the origin of the funds used in the context of a business relationship. For example, an explanation by the customer stating that funds consist of the proceeds generated by a business would not be sufficient and more detailed information on the business concerned as well as producing copies of invoices or contracts to substantiate such explanation need to be requested. The source of funds to be utilised for an occasional transaction must also be identified by The Company.

3.5. Risk- assessment procedures

The Company must identify and assess ML/FT risks posed by our customers, products and services. The risk assessment procedure shall include the below , together with automated analyses of betting patterns, deposits and withdrawals:

3.5.1. Customer risk

This risk is generally based on the person's economic activity and/or source of wealth. The following is a list of categories of customers whose activities may pose a higher risk:

- Customers conducting their business relationship or transactions in unusual circumstances;
- Customers where the structure or nature of the entity or relationship makes it difficult to identify the true owner or controlling interests;
- Cash and cash equivalent intensive business, cash is not accepted by the company.

- Use of intermediaries within the relationship who are not subject to adequate AML/CFT laws and measures and who are not adequately supervised;
- Customers that are PEPs (in General The Company will not service PEPs);
- Customers who are subject to sanctions or other economic measures.

3.5.2. Product/service risk

Some products/ services are inherently more risky than others and are therefore more attractive to criminals. The following is a list of number of factors that The Company should take into consideration when determining the risks of products and services:

- The nature of the product/service offered by the Company, that of gambling related services, may be more attractive to criminals looking to launder money. This is to be kept in mind when analysing customers and transactions. Vigilance must be placed upon customer backgrounds and types, together with betting behaviour in order to ensure that our platform is not used to launder the proceeds of crime.

3.5.3. Interface risk

The channels through which a subject person establishes a business relationship and through which transactions are carried out may also have a bearing on the risk profile of a business relationship or a transaction. The use of internet for the provision of services is considered as a high risk, in view of the rapidity with which online transactions may be conducted and the level of anonymity that such transactions may offer. Customers dealing in crypto currency should be treated as high-risk.

3.5.4. Geographical risk

This risk relates to the geographical location of the business/economic activity and the source of wealth/ funds of the business relationship. The following list should be assessed in determining when a country poses a higher risk:

- Countries subject to sanctions, embargoes or similar measures issued by international organisations such as United Nations Security Council.
- Countries identified by credible sources as lacking appropriate AML/CFT laws, regulations and other measures.
- Countries identified by credible sources as providing funding or support for terrorist activities that have designated terrorist organisations operating within them.
- Countries identified by credible sources as having significant levels of corruption, or other criminal activity.

APPENDICES

NON-REPUTABLE AND NON COOPERATIVE JURISDICTIONS

The following is a list of countries recognised by the Financial Action Task Force as high risk and non-cooperative jurisdiction as per the FATF Public Statement & On-going Process Document which is amended and updated from time to time:

Afghanistan
Albania
Algeria
Angola
Argentina
Cambodia
Cuba
Democratic People's Republic of Korea
(DPRK)
Ecuador
Ethiopia
Indonesia
Iran
Iraq
Kuwait
Lao PDR
Myanmar
Namibia
Nicaragua
Pakistan
Panama
Papua New Guinea
Sudan
Syria
Tajikistan
Turkey
Uganda
Yemen
Zimbabwe