

MIBS N.V.

AML/CFT Policy

DOCUMENT RECORD

Version	Security	Date	Description	Author
1.0	Confidential	01 May 2025	Policy creation	MLRO
		01 May 2025	Policy approved	
1.1	Confidential	30 May 2025	Policy update	Compliance

TABLE OF CONTENTS

INTRODUCTION	5
SCOPE	6
LAWS AND APPLICABLE LEGISLATIONS	6
NOTICE	7
OBJECTIVES OF THE POLICY	8
GOVERNANCE	8
THE MLRO	9
MLRO Responsibilities	10
AML & CFT POLICY AND PRINCIPLES	10
UNDERSTANDING MONEY LAUNDERING AND FUNDING OF TERRORISM	11
What is money laundering and terrorist financing?	11
Why are anti-money laundering and counter-terrorist financing important to the company?	11
Typical signs of money laundering and terrorist financing	11
Money laundering	12
The cycle of money laundering	12
The principal offenses of money laundering	13
Terrorist financing	14
The principal offenses of terrorist financing	14
CUSTOMER SCREENING	17
Adverse Media	17
Financial Sanctions	18
Politically Exposed Persons (PEPs)	18
RISK MANAGEMENT	20
Risk Appetite and Customer Acceptance	20
Jurisdiction Risk	20
Business Risk Assessment (BRA)	21
Customer Risk Assessment (CRA)	21
ONBOARDING OF NEW CUSTOMERS	23
Timing of Due Diligence	24

Levels of Due Diligence	24
LEVEL 1: Simplified Due Diligence (SDD)	24
LEVEL 2: Customer Due Diligence (CDD)	25
LEVEL 3: Enhanced Due Diligence (EDD)	28
SOURCE OF FUNDS AND WEALTH	32
Identification and verification Source of Wealth and Funds	33
Source of Wealth and Funds Supporting Documentation	33
CUSTOMERS FAILING TO PROVIDE DUE DILIGENCE INFORMATION	36
ONGOING MONITORING	37
Periodic Ongoing Monitoring	38
CDD: IP Check	38
CDD: Double Customer Check	38
Transaction monitoring	39
Deposit without wagering	39
INTERNAL REPORTING	40
Suspicious activity	40
Internal escalation	40
Failure to report	40
Tipping-off and prejudicing an investigation	41
EXTERNAL REPORTING	42
REQUESTS FROM AUTHORITIES	43
EMPLOYEE SCREENING	44
EMPLOYEE TRAINING	44
POLICY COMPLIANCE AND REVIEW	46
RECORD KEEPING	46
AUDITING	47
WHISTLEBLOWING PROCEDURE	48
DATA PROCESSING AND RETENTION	48
Processing of special categories of personal data	48
Retention of documents and data	48

INTRODUCTION

MIBS N.V. also referred to as (the “company”) is a Curaçao registered private limited company, established to offer remote gaming services, including casino, live casino and sports betting.

Money laundering and terrorist financing have become a subject of significant international concern. With that in mind, the company has established a strong AML/CFT control function, endowed with highly effective risk-based anti-money laundering policies, controls, and procedures.

The company is committed to employing best practices along with a high standard of effective anti-money laundering and counter terrorist financing measures.

To accomplish this task, the company uses policy development, various controls, procedures and training to not only provide a clear understanding of anti-money laundering concepts, legal obligations, relevant offenses and practical safeguards, but also to reinforce these through a strong culture of ethics and compliance.

SCOPE

The scope of this policy is to establish policies and procedures on internal controls, risk assessment, risk management and compliance in relation to AML and CTF. The policy has been created in compliance with the license held and ensures to:

- Remain alert to the possibility of ML or FT;
- Report all suspicions to the MLRO email address in accordance with the AML/CTF policy and SAR procedures;
- Comply fully with all AML procedures including: customer identification, monitoring, record keeping, awareness and reporting;
- Attend any relevant training and updates, keeping up to date with new and evolving threats;
- Complete the mandatory AML/CFT training periodically to ensure compliance and adherence to the policy;
- Ensure that the company is not used for illicit activity;
- Take the most reasonable and appropriate actions to mitigate the risks associated with ML, FT, and other financial criminal activities, including fraud, corruption etc.

This policy and procedure is applicable to all employees, contractors, affiliates and any other individual working on behalf of the company. The company is determined and committed to prevent the carrying out of financial activities through its systems that may be related to ML or FT.

The company shall comply with its obligations at law by establishing the necessary and relevant processes to prevent ML and FT and to ensure any suspicious activities are escalated to the relevant authorities.

The policies outline the general and minimum standards of internal AML and CFT which should be adhered to by the company's management, employees and any third party working on behalf of the company.

LAWS AND APPLICABLE LEGISLATIONS

Relevant AML and CFT legislation:

- 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);
- Curaçao Gaming Control Board Regulations for the combating of Money Laundering, the Financing of Terrorism and Proliferation of weapons of mass destruction, last update January 2025.
- EU AML directive 2021/0250 (COD)
- Regulation (EU) 847/2015 on Information accompanying transfers of funds
- EC 1781/2006 of the European Parliament and the Council of May 2015 on the prevention of the use of the financial system for Money Laundering and Terrorist Financing

NOTICE

All employees will be asked to read this policy and any ancillary documentation provided by the company and are to confirm in writing or by email that they understand their personal responsibilities arising from the policies and procedures.

Relevant training will also be delivered to further ensure that the policies and procedures are understood in their entirety along with the company's corporate responsibilities. This policy sets out practical guidance to all employees in gaining awareness and understanding of the relevant Anti-Money Laundering (AML)/Countering the Financing of Terrorism (CFT) obligations under the various laws and regulations. It provides direction in relation to the fundamental aspects of customer onboarding, ongoing monitoring, systems, and controls

that must be applied by the company in its efforts to combat money laundering and terrorist financing.

The policy also sets out the responsibilities of the senior management, the Money Laundering Reporting Officer (MLRO) and all staff of the company, in recognising and dealing with AML/CFT risks and obligations.

“Senior management” means an officer or employee with sufficient knowledge of a company’s money laundering and terrorist financing risk exposure and sufficient seniority to take decisions affecting its risk exposure, who does not need, in all cases, to be a member of the board of directors.

OBJECTIVES OF THE POLICY

The company is obligated to adopt policies, procedures and training measures. These include outlining the responsibilities of senior management to prevent and detect the commission of money laundering and terrorist financing.

The company abides by and adheres to all applicable laws and regulations regarding AML/CFT in all jurisdictions where it conducts its business. To achieve that, the company has developed and implemented a comprehensive set of measures to identify, manage and control all AML/CFT risks at all stages of the business relationship with its customers.

The company, its staff and contractors are committed to the highest standards of openness and integrity. It has implemented a risk-based approach to anti-money laundering (AML), countering the financing of terrorism (CFT), antifraud and anti-corruption measures, which have been designed to effectively mitigate against the risk of financial crime.

The company, its staff, and contractors must take all reasonable steps to anticipate and prevent having its services used for financial crime purposes. Any failure to do so will have direct and significant consequences for the company and its senior management. Non-compliance with the company’s AML/CFT obligations poses various risks, such as regulatory, legal, commercial, and reputational risk.

This policy should be read in conjunction with the Business Risk Assessment.

GOVERNANCE

The company adheres to the three lines of defense in order to ensure that a level of control is being held and that reporting is carried out efficiently without any unnecessary barriers. The lines of defense are being:

The first line of defense is the customer facing and customer support, carrying out transaction monitoring, customer execution of due diligence and ensuring that all policies are being adhered to.

The second line of defense is the Money Laundering Reporting Officer and compliance team, who are tasked

with the compliance monitoring, point of contact to the regulators, reporting of suspicious transaction, set policies and standards

The third line is the audit function.

The governance structure is to promote immediate reporting to the MLRO, ensure that internal controls and compliance management is also being adhered to, and to also ensure that the audit function may provide an annual gap analysis in order to mitigate any potential risk. The structure also ensures that the decisions are taken at the appropriate level.

THE MLRO

The main duties of the MLRO are listed below.

- To prevent the company from being exploited for financial criminal activities by being in compliance with all applicable legal requirements;
- To ensure that the company takes the most reasonable and appropriate actions to mitigate the risks associated with money laundering, terrorist financing, and other financial criminal activities, including fraud, corruption, etc.;
- Remaining alert to the possibility of money laundering or terrorist financing;
- Ensuring that all suspicions are reported to the MLRO in accordance with the AML/CTF policy and SAR procedures;
- Complying fully with all AML policies and procedures including customer identification, transaction monitoring, record keeping, training and reporting;
- Ensuring attendance of any relevant training and updates provided so that the company is able to keep up to date with new and evolving threats; and,
- Confirmation the completion of any mandatory periodic AML/CFT training to ensure compliance and adherence to the policy.

The role of the MLRO shall be to:

- Receive reports from its employees, contractors or through software solutions used to analyze transactions, on information or matters that may give rise to knowledge or suspicion of ML/FT, or that a person may have been, is or may be connected with ML/FT.
- Consider these reports to determine whether knowledge or suspicion of ML/FT subsists or whether a person may have been, is or may be connected with ML/FT.
- Report knowledge or suspicion of ML/FT or of a person's connection with ML/FT to the relevant FIU; and
- Respond promptly to any request for information made by the relevant FIU.

MLRO Responsibilities

The MLRO's responsibilities include:

- Continuously monitoring and checking that the company complies with its legal and regulatory obligations, these guidelines and hereto related controls.
- Providing advice and support to the company's employees / contractors on AML/CFT rules.
- Informing and training on AML/CFT rules.
- Continuously briefing on new trends, patterns and methods as well as other relevant information to prevent ML/FT.
- Being responsible for providing data/information to the police or relevant authorities in the prescribed manner.
- Checking and regularly assessing if the company's internal guidelines and controls are sufficient to prevent ML/FT in the business.
- Making recommendations to the relevant stakeholders based on the observations made.

The MLRO who reports to the CEO on AML/CFT issues, may appoint one or several persons to assist and also delegate authority to them.

AML & CFT POLICY AND PRINCIPLES

The company has implemented standards and principles which include:

- Establishing and maintaining a risk-based approach towards assessing and managing the money laundering and terrorist financing risks for each of its customers;
- Establishing and maintaining risk-based customer due diligence measures, for the identification and verification of its customers, including enhanced due diligence measures and ongoing customer and transaction monitoring;
- Implementing procedures for reporting suspicious activity internally and to the relevant law enforcement authorities, as appropriate;
- Maintenance of appropriate records for prescribed periods;
- Training, awareness-raising sessions, and regular screening.

The company's terms and conditions highlight its commitment to compliance with all applicable laws and regulations. No customer will be onboarded unless they have agreed to the terms of use.

The company will take all reasonable measures to safeguard against the possibility of customers depositing funds originating from criminal activity or depositing funds by using a payment facility for which the customer is not authorized to use. It shall implement measures to make sure that it does not allow activities or transactions that should be prohibited, such as any such activities or transactions linked to illicit activity or fraud.

UNDERSTANDING MONEY LAUNDERING AND FUNDING OF TERRORISM

What is money laundering and terrorist financing?

Money laundering is the process through which the proceeds of crime and their true origin and ownership are changed and disguised so that the proceeds appear to have come from a legitimate source. Terrorist financing is the provision or collection of funds with the intention or knowledge that the funds be used in order to carry out any act (s) of terrorism.

The main difference between money laundering and terrorist financing is that the source of funding for terrorist activity is generally lawful and unlike money laundering, a relatively small amount of money is required to fund the attacks which makes it easier for criminals to by-pass the legitimate financial system. Many of the techniques used to disguise the destination of terrorist funds are identical to those used to disguise the source of illicit funds. Transactions are to be monitored to identify if any linkages are to be made with terrorist or criminal activity.

Why are anti-money laundering and counter-terrorist financing important to the company?

The AML and CTF regime is designed to prevent our services being used by criminals and bad actors. The company has regulatory obligations to identify, analyze and deter money laundering and terrorist financing activity. Failure to meet its obligations can lead to criminal sanctions, fines, reputational damage, and operational risk, such as the loss of licenses.

Typical signs of money laundering and terrorist financing

The company must remain vigilant to any warning signs, red flags and indicators of money laundering and terrorist financing. Moreover, upon the identification of any such red flags, there is an obligation on all officials and its employees to make the enquiries and take the actions that a reasonable person (given the same qualifications, knowledge and experience) would have taken in the same circumstances.

- The customer has deposited funds with the company, and the origin of the funds is unknown;
- Complex or unusually large transactions;
- Transactions with no apparent logical, economic or legal purpose;
- Asset transfers where there is a variation between the account holder identity and the person making or receiving the deposit in fiat currency;
- Movement of funds between accounts, institutions, or jurisdictions without logical purpose or reason;
- Transactions or IP sign-ins involving high-risk jurisdictions;
- Large payments incurring fees with instructions terminated shortly after and the customer requesting the funds be returned;

- Unusual instructions or requests from customers outside of usual practice. One must understand the purpose of the customer's actions;
- Cash-based transactions involving the physical movement of currency, with payments being broken down into smaller amounts to avoid detection;
- Stolen credit cards;
- Forgery of documentation, collusion (for which such is not possible at the current stage of operation);
- The use of impermissible software tools;
- The provision of false registration data or other requested information.

Money laundering

“Money laundering” means:

- a) the 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, for the purpose of concealing or disguising the illicit origin of the property or of assisting any person who is involved in the commission of such an activity to evade the legal consequences of that person's action.
- b) the concealment or disguise of the true nature, source, location, disposition, movement, 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.
- c) the acquisition, possession, retention or use of property, knowing or suspecting, at the time of receipt, that such property was derived from criminal activity or from an act of participation in such an activity.
- d) participation in, association to commit, attempts to commit and aiding, abetting, facilitating, and counseling the commission of any of the actions referred to in points (a), (b) and (c).

The cycle of money laundering

Typically, money laundering involves three stages:

Placement

Placement is the stage where the money is introduced into the financial system. At this stage, it is still possible to link the funds to their illegitimate source. The placement stage initiates the process of money laundering which has the ultimate aim of incorporating the funds derived from illicit activity into the financial system.

During the placement stage, it is very important for the company to understand where the funds utilized by its customers are being derived from, especially since any bad actor who has the intention of committing the crime of money laundering seeks to dispose of the money derived from criminal activity without attracting any attention.

Bad actor intending to launder illicit funds can make use of several methods during the placement stage including the use of cash deposit cheques, traveler's cheques, gambling services, loan repayments, life insurance policies, structured deposits (e.g. deposits aimed at remaining under certain thresholds, the purchase and sale of assets without legitimate commercial purpose, and any other means to mix legitimate and illegitimate funds.

Layering

When the funds derived from illicit sources have been deposited in the financial system following the placement stage; typically, the next stage is the process of layering. Layering involves the separation of illicit proceeds from their source by layers of financial transactions intended to conceal the origin of the proceeds.

Layering is used to convert the proceeds of the crime into another form by creating complex layers of financial transactions to obfuscate the source and ownership of funds. This process is directed at trying to confuse any investigation by making it difficult to trace the origin of the funds. For example, this could involve electronically moving funds from one jurisdiction to another, moving funds between different financial institutions or to different accounts within the same financial institution.

Integration

At this stage the money derived from criminal activity has been made to appear legitimate and is placed once again into the financial system in what appears to be normal business or personal transactions. By the integration stage, it is exceedingly difficult to distinguish between legal and illegal wealth.

The money launderer might invest the funds in real estate, financial ventures or luxury assets. Integration is generally difficult to spot unless there are great disparities between a customer's legitimate employment, business or investment ventures and a customer's wealth, income, or assets.

We are most likely to become involved in the integration stage but potentially could be involved in any stage.

The principal offenses of money laundering

A principal money laundering offense is committed:

- Conceal, disguise, convert, transfer, or remove criminal property
- Enter or become concerned in an arrangement which facilitates the acquisition, retention, use or control of the criminal property for or on behalf of another
- Acquire, use or have possession of criminal property
- Concealing

This includes concealing or disguising its:

- Nature
- Source
- Location
- Disposition
- Movement
- Ownership

Possession means having physical custody of the criminal property. You will have a defense to a principal money laundering offense if a person submits a Suspicious Activity Report (SAR) to the MLRO.

Terrorist financing

“Terrorist financing” means financing acts of terrorism, i.e. the provision or collection of funds, by any means, directly or indirectly, with the intention that they be used or in the knowledge that they are to be used, in full or in part, to carry out any of the offenses within the meaning of Articles 1 to 4 of Council Framework Decision 2002/475/JHA of 13 June 2002 on combating terrorism.

Terrorist financing is a very serious threat to businesses and must be taken as seriously as money laundering. Terrorists need funds to plan and carry out activities. Such threats are not taken lightly by the company due to the possibility of loss of life.

In general terms, terrorist financing is:

- The provision or collection of funds
- From legitimate or illegitimate sources
- With the intention or in the knowledge
- That they should be used in order to carry out any act of terrorism
- Whether or not those funds are in fact used for that purpose, i.e.: Principal terrorism offenses of:
 - Fundraising
 - Use or possession
 - Arrangements
 - Money laundering
 - Failure to disclose offenses
 - Tipping-off offenses

When dealing with terrorist financing, it is important to note that funds do not necessarily have to be derived from criminal activities. The funding of terrorism can adopt a similar methodology to that used for money laundering however the intent and the scope of such acts vary from one another. The professional standards enforce Customer Due Diligence and

KYC on transactions and have made the activity of terrorist financing more difficult for those who are willing to pursue it.

Many of the techniques used to disguise the destination of terrorist funds are identical to those used to disguise the source of illicit funds.

The company recognizes the importance of KYC and has in place practices to comply with the professional standards. The process being followed is that of keeping records of beneficial owners, business entities and the applicants for business.

Every customer who attempts to or successfully makes a deposit will be screened against the sanction lists and then daily compared automatically to detect any changes to such designated individuals or entities that have been listed on the international sanctions list. The software is also set to provide notification in case of any changes.

The compliance function, as part of its ongoing monitoring of business relationships, or when notified or becoming aware of any change in the beneficial ownership pertaining to the customer account is to physically compare beneficial owners, and where suspicion has raised any intermediary or known controlling party against Sanction searches held on the system and physically check them against the following sanction lists:

- <https://www.un.org/en/sc/documents/resolutions>
- <https://www.un.org/sc/suborg/en/sanctions/un-sc-consolidated-list>

If such searches reveal a positive match, and the match has met several criteria, such match will be reported accordingly to the relevant authority. The following criteria are applicable for a match to be determined as a positive:

- Name and surname
- Date of birth
- Jurisdiction
- Photo identification
- Identification or passport number

If such a match has been found, one should also investigate through open sources to obtain further information and immediately inform the MLRO by following internal reporting procedures. The MLRO should then investigate any suspicion, knowledge or reason to believe and report where necessary. The MLRO shall also have the responsibility of ensuring that the screening is being carried out as instructed.

The principal offenses of terrorist financing

All offenses carry heavy criminal penalties. In relation to funding of terrorism one must also be aware of the following:

- Fundraising for terrorism

- Using or possessing money for the purposes of terrorism or derived from criminal activities.
- Involvement in funding arrangements and
- Money laundering (facilitating the retention or control of money which is derived and/or destined for terrorism).

This obligation is significantly different, as it does not just cover "proceeds" of crime, but all funds, regardless of their origin.

Definition of financing the proliferation of weapons

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

CUSTOMER SCREENING

The company recognizes the importance of the customer profile and has in place practices to comply with the laws and regulations in relation to, identification, verification and screening of the customer for sanctions, political exposure (PEPs) and adverse media.

The process being followed is that of keeping record of the applicants for business and for which upon initiation of the registration of the account, the customer will be immediately screened by the use of a third party provider being Global Data Consortium and/or Trapets and block any customer who has registered as a positive match.

Those customers who are dubious shall be passed on to the MLRO for further verification. The MLRO may appoint anyone working within the unit to investigate such matters. The lists of individuals are automatically scanned by Global Data Consortium and/or Trapets on first deposit.

If such searches reveal a positive match, and the match has met several criteria, such match will be reported accordingly to the relevant authority. The following criteria are applicable for a match to be determined as a positive:

- Name and surname
- Date of birth
- Jurisdiction
- Photo identification
- Identification or passport number

If such a match has been found, one should also investigate through open sources to obtain further information and immediately inform the MLRO by following internal reporting procedures. The MLRO shall also have the responsibility of ensuring that the screening is being carried out as instructed and sampling of the data shall be carried out and recorded accordingly. The company reserves the right to request further documentation in relation to any possible match for which more documentation will be deemed necessary to verify such suspicion.

This policy sets out the company's process for screening of new and existing customers for financial sanctions (FS), adverse media and Politically Exposed Persons (PEP).

Adverse Media

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

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

Adverse media hits showing predicate offenses of ML such as mafia, forgery, drug trafficking and fraud and terrorism amongst many others, shall be reported due to the sensitivity of the crime and the involvement of financial crime. Should any predicate offense raise concerns, they shall be raised with the MLRO accordingly.

Financial Sanctions

The Kingdom Sanction Act, The United Security Council Resolutions and the EU Regulations impose several sanctions on both individuals and entities that are known or have been involved to be active in the field of terrorism of funding thereof, and the funding of proliferation of weapons of mass destruction.

Should any of the company's customers be a person or entity listed under the Kingdom Sanction Act, OFAC, UN, EU or any other national sanctions or who is directly or indirectly owned or controlled by a listed person or entity, the freezing measures shall apply.

The company shall have the capacity to monitor and freeze any funds from sanctioned individuals or legal entities. If a customer is listed under any sanction, who is directly or indirectly involved or the provenance of funds is from ownership, involvement or controlled by an individual seeking a business relationship with the company, the following actions shall be conducted:

- All funds are to be frozen, including financial assets and economic resources, whether owned directly or indirectly by a person or an entity.
- All those assets being financial or economic resources, are not to be made available to or for the benefit of the designated persons or entities.
- If one suspects that a transaction, whether completed or attempted, is related to FT, he/she should immediately inform the MLRO by following internal reporting procedures.
- If the MLRO knows, rather than suspects, that a transaction is related to property owned or controlled by or on behalf of a terrorist or a terrorist group, he/she should not complete the transaction and report it to the relevant authority immediately.

Politically Exposed Persons (PEPs)

"Politically exposed persons" means natural persons who are or have been entrusted with prominent public functions, other than middle ranking or more junior officials. The definition also covers their immediate family members or persons known to be close associates of such persons.

For the purposes of this definition the term "natural persons who are or have been entrusted with prominent public functions" includes the following:

- a) Heads of State, Heads of Government, Ministers, Deputy or Assistant Ministers, and Parliamentary Secretaries.
- b) Members of Parliament or similar legislative bodies.
- c) Members of the governing bodies of political parties.
- d) Members of superior, supreme, and constitutional courts or of other high-level judicial bodies whose decisions are not subject to further appeal, except in exceptional circumstances.
- e) Members of courts of auditors or of the boards of central banks.
- f) Ambassadors, charges d'affaires and high-ranking officers in the armed forces.
- g) Members of the administrative, management or supervisory boards of State-owned enterprises.
- h) Anyone exercising a function equivalent to those set out in paragraphs (a) to (f) within an institution of the European Union or any other international body. Family members include the following
 - I. the spouse, or a person considered to be equivalent to a spouse, of a politically exposed person;
 - II. the children and their spouses, or persons considered to be equivalent to a spouse, of a politically exposed person;
 - III. the parents of a politically exposed person; Persons known to be close associates means:
 - a) natural persons who are known to have joint beneficial ownership of legal entities or legal arrangements, or any other close business relations, with a politically exposed person;
 - b) natural persons who have sole beneficial ownership of a legal entity or legal arrangement which is known to have been set up for the de facto benefit of a politically exposed person.

PEPs are classified as a ML risk since they may be exposed to property that has been generated by corruption and bribery because of their position. If a PEP or close associate is found, the customer will be escalated to the MLRO. Despite the fact that the FATF allows transactions with PEPs, the policy is that no business is conducted with PEPs / shall not be offering any services to PEPs and upon a customer becoming a PEP, the account shall be terminated.

RISK MANAGEMENT

Risk Appetite and Customer Acceptance

The company currently has a high-risk appetite when it comes to customer acceptance but a medium risk business appetite meaning that the residual risk of any product or service has to have sufficient controls in place to mitigate such risk to be within controllable boundaries and for which the company has control over the behavioral pattern and relationship with the customer.

The policies and procedures hereunder are all reflective of such concepts and are therefore in place to further activate the desired result in ensuring proper risk management and mitigation.

The company shall also ensure that in the event a customer is generating funds derived from a non-acceptable business which has been deemed as illegal or immoral, such customer shall be subject to an internal investigation as accounts are to be blocked due to the pretense of a false declaration.

Jurisdiction Risk

The company has adopted a procedure of reviewing and ranking the jurisdictions involved in the company's operations, at a minimum annually. The jurisdiction list is compiled via several sources (see the list of sources below). An exhaustive assessment is carried out, and an internal scoring is assigned accordingly; such risk level will be then reflected as part of the customer risk assessment.

The development and implementation of appropriate measures and procedures on a risk-based approach, and for the implementation of customer Identification and Verification and Due Diligence Procedures, the MLRO and compliance officer shall consult data, information and reports (e.g. customers from countries which inadequately apply Financial Action Task Force's (FATF), country assessment reports) that are published in the following relevant international organizations in order to determine the geographical risk posed by a customer:

- FATF – www.fatf-gafi.org
- Business and sanctions consulting <https://www.bscn.nl/sanctions-consulting/sanctions-list-countries>
- The Council of Europe Select Committee of Experts on the Evaluation of Anti-Money Laundering Measures (MONEYVAL) – www.coe.int/moneyval
- The EU Common Foreign & Security Policy (CFSP) – http://ec.europa.eu/external_relations/cfsp/sanctions/list/consol-list.htm
- The UN Security Council Sanctions Committees – www.un.org/sc/committees
- The International Money Laundering Information Network (IMOLIN)- https://www.imolin.org/imolin/amlid/index.jsp?lf_id=
- The International Monetary Fund (IMF) – www.imf.org

- The Office of Foreign Assets Control (OFAC) of the US Department of the Treasury – <http://www.treasury.gov/resource-center/sanctions/SDN-List/Pages/consolidated.aspx>
- Basel international jurisdiction list

Business Risk Assessment (BRA)

The BRA is an encompassing view of inherent risks, vulnerabilities and threats to the company, the mitigating factors conducted and the residual risk. The company's policies, internal controls, compliance management and procedural documentation, is influenced by the BRA.

The residual risk, as a result of the BRA determines whether a particular risk falls within the acceptable risk appetite of the company or if such risk will be outrightly refused. For example, the BRA is conducted prior to the launch of any product to identify the inherent risk associated, mitigating factors, and whether the residual risk of such product fits the company's acceptable risk appetite. If the risk does not fall within the company's acceptable risk appetite such product's risk mitigators will be increased. If such a product's risk still falls within an unacceptable level, the product will be discontinued.

The factors which are included in the BRA are as follows:

- Product / Service
- Transaction
- Geography
- Customer
- Delivery Channel (Customer Interface)

The manifestation of risk of the factors above are assessed in relation to ML and FT. In developing the operational AML/CTF policy and procedures, the company has reviewed its business processes against the criteria set out above to take a 'risk-based approach' to the development of AML/CTF controls. The BRA summarizes the factors into low, medium and high risk. The Curacao National Risk Assessment was taking into consideration for this BRA.

New or material changes shall warrant a re-evaluation of the BRA; such changes shall also be applicable upon introduction of new products, services, jurisdictions and payment methods. Changes within the regulatory framework shall also be considered as pertinent elements that shall contribute to a review of the risk.

Customer Risk Assessment (CRA)

The company has developed a robust internal scoring from which the level of due diligence is requested from the customer. The risk assessment is a pertinent aspect in assessing factors which are obtained through the customer profile which is to be provided in detail by the customer. By identifying and assessing the money laundering risks, the company can take the best steps to mitigate and monitor those risks.

Risk factors from which the risk is likely to emanate are from and are prevalent in the company's risk assessment are:

1. Jurisdiction risk
2. Customer risk
3. Interface risk
4. Transaction risk
5. Product and service risk
6. Fraud and behavioral patterns

Understanding the risks that may arise from the above factors, the company has taken up the development of sound risk management practices, to help assist the officers involved in the process and tools to manage the risk posed by the threats of money laundering, funding of terrorism or other illicit activity.

The level of due diligence required is dynamic as the risk depends on the actions and behavioral patterns of the customer. The company has a twofold approach to the CRA:

- Risk assessment: The risk assessment is in place to indicate behavioral patterns and pertinent information emanating from the customer.
- Transactional triggers: These triggers are serious instances which give rise to possible ML/FT therefore all transactional triggers require an internal analysis of the action.

The risk score of the customer shall reflect the customer's current position whether at onboarding or ongoing monitoring. The customer is assigned a score which determines if the customer is Low, Medium or High Risk. Risks may be cleared following a policy assessment and/or the customer providing sufficient information to clarify any alerts generated by the system, the risk assessment can only be re-evaluated by the MLRO, with a written rationale to be left on the customer's account.

Any alerts cleared shall be recorded but shall not affect the risk score of the customer. The risk score can be overwritten if an officer has reasonable doubts. For example, if an officer would like to place a low risk customer as a high risk, if reasonable justification is provided, they can do so.

The risk assessment is pertinent in assessing factors obtained through the profile to be provided in detail by the customer. Each criterion of risk will determine a set level of due diligence for which the information required is readily

available from a list of due diligence requirements. A justification for the level of due diligence will have to be provided, including any reasoning behind the assigned risk category.

ONBOARDING OF NEW CUSTOMERS

This section describes the criteria for accepting new customers based on their risk categorisation. Following a riskbased approach for every customer, it will be determined what level of due diligence is to be applied concerning identification, business relationship and transaction level.

The Company will perform (CDD) under specific circumstances to ensure compliance with AML regulations and to protect the integrity of its operations. The Company must undertake CDD measures when players engage in financial transactions that amount to XCG 4,000 or more. This includes any deposits or withdrawals made by the player.

In addition to financial transactions, the casino must carry out CDD for any occasional transaction that is equal to or exceeds XCG 4,000. Furthermore, if there is any suspicion of money laundering or terrorist financing, the company is obligated to conduct CDD. This also applies in situations where there are doubts about the accuracy or completeness of previously obtained identification information from the player.

Financial transactions are defined specifically as deposits and withdrawals; bonuses are excluded from this category. Conversely, wagered amounts and winnings are classified as gambling transactions and do not fall under the definition of financial transactions.

To effectively monitor and determine when a player reaches the XCG 4,000 threshold for CDD purposes, the Company will evaluate not only individual transactions but also any series, combination, or pattern of transactions that exceed this amount. This evaluation will be conducted daily and will include all deposits, withdrawals, and peer-to-peer transfers made by the player.

Moreover, Company Name maintains a strict policy against anonymous accounts or accounts held under fictitious names. The casino is committed to identifying each player by collecting their name and other relevant information, which is essential for determining the purpose and nature of the business relationship

Where the level of risk is above the level the Company is willing to accept, appropriate steps must be taken to mitigate the risk. If the risk cannot be mitigated to an acceptable level, the relationship must be terminated.

Upon registration, the customer, shall provide the following identification information:

- First name
- Last name
- Date of birth
- Residence address (Building, street, city, country)
- Email and/or mobile phone number

Due to the non-face to face customer onboarding nature, the company has implemented mandatory verification for which tools and technology will be utilized to limit the risk. The company shall reserve the right to block accounts and request alternative documentation should it be deemed necessary.

In order for the company to know it is dealing with a real person, documentation is required at certain intervals to corroborate as much as the information submitted as possible. The company shall obtain sufficient evidence of identity to verify the person is whom they claim to be.

A customer's residential address is an essential part of their identity, and when it is not present on identification documents, it will have to be obtained separately (once the relevant due diligence level is reached).

The KYC will be verified via the KYC provider 'SumSub' who will ensure that the documentation provided corresponds to the information currently held on the customer and that the KYC is valid. If the documentation provided is deemed not to be valid or sufficient, further documentation may be requested from the customer.

Following the risk-based approach, at onboarding, a risk assessment of the ML and FT risk posed by the customer is carried out based on the information provided by the customer and checks conducted. The risk assessment will rate the customer as low, medium or high risk. Due diligence and ongoing monitoring will be carried out in proportion to this risk. If the risk is deemed Medium or High, further information and documentation is required from the customer. If the account is rated High Risk and/or is exhibiting trends or there is suspicion, knowledge or reason to believe it must be reviewed by compliance personnel and brought to the attention of the MLRO for further investigation.

Timing of Due Diligence

It shall be pertinent that upon request of any documentation and/or information from the customer, a 30 day limit is placed upon the account. During such time, all withdrawals will be blocked until all the necessary information and/or documentation is successfully provided. Failure to provide the requested due diligence will result in the termination of the business relationship.

Levels of Due Diligence

LEVEL 1: Simplified Due Diligence (SDD)

The company collects identification information from every customer during the account opening (registration) process, which at a minimum includes – name, address and date of birth. The company also carries out Politically Exposed Persons ("PEP"), adverse media, and sanction screening checks. A customer may only remain on SDD should the risk assessment be a low risk. If following a risk assessment, a customer's risk is deemed to be low, the identification of the customer shall be carried out prior to the establishment of a business

relationship. Electronic or bank identification shall be deemed as acceptable means for identification and verification purposes.

In those cases where it is detected that the customer is acting on behalf of, for the sake of clarity, beneficial ownership shall mean any person who is funding the account, hence if a person has an account which is funded by a third party, that third party is considered to be a customer and a beneficial owner. However, such accounts shall be refused by the company.

Such can be detected by:

- Customer requesting to send funds not the original account hence not following closed loop
- Customer is using a payment instrument which does not pertain to the identification documentation held
- Upon review it is identified that the customer is playing on behalf of someone else

If the MLRO or any of the AML/CFT team deem that a low-risk customer, due to information available, is likely to threaten the good standing of the AML/CFT function within the company, the customer shall not be considered lowrisk. The risk level shall be overridden with justification provided, representing the actual risk level posed by the customer.

LEVEL 2: Customer Due Diligence (CDD)

The company's due diligence procedures deal with identifying customers, understanding their expected product/service usage, and their source of funds and source of wealth. CDD measures based on the customer risk profile and to further substantiate the customer risk profile the following information shall be mandatory assessed:

- Identity verification for every new customer
 - Assessing the risk profile of every customer
 - Transaction analysis
 - Analysis of the historical pattern of the customer's transaction activity
 - Surveillance of game play
 - Ban of anonymous or fictitious accounts
- Customer Due Diligence (CDD) Measures

The company takes measures for CDD:

- When establishing a business relationship (subsists for a period of time);
- At occasional transactions relating to the pay-out of profits or payment of stakes of an amount equal to €2,000 or more; and
- For transactions the amount of which are less €2,000, if the company realizes, or ought to realize, that the transactions relate to one or several other transactions which together amount to at least €2,000.

Identity verification

The company identifies and verifies the customer's identity, and obtains basic customer data (name, personal identity number, registered address, telephone number, e-mail etc.). Also, ensuring that the customer's specified/used bank account or payment method belongs to them.

As the company's customers are non-face-to-face natural persons, the company identifies and verifies their identity remotely:

- Through an established and recognised electronic identification system or equivalent; or
- By retrieving data on the person's name, address, personal identity number or equivalent and verify these data against external records, certificates or other equivalent documentation.

Such which shall be outsourced to a third party provider and if required also have the ID document screened against if upon testing suspicion is raised in relation to adequacy of the document. The term outsourced means will provide the technology but all obligations and responsibilities remain with the company.

All customers entering the platform shall be subject to completion of identification including PEP, financial sanction and adverse media checks for which the following is to be obtained:

1. Identity verification
2. Address Verification
3. A selfie

Identity verification of the customer is to be provided as a form of government-issued document/s, such document/s should contain photographic evidence of identity. Acceptable documentation shall be as follows:

- a valid unexpired passport (preferably does not expire in the following six (6) months);
- a valid unexpired national or other government-issued identity card;
- a valid unexpired residence card; or
- a valid unexpired driving license (must hold nationality)

The documentation will be reviewed by a third party provider and if required also by

If a customer holds a bank or e-ID such shall be deemed to be sufficient for the identity and address verification.

If there is a suspicion regarding an identification document further documentation is to be requested. Those customers who do not reside within the European Union, and reside in a high-risk jurisdiction or where the customer presents a high ML/FT risk, the company shall

reserve the right to request further information and documentation pertaining to the customer in order to satisfy any risk or questions related to the identified threat.

Address verification

At this stage (CDD), the customer's address shall also be verified. The address is verified by one of the following documents (which are not more than six months old) that clearly shows the customer's name and residential address:

- A recent utility preferably not older than six (6) months;
- A recent statement preferably not older than (6) months, from a recognised credit institution;
- Correspondence from a central or local government authority, department or agency;
- A record of visit to the address by a senior official of the subject person;
- Any identification document where a clear indication of residential address is provided; or
- Certificate of conduct issued by a law enforcement authority.

In relation to utility bills when verification of a utility bill is done by the company it is to verify that the said document has been issued in relation to the services linked to that residential property. A bill issued in relation to a fixed line telephone service installed on that property would be also acceptable. Mobile telephone bills which are not linked to a fixed premise are not acceptable.

The address verification documents will be uploaded via the provider who will ensure:

- The documents provided are a valid form of Address Verification documentation;
- The documents provided are not more than 6-months old;
- The details provided on the address verification documentation match the customer's account;
- The address verification documentation looks legitimate and not tampered with; and
- The address verification documentation is held on file for a minimum of 5 years.

If a customer holds a bank or e-ID such shall be deemed to be sufficient for the identity and address verification. If there is a suspicion regarding the address verification document further documentation is to be requested.

Those customers who do not reside within the European Union, but reside in a high-risk jurisdiction or where the customer presents a high ML/FT risk, the company shall reserve the right to request further information and documentation pertaining to the customer in order to satisfy any risk or questions related to the identified threat.

The company understands that CDD is a dynamic ongoing process; throughout ongoing monitoring, certain changes, events or triggers will require the Company to re-complete

some or all the CDD measures. The completion of CDD will result in a customer either successfully passing CDD or alternatively being classified as high risk and being immediately subject to EDD.

N.B. if a customer has a change in I.P. of over 90 days, the customer will be prompted to update the proof of address.

LEVEL 3: Enhanced Due Diligence (EDD)

The company applies Enhanced Due Diligence (EDD) measures on a risk sensitive basis in any situation which by its nature can present a higher risk of ML and/or FT, as well as when certain thresholds are reached.

EDD checks include account reviews, adverse media screening, full review of game and transaction history, recording occupation and source of wealth, verification of source of funds and source of wealth, and requests for certified identification documents.

Enhanced Due Diligence ("EDD") Measures

The enhanced measures are supplemented by such additional measures which are required to prevent the high risk of ML/FT, especially for those high-risk customers. At a minimum, the company:

- Retrieves additional information on the customers' financial situation and information on where the customers' financial resources derive from; and
- Gets approval from the relevant senior manager to conclude or cancel a business relationship with the customer, where deemed necessary.

Additional measures implemented by the company include:

- Adverse media checks on the customer through online searches for articles or other relevant information with allegations of criminal activity or terrorism or dealings with criminals or criminal activity.
- Increased frequency for the updating of CDD documentation to ensure that the information is up to date and correct.
- Increased frequency and intensity for reviewing transactions, e.g. that controls must always be made for transactions over certain thresholds (at reasonable levels).

As stated throughout the policy and procedures, EDD is to be applied without delay in instances where the customer is likely to pose a higher than normal ML/FT risk. The MLRO and the AML/CFT team are to have a full overview of customers deemed to be of a higher risk.

EDD shall require additional measures concerning where the threat is emanating from, achieved via source funds and/or wealth requests. The company is to keep all documentation regarding the customer's identity, documentation verification and the risk assessment.

Once EDD has been completed the residual risk is to be adequately assessed in the risk assessment and sufficient ongoing monitoring is to be conducted to address any residual risk. If the residual risk is greater than the company's risk appetite (and cannot be lowered to a satisfactory level by mitigating measures) the account shall be terminated.

EDD verification measures are as follows (note that each will not be required on every EDD verification but based on the information provided by the customer and the risks presented):

- Obtaining additional information and, as is appropriate, substantiating documentation on the intended nature of the business relationship;
- Carrying out additional searches (e.g., internet searches using independent and open sources) to better inform the customer's risk profile;
- Consider the source of wealth and funds involved in the transaction or business relationship to ensure they do not constitute the proceeds of crime. In order to investigate this it could include obtaining appropriate documentation concerning the source of wealth or funds even on the beneficiaries;
- Increasing the frequency and intensity of transaction monitoring; Increasing the number and timing of controls applied and selecting patterns of transactions that need further examination;
- Increasing awareness of higher-risk customers and transactions across all departments who have a business relationship with the customer. Increasing awareness also includes the possibility of conducting enhanced briefing with engagement teams responsible for the customer; and
- Obtain Senior Management approval for the continuation of the relationship in cases where the doubt has been raised on approval of the customer.

For high risk customers the system every 12 months or when any transactional triggers are activated will automatically provide an alert on the account. The MLRO can override any risk assessment and therefore be placed on monitoring for which the relationship will be assessed more frequently.

In relation to identification, when the customer is at high risk, or doubts are raised in relation to the identity of the customer, although the customer is registered with electronic or bank identification, a document listed in the verification section is to be obtained.

The following information is obtained at due diligence level 3 to provide information on the profile of a customer.

This information shall be used to further substantiate the business relationship and provide the company with relevant information pertaining to the funds used in the business relationship.

Status of employment:

- a) Retired

- b) Self-employed
- c) Employed
- d) Part-time employment
- e) Student
- f) Unemployed

Proof of income which are risk ranked to reflect the risk of the provenance of the funds as per CRA flow:

- a) Salary income (Low Risk)
- b) Fixed deposit – Savings (Low Risk)
- c) Sale of property (Medium Risk)
- d) Sale of company (Low Risk)
- e) Income from investments (Medium Risk)
- f) Inheritance (medium Risk)
- g) Company profits/ distributed Dividend (Low Risk)
- h) Loan (High Risk)
- i) Crypto investments/ Mining (High Risk)
- j) Funds generated from winnings (Medium Risk)
- k) Pension (Low Risk)
- l) Gift (Medium Risk)
- m) Rental income (Medium Risk) Gross annual income:

A drop down for gross annual income is to be in place, the risk is assessed depending on the salary brackets for which are likely to increase the risk of ML/FT

- a) Euro 5,000 - Euro 19,999
- b) Euro 20,000 - Euro 39,999
- c) Euro 40,000 – Euro 59,999
- d) Euro 60,000 – Euro 79,999
- e) Euro 80,000 - Euro 89,999
- f) Euro 90,000+

A policy review of the account shall be conducted to ensure the customer is properly risk assessed and to corroborate as much of the SOW/F information provided as possible via open source intelligence and research shall be carried out on those customers for which there is a concern in relation to the funding of the account or upon review. If there is a mismatch between the information provided by the customer and background research, this could lead to a ML/FT concern leading to the customer being risk-rated High and SOW/F documentation requested to corroborate SOW/F information provided.

Mandatory Enhanced Due Diligence

EDD will be conducted in the following situations:

- customer is determined to be a high net worth individual who has over two million (2M) Euro in total assets this shall be carried upon review;
- customers with multiple revenue streams from which the provenance of funds is not easily identified;
- customers receiving funds to or from high-risk or non-reputable jurisdictions as per internal jurisdiction risk assessment this shall be carried out upon review of the account;
- customers who are from a high risk or non-reputable jurisdictions as per internal jurisdiction risk assessment;
- customer triggers any of the transactional or fraud triggers shall be temporarily placed on EDD until the situation is rectified and documentation obtained, if not such shall be raised to the MLRO;
- customer deposits more than Euro 10,000 in a 365-day period; and
- customer net losses reached Euro 30,000 in a 365-day period.

Customers at the CDD level shall be rated EDD temporarily until the SOW/F shall be requested if either of the above thresholds are reached. If at the time the above thresholds are reached, the customer is rated as medium risk (CDD), then the customer is only temporarily rated as a High Risk (EDD) until SOF/SOW is verified, at which point the customer goes back to medium risk (CDD). If the customer's SOF/SOW is not verified the account is suspended and the customer will remain on the EDD level. If they wish to reactivate the account, the customer will have to provide SOF/SOW verification documentation.

Should the customer exceed such a threshold, the customer will be prompted to provide the source of funds for the transactions, and a re-evaluation of the customer's profile will be conducted.

We can only request information from the customer which assists us in addressing a concern or understanding how the customer is financing their activity. If a customer refuses to provide any information or fails to provide the necessary information within the relevant time period, we will suspend the account, stop processing any further wagering and shall be effectively blocked. The case shall be raised further with the MLRO to decide whether the case warrants further reporting to the relevant authority by analyzing activity to identify knowledge, suspicion or reason to believe ML/FT.

SOURCE OF FUNDS AND WEALTH

The Source of Funds (SOF) is how the funds used for a particular transaction (or future transactions) were generated, and the Source of Wealth (SOW) describes the activities that have generated the total net worth of a customer.

We are required to take reasonable steps to ensure that the transactions are consistent with our knowledge and profile of the customer.

SOF/SOW may be requested at any point in the business relationship depending on the CRA; for example, customers may be asked to provide SOF/SOW in the following circumstances:

- Due to ML/FT concerns on the account, the customer is deemed to be High risk following a CRA;
- Adverse media hits, especially regarding Fraud or Financial Crime;
- If a customer generates income through trading of financial assets;
- Customers who are from high-risk jurisdictions;
- A suspicion that the customer is financing their activity via funds originating from high-risk jurisdictions.

If following the request for documentation, it is found that the customer's source of wealth or funds is coming from a high-risk or non-reputable jurisdictions, such customers are to be immediately brought to the attention of the MLRO, as well as, in the following cases:

- Suspicion or confirmation of a customer's bankruptcy or tax avoidance purposes;
- The level of the customer's activity is inconsistent with their profile;
- Suspicion raised from KYC received, for e.g. fake documents or transactions from bank statement;
- A suspicion that a customer's activity is funded via a third party.

SOW/F shall be re-verified periodically according to the customer's level of risk Medium-Risk customers shall have SOW/F re-identified every 24 months and High Risk customers shall have SOW/F re-verified every 12 months. A policy review of the account is conducted and there is a mismatch on the SOW/F information provided by the customer and background research. SOW/F verification is required to corroborate the information provided by the customer.

Our focus during the SOF/SOW request shall be to understand how the customer funds their transactions. We must document and keep on file our investigations into the customer's SOW/F, including any questions asked, responses received and supporting evidence provided, which must be updated on an ongoing basis. If our team has any concerns about the source of funds, we must consider whether we need to submit a SAR to the MLRO.

Identification and verification Source of Wealth and Funds

It shall be pertinent to distinguish between the identification and verification of the source of wealth and funds. At CDD level the customer will be prompted to provide the following information to obtain an identification of the source of wealth and funds.

- Status of employment
- Proof of income (from SOW/F)
- Gross annual income

In situations where verification is required, the customer will be required to provide supporting documentation to verify the income stated in the identification process. The term identification shall be where we obtain information that is not corroborated by verification documents, for which verification shall mean evidence of the information stated is to be corroborated by reliable documentary evidence.

Source of Wealth and Funds Supporting Documentation

The source of funds and source of wealth used in a relationship with a customer can usually be established upon review of the transactions of the economic activity from where the customer obtains such funding. Below is sample documentation to be requested in the SOW/SOF process.

Salary income:

- Bank statement(s) showing receipt of salary (Documentation is to be 3 to 6 months old).
- Additional evidence, if required:
- Original or certified copy of a payslip (or bonus payment);
- Letter from employer confirming salary on company letterhead; or
- Copy of tax return annual statement.

Company profits:

- Distribution of dividends certificate;
- Bank statement clearly showing receipt and origin of the dividends (Documentation is to be 3 to 6 months old or the period of the distribution if it exceeds 6 months).
- Additional evidence, if required:
- Latest audited accounts (if self-employed/own company) and company bank statement for the past six (6) months;
- A declaration from a certified accountant stating that the company is held in good standing order, confirming dividend, share capital and profits generated. The letter shall include a declaration of beneficial ownership of the company;
- Certificate of incumbency; or
- Copy of invoices showing trading activities of sales and purchases.

Sales of shares or other investments/liquidation of investment portfolio/bonds:

- Bank statement clearly showing receipt of funds and investment company name or interest on bonds received (Documentation is to be 3 to 6 months old or the period of the sale if it exceeds 6 months).
- Additional evidence, if required:
- Certified investment/savings certificates, contract notes or cash-in statements.

Sale of property:

- Copy of contract of sale;
- Bank statement showing proceeds of the sale (Documentation is to be 3 to 6 months old or the period of the sale if it exceeds 6 months).
- Additional evidence, if required:
- A letter from a licensed solicitor or regulated accountant stating property address, date of sale, proceeds received, and name of the purchaser on letter-headed paper.

Sale of the company:

- A letter detailing company sale signed by a licensed solicitor or regulated accountant on letter-headed paper; and
- Bank statement clearly showing receipt of the sale and origin of the funds (Documentation is to be 3 to 6 months old or the period of the sale if it exceeds 6 months).
- Additional evidence, if required:
- Copies of media coverage (if applicable) as supporting evidence.

Inheritance:

- Copy of the deceased's will; and
- Bank statement(s) showing receipt of funds (Documentation is to be 3 to 6 months old or the period of the inheritance if it exceeds 6 months).
- Additional evidence, if required:
- Signed letter from a licensed solicitor or estate trustees on letter-headed paper;
- Grant of probate (with a copy of the will), which must include the value of the estate.

Loan:

- Copy of the loan agreement; and
- Bank statement(s) showing receipt of the loan
- Additional evidence, if required:
- A copy of the identification documents of the individual/s granting the loan.

Gift:

- Letter from the donor explaining the reason for the gift and the source of the donor's wealth;
- Certified identification documents from the donor; and
- Bank statement showing the origin of the gift payment clearly (Documentation is to be 3 to 6 months old or the period of the gift if it exceeds 6 months).
- Additional evidence, if required:

The donor is to provide identification documents from the following:

- Passport or national identification document; or
- Portrait photograph ("selfie") of donor holding their identification document;
- Bank statement clearly showing receipt and origin of the gift.

Fixed deposit – Savings:

- Savings statement.
- Additional evidence, if required:
- Evidence of account start, either; a letter from the account provider or the first statement;
- Additional evidence showing the origin of the savings held.

Funds generated from gambling/gaming winnings:

- Receipt of winnings; and
- Documentation (e.g. bank statement) showing the origin of the funds.

Pension:

- Bank statement showing the release of pension payment and indicating the name of the pension fund making said payment.
- Additional evidence, if required:
- Copy of the pension statement.

Mining:

- Ledger of the amount of cryptocurrency mined; and
- Wallet address and transaction hash to which the mined cryptocurrency was delivered.

Crypto-Investments

- Ledger of trades and initial investment

CUSTOMERS FAILING TO PROVIDE DUE DILIGENCE INFORMATION

Where we are unable to complete CDD measures, the general rules are that we must:

- Not carry out a transaction for the customer;
- Not accept funds from or transfer funds to a customer;
- Not establish a business relationship with a customer;
- Terminate any existing business relationship with the customer; and
- Consider whether an STR/SAR is required.

There are very limited circumstances in which the above rules will not apply, e.g. we may not be able to verify the customer's identity during establishing a business relationship. This action may be necessary to avoid interrupting the normal course of business and where there is little risk of ML. This action is only allowed on the condition that the verification is completed as soon as practicable after first contact is established.

Customers shall be given a 30-day timeframe from the date of first correspondence to respond to due diligence information requests during which the withdrawals will be blocked. If the customer does not respond to the request they will be sent reminders on day 7, 15 and 25 from the date of the first correspondence. This 30-day time period shall be extended depending on the correspondence and information provided by the customer. If the customer does not provide the due diligence information required within 30 days from the last day of correspondence, the account shall be fully blocked, and the customer when accessing their account will only be able to see the information request which will need to be answered in order to unblock the account.

ONGOING MONITORING

Ongoing monitoring is an intrinsic part of the due diligence process. It must be performed on all matters, regardless of the risk rating of the customer, to detect unusual or suspicious transactions. The primary objective of ongoing monitoring is to:

- a) 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 and that the funds are obtained from legitimate lines of business;
- b) Ensuring that the documents, data or information held by the subject person are kept up to date.
- c) Keep- up-to date information used for CDD or EDD purposes (identity and verification documents); (the system will alert those instances where the documentation is about to expire);
- d) Stay alert to changes in the customer's risk profile and anything that gives rise to suspicion; and
- e) Monitor transactions for possible indicators of ML/FT.

The company shall examine, as far as reasonably possible, the background and purpose of all transactions that fulfill at least one of the following conditions:

- a) complex transactions that have no apparent economic or visible lawful purpose;
- b) large transactions that have no apparent economic or visible lawful purpose;
- c) unusual patterns of transactions that have no apparent economic or visible lawful purpose; and
- d) transactions which are particularly likely, by their nature, to be related to ML/FT.

A policy review of the account can be conducted at the CDD threshold to ensure the customer is properly assessed. Open source intelligence is also to be used and to corroborate SOW/F information provided this shall be carried out on those customers for which have raised concern in relation to the funding of the account or upon review.

If there is a mismatch between the information provided by the customer and background research, this could lead to a ML/FT concern leading to the customer being risk-rated High and SOW/F documentation requested to corroborate SOW/F information provided.

Ongoing monitoring can trigger a further risk assessment of the customer due to transactional alerts, and if transactions are involved in the alert, they will be scrutinized to establish whether any suspicious activity or transactions are occurring.

A review of the account will be conducted as stated both on the identification and verification information and the transactions. Accounts can have their risk ratings increased via override, such will indicate that the account is to be reviewed more frequently.

Periodic Ongoing Monitoring

Accounts shall be periodically reviewed from the date of the last CRA based on the customer's level of risk:

- High Risk: 12 months (1 year)
- Medium Risk: 24 months (2 years)
- Low risk : 36 months (3 years)

The above time frames are a backstop for when an account review is required. If the customer triggers before and a review is conducted, the periodic review timer restarts and is set from the date of the last customer review.

The company monitors ongoing business relationships and assesses transactions in order to detect activities and transactions that:

- Deviates from what the company has reason to expect based on its customer due diligence, knowledge of the customer, their business and risk profile.
- Deviates from what the company has reason to expect based on its due diligence of other customers and the products and services, as well as the information provided by the customer and other circumstances.
- Display any unusual patterns of behavior that may indicate illegal activity. Are likely to be part of money laundering and/or financing of terrorism.

Risk factors to be given particular consideration in the monitoring of business relationships and transactions include:

- Gambling or transaction patterns that differ from what is normal or what the customer indicated when the business relationship was established.
- The customer carries out unusually large transactions.
- The customer requests withdrawal to a different account than the account that has been verified to belong to the customer (it is noted that such withdrawals are not possible).
- The customer requests to transfer their gambling account or winnings to someone else (it is noted that such transfers are not possible).

CDD: IP Check

The customer's IP address is registered. Upon registration, a review is done as to whether the customer's IP address corresponds to the registered country. If there is a mismatch, the customer account is marked for further checks.

CDD: Double Customer Check

Every customer can open only one account per brand. If a customer tries to open multiple accounts, these will be blocked. The company has measures in place to deter customers from being able to open multiple accounts.

Transaction monitoring

Transaction monitoring shall be based on:

- Automated software (the transactions will be reviewed in real-time);
- Post transaction monitoring the depending on the risk assessment of the customer meaning the review frequency of the account holistically; and
- Triggers, rules and events.

Transaction monitoring is not only determined by the level of risk posed by the customer, but there are also triggers based on (but not limited to) if the customer is exceeding their expected level of activity as determined by the customer's profile IP changes, large or complex transactions and on the rationale behind the activity of the customer.

The company's transaction monitoring is conducted on a risk-based approach under which the intensity of measures preventing ML and/or FT depends on the level and nature of the identified risks. Where a higher risk of ML and/or FT is detected, a more enhanced and focused approach is used and stricter thresholds, rules and measures are implemented. If discrepancies or suspected activities/transactions are noted, the company assesses whether there are reasonable grounds to suspect ML and/or FT or that property otherwise derives from criminal activity.

Employees must report any suspicion of ML and/or FT to the company's MLRO for controlling and reporting obligations. In case of deviation or suspicious activities/transactions, the customer's risk profile is also updated.

Deposit without wagering

It is important to note that due to the current AML/CFT regulations, the customer may deposit money only in order to play and use our services. Therefore, the company adopts a procedure whereby the deposits must be wagered at least once before a withdrawal can be processed.

The company is not a financial institution or credit institution and does not grant interest on deposits. In any case, it reserves the unlimited right to apply certain restrictions to the payment methods if selected.

INTERNAL REPORTING

Suspicious activity

Suspicious activity is any customer activity that is outside of the ordinary, in other words activity that is not normal or expected activity given the customer's profile. All suspicious activity must be investigated and given due consideration. Therefore, it is crucial that the MLRO understand the customer profile, as this understanding is used to determine if there is knowledge, suspicion, or reason to believe that the business or customer is engaging in money laundering or terrorist financing activities.

Any unusual customer activity or transactions that are not commensurate with the established profile of the customer should be considered as a potential indicator of suspicious activity. Following the detection of any potential suspicious activity, the subsequent investigations should establish the reasons for the unusual activity or transaction in order to either eliminate or confirm the suspicion raised. If it is confirmed, the transaction and or the activity must be reported to the MLRO as soon as possible. Failure to do so is an offense that could result in immediate relief of duty.

Internal escalation

Customers involved in any form of suspected fraudulent activity suspicion, knowledge or reason to believe that money laundering or funding or terrorism, funds or any involvement in activities related to terrorism or/ and any suspicious transaction or activity will be reported to the appropriate authorities within the stipulated time frame of immediately upon raise of suspicion. This refers in particular to the illegal depositing of funds obtained from ill-gotten means.

The MLRO must determine if the information contained in the report does give rise to a knowledge, reason to believe or suspicion of ML/FT in which case the MLRO should proceed to submit a STR/SAR to the FIU in a prompt manner and avoid any unnecessary delays. If there are instances where the request for further information to make a determination on whether to report, the MLRO shall instruct a time frame by which the information is to be received. In instances where the customer does not collaborate or provide further information such is deemed to raise more suspicion and the report shall be submitted to the FIU accordingly.

Failure to report

Making a SAR/STR to the MLRO can be a defense to a principal money laundering or funding of terrorism offense. Failing to make a SAR/STR to the MLRO where the person knows, has reason to believe or suspect money laundering is an offense in itself which is punishable by immediate relief of duty.

Tipping-off and prejudicing an investigation

Personnel will commit the tipping-off offense if disclosure is made to the individual customer to whom the disclosure relates to and that any other individual not pertaining to the designated individuals within the AML/CFT unit that the company has:

- Made a SAR/STR to the MLRO
- Made available information pertaining to the customer
- Disclose information that is likely to prejudice any investigation that might be conducted following the SAR/STR has been submitted

Personnel will commit the prejudicing of an investigation offense if disclosing to any third party that an investigation is being contemplated or is being carried out and. Tipping-off can be carried out either prior to an SAR/STR being submitted or after such submission has been made. Staff will not commit tipping-off by discussing concerns with or submitting a SAR/STR to the MLRO.

Tipping off offense cannot be committed if a report has not been submitted and personnel liaise with customers or colleagues as part of their enquiries into an unusual activity. However, personnel cannot disclose information or leak information about any suspicion being raised. Personnel can make enquiries to obtain further information to help to decide whether there is suspicion, knowledge or reason to believe, and remove any concerns that personnel have pertaining to a case that has been cleared, although such information must be kept internally.

It is also not tipping-off to warn customers of the duties under the AML/CTF regime by providing them with the company's terms of business

EXTERNAL REPORTING

The company takes any form of illicit activity very seriously, and any fraudulent activity is strictly prohibited. Fraudulent activity may include, but is not limited to:

- Forgery of documentation;
- Collusion (for which such is not possible at the current stage of operation);
- The use of impermissible software tools to render the customer anonymous;
- The provision of false registration data or other requested information;
- Any red flag identified above.

Where there is suspicion, knowledge or reasonable grounds to suspect that the customer is involved in fraudulent activity, ML/ FT will be reported to the appropriate authorities within the stipulated time frame, which is immediately upon the suspicion being raised. All personnel have direct access to the MLRO, and such reports should be raised immediately. The MLRO will then be responsible for reviewing the report and to escalate to the relevant FIU accordingly.

Once an STR/SAR has been escalated, it will be included in a STR/SAR central repository within the company. The company shall at all times retain any STR/SAR as follows:

1. Reports raised to the FIU;
2. Reports not raised also hold information on why the report was not raised.

The company may occasionally receive requests for information or notifications from regulatory authorities or law enforcement bodies regarding investigations of a criminal, civil or regulatory nature. When such requests for information are received, these are to be forwarded in their entirety to the company MLRO.

The company's MLRO will handle and process these requests in line with the following process;

- Record the receipt of such a request;
- Verify the legitimacy of the requesting company and individual making this request;
- Verify the legal basis under which such a request is made;
- Identify the customer account(s) relevant to the request;
- Analyze the customer information, including, amongst others, due diligence, transactions and ongoing monitoring information;
- Re-consider the customer's risk status considering the received request and take appropriate action depending on the case;
- Identify information that is relevant to the request and following a due assessment of the information, prepare and provide the information to the requestor; and

- Update the company records in respect of such a request and where appropriate, notify the relevant regulators or authorities with follow-up actions as per relevant regulatory obligations.

Reporting of suspicious activity or transactions and requests for information shall be done via the GOAML system by the MLRO.

The authorities will review the suspicion on information provided and send an acknowledgement within 24 hours. If more information is required, the MLRO will request it from the contacting person. In this time, transactions are not to be carried out without the consent of the MLRO. If the MLRO gives consent to proceed with a transaction, then that consent only applies to that specific transaction. If the customer requests further activities or transactions, further consent is required from the MLRO. Unless instruction has been given to terminate the business relationship.

One may raise an STR/SAR holding article 28 (referred to as TRN Report in GOAML) where if no response has been received within 24 hours from the SAR submission, the transaction can proceed unless the MLRO gives specific instructions to return the funds and block the account.

REQUESTS FROM AUTHORITIES

The company may occasionally receive requests for information or notifications from regulatory authorities or law enforcement bodies in relation to investigations of a criminal, civil or regulatory nature. When such requests for information are received, these are to be forwarded in their entirety to the MLRO.

EMPLOYEE SCREENING

It shall be the company's policy that new employees are to provide the following:

- Passport or I.D.;
- Proof of address; and
- where required, police conduct.

The company prior to engagement, shall run a PEP & Sanction check on potential employees, and the individual shall also be duly requested to obtain references from previous employers.

A copy of the due diligence required shall be kept on file for individuals that are required to hold positions which must be approved. Such shall be carried out at a minimum annually for the duration of the employment.

The company will monitor the activities of its employees during their employment to identify concerns of internal fraud or other criminal activity potentially affecting the company's operations. Employees are also encouraged to report internal suspicious or fraudulent activity by employees to the MLRO, and should they wish to remain anonymous, this can be done via an anonymous letter.

EMPLOYEE TRAINING

The company will develop ongoing employee training under the leadership of the MLRO and senior management. The company is obliged to provide training in relation to AML & CFT due to compliance requirements. Such training is compulsory and shall be completed by every employee as soon as possible upon commencement of employment and shall be refreshed at least annually. The training will be provided at different levels throughout the organization, for which all personnel shall be subject to at least a minimum level of understanding of AML/CFT and the internal policies concerning AML/CFT. The training will include, at a minimum:

How to identify red flags and signs of ML that arise during the employees' duties;

- What to do when risks are identified, including how, when and to whom to escalate unusual customer activity or other red flags and, where appropriate, to report;
- What employee' roles are in the company's compliance structure, and how to perform them;
- The company's record retention policy; and
- The disciplinary consequences (including civil and criminal penalties) for non-compliance with this Policy or applicable laws.

Additional specific training is provided to employees whose specific job in whole or in part is to oversee that no ML or FT occurs using the company's services. This training will be more specific and role-focused e.g. payments personnel may undergo further training

regarding how to recognise AML transaction red flags, AML personnel will receive more in-depth AML training. Training will be tailored and updated based on the typologies and trends in the industry to ensure that all relevant staff are kept abreast of the AML/CFT landscape, both from a regulatory and business perspective.

All training provided to an employee, or which the employee participates in, shall be recorded within the Company's training records and provided upon request. The Company ensures the suitability of the persons employed to carry out tasks relevant to the prevention of ML/FT.

The Know Your Employee (KYE) assessment is based on the carrying out of interviews and the collection of where required certificates, references, identification documents (passport/identity card), and police conducts. The analysis of the interview and the documents collected are used to decide on employment matters. The KYE documentation obtained prior to the onboarding of the individuals is reviewed by HR every 2 years from the start of the individual's employment with the company. New employees would also need to undergo training. A probation period is applied where deemed appropriate so that the company may, if necessary, take a quick action with regards to unsuitable persons operating with the company's operations.

POLICY COMPLIANCE AND REVIEW

Compliance will be continually monitored through any or all of the following methods: file audits; review of records maintained; reports or feedback; and any other method.

We will review this policy at least annually as part of our overall risk management process. We will also review this policy if:

- There are any major changes in the law or practice;
- We identify or are alerted to a weakness in the policy; or
- There are changes in our business, our customers or other changes which impact this policy.

RECORD KEEPING

The company shall retain the following documents and information for a period of five years after the customer relationship is terminated. Upon expiry of the retention periods referred to above, the Company shall delete all personal data unless otherwise instructed by a relevant authority. The documents may be requested to be kept for an additional five-year period or if it shall be considered necessary not to jeopardize any investigation or ongoing investigation, kept for the duration communicated by any relevant or investigative authority.

A list of documentation to be kept for a period of five years are:

- Policies and documentation;
- A copy of the BRA any changes or resolutions;
- A copy of the CRA and any changes;
- Copies of all policies and procedures, internal controls and compliance management.
- Customer due diligence:
- A copy of all documentation received from the customer;
- A copy of any correspondence received from the customer;
- Information on the purpose, nature and expected activity;
- All transactions;
- Supporting documentation for transactions;
- Customer Risk Assessments.

Related to the MLRO:

- Internal reports made to the MLRO;
- Reports escalated to the FIU, and follow-up submission;
- Reports including rationale of reports not filed with the FIU;
- Copy of any agreements with any vendor or third-party provider.

All Information and documentation collected for CDD purposes must be in a language that is understood by employees responsible for AML/CFT. Where information and documentation is obtained in a language that is not understood, a translation is to be made and a copy of the translation kept on file for ease of reference.

AUDITING

The company will outsource its audit function that is independent and responsible for reviewing the internal guidelines, controls and procedures for complying with its obligations under the applicable regulations.

Even though such a function will be outsourced, ultimate responsibility lies with the company. Such function reviews and regularly assesses whether the company's:

- 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.

In addition, the company's AML/CFT policy is audited on an annual basis to ensure the effectiveness of such internal controls. The independent audit function provides recommendations to the relevant persons based on the observations made by such an audit function and ensures that these actions are implemented. The audit shall also evaluate Company Name'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.

Examination by the CGA

Company Name 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.

WHISTLEBLOWING PROCEDURE

All employees may disclose information regarding improper practices by their employers or other employees and to protect employees who make said disclosures from detrimental actions. Employees may file a report to the whistleblower via email.

DATA PROCESSING AND RETENTION

Processing of special categories of personal data

Special categories of personal data in the meaning of Article 9.1 of Regulation (EU) 2016/679 ("GDPR") may be processed if necessary, to:

- a) Assess if the customer is a PEP or family member or a person known to be a close associate to a PEP.
- b) Assess the customer's risk profile.
- c) Assess suspicious transactions/activities and comply with the monitoring obligation.
- d) Provide information to the police in accordance with these guidelines and answer questions from the police regarding ML and/or FT.
- e) Retain documents and data if it is permitted to process them in accordance with (a)-(d).

Personal data referred to in Article 10 of the GDPR (relating to criminal convictions and offenses) may be processed under the conditions set out in points (b)-(e) above.

Retention of documents and data

The company retains documents and data for five years from the end of the business relationship where it concerns:

- CDD and EDD information and documentation
- Transactions subject to CDD and EDD requirements, documents and data retained for ten years, when:
 - Documents or information indicate ML and/or FT or otherwise derive from criminal activity.

- The customer's account has been reported to the FIU in accordance with these guidelines.
- An authority has informed the company that such documents or data need to be retained for a longer period of time.

The retention period is calculated from performance of the measures/transactions or where a business relationship has been established, the relationship was terminated. If a single transaction has not been executed as a result of suspicion of ML and/or FT, the retention period is calculated from the time the decision was made not to execute it.

The documents/data is dated and stored safely (electronically or paper) and is easy to identify, obtain and compile.

APPROVED AND SIGNED BY

Jorge Luis Castillo obo FO Management Ltd.	Managing Director	30/05/2025	Signature Signed by: <i>Jorge Luis Castillo</i> 65BCCEA8C2A74F0...
Miodrag Miletikj	MLRO	13/05/2025	Signature Signed by: <i>Miodrag</i> 3FB1D1E1B5874D5...