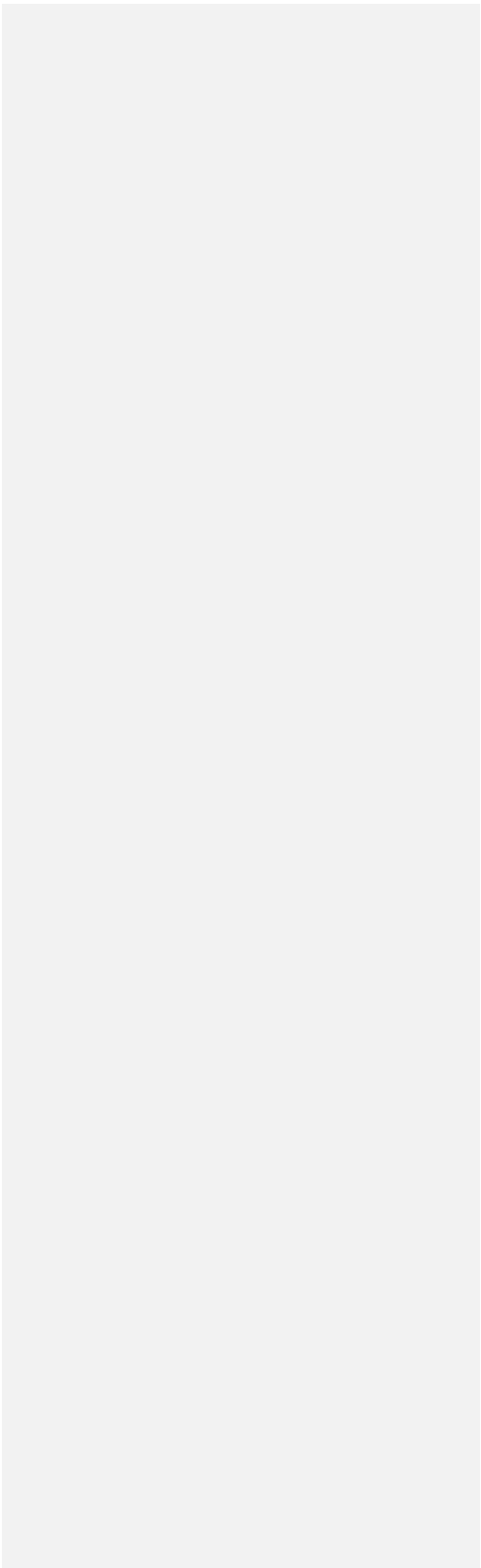


**01.01.2024**

**AML/CFT Policy**  
**Cetus Technology N.V**



|                                                                                         |          |
|-----------------------------------------------------------------------------------------|----------|
| <b>Table of Contents</b>                                                                |          |
| <b>Introduction</b>                                                                     | <b>5</b> |
| <b>Scope</b>                                                                            | <b>5</b> |
| <b>Laws and Applicable Legislations</b>                                                 | <b>5</b> |
| <b>Notice</b>                                                                           | <b>6</b> |
| <b>Policy Objectives</b>                                                                | <b>6</b> |
| <b>Governance</b>                                                                       | <b>7</b> |
| <b>Anti-Money Laundering (AML) &amp; Countering Funding of Terrorism (CFT) Policy</b>   | <b>7</b> |
| <b>Understanding Money Laundering and Funding of Terrorism</b>                          | <b>7</b> |
| What is money laundering and terrorist financing?                                       | 7        |
| Why are anti-money laundering and counter-terrorist financing important to the Company? | 8        |

|                                                                  |           |
|------------------------------------------------------------------|-----------|
| The cycle of Money Laundering                                    | 8         |
| Money Laundering Offences                                        | 8         |
| Offences relating to money laundering                            | 8         |
| Typical signs of Money Laundering and the Financing of Terrorism | 9         |
| Terrorist financing                                              | 10        |
| Terrorist Financing Offences                                     | 10        |
| <b>Customer Screening</b>                                        | <b>11</b> |
| Negative Media                                                   | 11        |
| Financial Sanctions                                              | 12        |
| <b>Freezing of assets</b>                                        | <b>12</b> |
| Politically Exposed Persons (PEPs)                               | 13        |
| <b>The Role of the MLRO</b>                                      | <b>14</b> |
| MLRO Responsibilities                                            | 14        |
| <b>Reporting Procedures</b>                                      | <b>15</b> |
| Suspicious activity or transaction                               | 15        |
| Internal reporting                                               | 15        |
| <b>External reporting</b>                                        | <b>16</b> |
| Failure to report                                                | 16        |
| Tipping-off and prejudicing an investigation                     | 16        |
| Requests for information                                         | 17        |
| <b>Business Risk Assessment (BRA)</b>                            | <b>17</b> |
| <b>Customer Risk Assessment (CRA)</b>                            | <b>18</b> |
| Onboarding of New and Prospective Customers                      | 19        |
| Timing of Due Diligence Measures                                 | 20        |
| LEVEL 1: Customer Due Diligence (CDD)                            | 20        |
| LEVEL 2: Customer Due Diligence (CDD)                            | 20        |
| Identification Verification                                      | 20        |
| Address verification                                             | 21        |
| LEVEL 3: Customer Due Diligence (CDD)                            | 22        |
| Information on the economic profile                              | 22        |
| LEVEL 4: Enhanced Due Diligence (EDD)                            | 23        |
| Mandatory Enhanced Due Diligence                                 | 24        |
| Identification and verification Source of Wealth and Funds       | 25        |
| Source of Wealth and Funds and Supporting Documentation          | 26        |
| Customers Failing to Provide Due Diligence Information           | 27        |
| Ongoing and Transaction Monitoring                               | 27        |
| Transaction Monitoring                                           | 29        |
| <b>Employee Screening</b>                                        | <b>30</b> |
| <b>Record Keeping</b>                                            | <b>30</b> |
| <b>Internal Auditing</b>                                         | <b>31</b> |
| <b>Employee Screening</b>                                        | <b>31</b> |
| Employees Training                                               | 32        |
| Periodicity                                                      | 32        |
| Training Records                                                 | 32        |
| <b>Policy Review</b>                                             | <b>32</b> |

## Introduction

Cetus technology n.v

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 offences 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 licence held within the Maltese jurisdiction 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 in accordance with their respective roles and responsibilities within the company;
- Attend any relevant training and updates provided by the Money Laundering Reporting Officer (MLRO) 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 companies management and employees.

## Laws and Applicable Legislations

Relevant ML and CFT legislation:

- Directive (EU) 2018/843 of the European Parliament and of the Council suggested:

The policies set forth herein (the "Policies") are intended to satisfy the statutory requirements of the relevant legislation and to provide direction to Cetus Technology (the "Company") in complying with its obligations at law by taking all reasonable steps and exercising all due diligence to avoid the commission of an offence of money laundering or funding of terrorism. Based on the requirements of various statutory obligations, including the National Ordinance when rendering services, the National Ordinance on reporting of unusual transactions, the Sanctions National Ordinance, and the Kingdom Sanctions Act, and the Regulations for Combating Money Laundering, Financing of Terrorism, and the Proliferation of Weapons of Mass Destruction, and other pertinent legal instruments (collectively "Curacao AML/CFT laws", please vide the Communication from the Curacao Gaming Control Board (Ref: GS/U215/24), pg 1 et seq), the Company has taken a position on who can and cannot be accepted as a customer.

The Company is aware that criminals and terrorists may attempt to use the Company's services to channel funds from illegal activities.

The National Ordinance on the Reporting of Unusual Transactions (NORUT) provides indicators to help identify unusual transactions. These indicators (consisting of objective and subjective indicators) describe when an (executed or intended) transaction is to be labelled as unusual, and thus should be reported to the pertinent national authorities. The Curacao AML/CFT laws also provide statutory obligations which the Company shall adhere to as to indicators and regulations as to customer acceptance or otherwise.

- 

Commented [1]: Add relevant legislations of Curacao

Formatted: Font color: Auto

## Notice

All employees will be asked to read this manual and any ancillary documentation provided by the Company and are to confirm 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 document (the "Policy") sets out practical guidance to all users in gaining awareness and understanding of the relevant Anti-Money Laundering (AML)/Countering the Financing of Terrorism (CFT) obligations under the relevant 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 Company endeavours to comply with the obligations under the AML/CFT laws, regulations and directives, and under the data protection legislation. 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.

## Policy Objectives

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 and 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 and CFT risks at all stages of the business relationship with its customers.

The company and its staff 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), anti-fraud and anti-corruption measures, which have been designed to effectively mitigate against the risk of financial crime.

The Company must have systems and controls to counter and prevent the furtherance of financial crime. As a regulated business, the Company has implemented an AML/CFT risk framework and a risk management strategy to reduce its exposure to financial crime risks.

The Company, its staff, and agents (where applicable) must take all reasonable steps to anticipate and prevent having its services or products 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.

Any technical queries or concerns on specific policy provisions and requirements should be directed to the MLRO being the Money Laundering Reporting Officer.

## Governance

The Company adheres to the three lines of defence 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 defence are being:

1. The first line of defence 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.
2. The second line of defence is the Money laundering reporting officer and the compliance team, who are tasked with the compliance monitoring, point of contact to the regulators, reporting of suspicious transaction, set policies and standards
3. The third line is the external audit and internal audit.

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 external 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.

## Anti-Money Laundering (AML) & Countering Funding of Terrorism (CFT) Policy

The Company has implemented a minimum 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 for all relevant employees.

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 (insert 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 authorised 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.

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

The anti-money laundering (AML) and counter-terrorist financing (CTF) regime is designed to prevent our services being used by criminals and bad actors. The Company has regulatory obligations to identify, analyse 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 licences.

### 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. Therefore, during the place stage, it is very important for the company to understand where the funds utilised 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.

#### 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.

### 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.

### Money Laundering Offences

There are some money laundering offences:

- The principal offences
- Failure to disclose offences
- The offences of tipping-off and prejudicing an investigation

### Offences relating to money laundering

#### Money laundering offences consist of individuals or entities who

1. conceals, disguises, converts, transfers or removes from the jurisdiction property which is, or represents, the proceeds of crime which the person knows, or suspects represents the proceeds of crime
2. enters into an arrangement which he knows, or suspects facilitates (by whatever means) the acquisition, retention, use or control of criminal property by or on behalf of another person
3. acquires, uses or has possession of property which he knows, or suspects represents the proceeds of crime
4. fails to disclose to the MLRO (in the regulated sector), knowing or suspecting or having reasonable grounds for knowing or suspecting that another person is engaged in money laundering or terrorist funding – this applies to any individual at whatever level (employee, manager, director)
5. fails to disclose when knowing or suspecting or having reasonable grounds for knowing or suspecting that another person is engaged in money laundering or terrorist funding – this applies to the MLRO or sole proprietor of a business
6. 'tips-off' any person that a disclosure has been made, knowing or suspecting that doing so is likely to prejudice an enquiry
7. makes a disclosure which is likely to prejudice a money laundering investigation or falsifies, conceals, destroys or otherwise disposes of documents which are relevant to the investigation

**Deleted:** There are three principal money

**Deleted:** Money

**Deleted:** laundering offences covering criminal activity and two related to money- laundering offences. These are shown below:

### Typical signs of Money Laundering and the Financing of Terrorism

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.

- Obstructive or secretive customers;
- Cases or instructions that change unexpectedly or for no logical reason, especially where:
- The customer has deposited funds with the company, and the origin of the funds is unknown;
- The transfer of assets changes at the last moment; or,
- Is requested to return assets or send assets to a third party.
- Loss-making transactions where the loss is avoidable or obvious;
- 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 (e.g. Iran, Uzbekistan, Turkmenistan, Pakistan, Sao Tome and Northern Cyprus. Kindly refer to the jurisdiction risk assessment);
- 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;
- "High-End" transactions involving substantial value and the use of the formal financial sector, such as solicitors, accountants, and other professionals (i.e. any other "professional enablers");
- 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.

## Terrorist financing

Terrorist financing is a very serious threat to financial services and businesses and must be taken as seriously as money laundering.

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.

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 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:

- <http://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.

### Terrorist Financing Offences

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.

All offences carry heavy criminal penalties. While the terrorist financing and money laundering regimes are different, they share similar aims and structures. Terrorist financing is a very serious threat to the business, and must be taken as seriously as money laundering.

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.

### Customer Screening

As a licenced entity, the Company recognizes the importance of the customer profile and has in place practises to comply with the laws and regulations in relation to, identification, verification and screening of new and existing customers for sanctions, political exposure and negative 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 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 on first deposit and on a daily basis thereof.

Commented [2]: outdated - use <https://www.sanctionsmap.eu/#/main>

and

<https://data.europa.eu/apps/eusanctionstracker/>

Commented [3]: what system is being used also what is the frequency? when will the first one be done?

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.

#### Negative Media

Negative media shall be deemed as information or intelligence, whether proven factual or alleged, related to serious financial crime, Terrorism, fraud, narcotics, or any crime that has an element of or could lead to ML/FT. Negative Media Screening is to be conducted when establishing a business relationship with a customer. Instances where a customer is connected to Negative Media, will be evaluated prior to granting a business relationship. Negative Media hits showing predicate offences of ML such as mafia, forgery, drug trafficking and fraud and terrorism amongst many others, shall be reported due to the sensitivity of the crime and the involvement of financial crime. Should any predicate offence raise concerns, they shall be raised with the MLRO accordingly.

#### Financial Sanctions

If a customer is listed under any sanction, even those not enforceable under local legislation such as OFAC or 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.

#### Freezing of assets

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. The sanctions followed are as follow;

Commented [4]: what system is currently being used please specify and also specify the fuzzyness used

UNSCR 1267 (1999) - Recalling the relevant international counter-terrorism conventions and in particular the obligations of parties to those conventions to extradite or prosecute terrorists, Strongly condemning the continuing use of Afghan territory, especially areas controlled by the Taliban, for the sheltering and training of terrorists and planning of terrorist acts, and reaffirming the conviction that the suppression of international terrorism is essential for the maintenance of international peace and security and hereby also determining the Freeze funds and other financial resources, including funds derived or generated from property owned or controlled directly or indirectly by the Taliban, or by any undertaking owned or controlled by the Taliban, as designated by the Committee established by, and ensure that neither they nor any other funds or financial resources so designated are made available, by their nationals or by any persons within their territory, to or for the benefit of the Taliban or any undertaking owned or controlled, directly by the Taliban, except as may be authorised by the Committee on a case-by-case basis on the grounds of humanitarian need;

UNSCR 1373(2001) - The Security Council hereby declares that the criminalised the wilful provision or collection, by any means, directly or indirectly, of funds by their nationals or in their territories with the intention that the funds should be used, or in the knowledge that they are to be used, in order to carry out terrorist acts; and to Freeze without delay funds and other financial assets or economic resources of persons who commit, or attempt to commit, terrorist acts or participate in or facilitate the commission of terrorist acts; of entities owned or controlled directly or indirectly by such persons; and of persons and entities acting on behalf of, or at the direction of such persons and entities, including funds derived or generated from property owned or controlled directly or indirectly by such persons and associated persons and entities;

UNSCR 1718(2006) - Aimed at the security council condemning nuclear tests by democratic people's republic of Korea Member States were bound to act against those activities and freeze the assets of involved entities and individuals of the DPRK. It would provide for an inspections regime to ensure compliance with its provisions, building on the existing work of the Proliferation Security Initiative. `

UNSCR 1737(2006) - Iran's failure to halt uranium enrichment such resolution declares the freezing of assets of those being engaged or directly associated with providing support for Iran's proliferation of sensitive nuclear activities.

Council Regulation (EC) No. 329 of 27 March 2007 concerning restrictive measures against the Democratic People's Republic of Korea, whereby instructs that funds shall be frozen, and no funds or economic resources shall be made available whether directly or indirectly or be made available for the benefit or a natural or legal person entities or bodies.

Further regulations consist of EU Regulations implementing these UNSCRs such as Council Regulation (EC) No. 2580 of 27 December 2001, Council Regulation (EC) No. 881 of 27 May 2002.

Further resolutions can be found and updated from, <https://www.un.org/securitycouncil/content/resolutions-adopted-security-council-2019>,

such resolutions are in tandem with the current situation or situations of unrest within a particular jurisdiction.

- All the above-mentioned regulations and resolutions lead to the following main salient points being:
- All funds are to be frozen including also 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 terrorist financing, he/she should immediately inform the MLRO by following internal reporting procedures.
- If the MLRO knows, rather than suspect, 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.

Note: Details of how any of the above may manifest itself are detailed in the business risk assessment. The manifestation of risk and the processes are further described hereunder.

## Politically Exposed Persons

### (PEPs)

A Politically Exposed Person 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:

- Heads of State, Heads of Government, Ministers, Deputy or Assistant Ministers, and Parliamentary Secretaries.
- Members of Parliament or similar legislative bodies.
- Members of the governing bodies of political parties.
- 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.
- Members of courts of auditors or of the boards of central banks.
- Ambassadors, charges d'affaires and high-ranking officers in the armed forces.
- Members of the administrative, management or supervisory boards of State-owned enterprises.
- 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
  - the spouse, or a person considered to be equivalent to a spouse, of a politically exposed person;
  - the children and their spouses, or persons considered to be equivalent to a spouse, of a politically exposed person;
  - the parents of a politically exposed person;

Persons known to be close associates means:

- 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;
- 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.

When a customer is flagged as a PEP, or is a family member of a PEP, or is a person known to be a close associate to a PEP; in addition to the regular CDD measures applied on the account, further measures are undertaken. Such customers are classified as high risk as per the Company's AML Policy and this Policy.

These additional measures include applying enhanced due diligence measures, monitoring the transactions/activities to an increased extent on an ongoing basis, and requesting information as to the source

of funds and source of wealth of the individual registering the account, if this is not already held.

Once a PEP customer is confirmed, the relevant Senior Management's approval is sought for the decision to be taken as to whether to continue with the business relationship or terminate the customer's account. This is also based on the recommendation of the MLRO.

Once an individual occupies the role of PEP, for 12 months following the individual ceasing to be a PEP, the Company shall still classify that individual as a PEP.

## The Role of the MLRO

The role of the MLRO shall be to:

- Receive reports from the subject person's employees, or through software solutions used to analyse 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 FIU.
- Respond promptly to any request for information made by the FIU.

## MLRO Responsibilities

The MLRO is responsible for continually checking that the Company complies with its AML/CFT obligations under the applicable regulations.

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 on AML/CFT rules.
- Informing and training the relevant employees on AML/CFT rules.
- Continuously briefing the relevant employees 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 persons 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.

## Reporting Procedures

### Suspicious activity or transaction

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.

### Internal reporting

The Company takes any form of illicit activity very seriously. Fraudulent activity, including acts of ML and FT, as determined at the Company's sole discretion 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.

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 escalated to the MLRO upon **immediate** raise of knowledge or suspicion via the Suspicious Transaction/Activity Report Form by submitting it electronically via email.

All personnel have direct access to the MLRO, and such reports should be raised **immediately**. Failure to do so is an offence that could result in immediate relief of duty.

### External reporting

Upon the escalation of an internal SAR/STR to the MLRO, 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 such a 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 there is a request for further information, to make a determination on whether or not 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 to be deemed to raise more suspicion and the report shall be submitted to the FIU accordingly. External reporting of such shall be **immediately** escalated 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 staff.

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.

#### **Record keeping by MLRO**

Once an STR/SAR has been escalated, it will be included in a STR/SAR central repository within the organisation. The Company's MLRO 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.

#### **Failure to report**

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

#### **Tipping-off and prejudicing an investigation**

Personnel will commit the tipping-off offence 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 an SAR/STR to the MLRO and/or submission of SAR/STR to the FIU
- Made available information pertaining to the customer
- Any information demanded by or transmitted to the FIU within the context of ML/TF analysis
- Any ML/TF investigations on a 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 offence 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. Personnel will not commit tipping-off by discussing concerns with or submitting a SAR/STR to the MLRO.

Tipping off offence cannot be committed if a report has not been submitted and you liaise with customers or colleagues as part of your enquiries into an unusual activity. However, one 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.
- Remove any concerns that personnel has 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 our terms of business.

#### **Requests for information**

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 Company legal counsel and the MLRO:

Depending on the nature of the request and whether the request for information is in relation to AML/CFT, the Company 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 organisation and individual making this request;
- Verify the legal basis under which such a request is made;
- Inform the requesting organisation that the request is being looked into and provide the appropriate contact information for the legal counsel and MLRO;
- Identify the customer (or customers) accounts relevant to the request;
- Analyse the customer's 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 for provision to the requestor, if any; 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.

## 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. Every Company employee is made aware of BRAs and updates, knowledge of which is tested periodically.

The Company activity has undertaken the obligation of conducting a Business Risk Assessment whereby all products / services / verticals and jurisdictions are given due consideration. A qualitative and a quantitative approach has been undertaken and the result of which was scrutinised through the application of a quantitative approach, through which assesses the risk posed by the customer, products, payment, transaction, interface, and geography.

The policies and procedures are influenced by the business risk assessment assessing the inherent and residual risk of risk factors and manifestation thereof. As a must every employee is to be made aware of such policy and knowledge of which is tested periodically.

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:

- Product / Service

- Transaction
- Jurisdiction
- 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 summarises the factors into low, medium and high risk. Due to the nature and evolving technology, the BRA shall be carried out every six (6) months.

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)

A risk-based approach describes the process to which the Company ensures that the systems and controls are based on the risk of money laundering the Company is facing. By identifying and assessing the money laundering risks posed by its customers, the Company can take the best steps to mitigate and monitor those risks.

Having an understanding of the risks that may arise from various factors, the Company has developed sound risk management practices to assist the officers involved in the process and tools to manage the risk posed by the threats of ML, FT or other illicit activity.

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

- Risk assessment: The risk assessment is in place to indicate behavioural 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.

The risk scoring mechanism encompasses the following risk factors:

1. Jurisdiction risk
2. Customer risk
3. Interface risk
4. Product risk
5. Payment and transaction risk

Risks may be cleared following a manual 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.

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

**Commented [5]:** how is the business risk assessment undertaken? is the business risk assessment carried out including also the controls currently in place

**Commented [6]:** here you are explaining the Risk Based Approach not the CRA, kindly draft section specific to your CRA and also what the weightings are and what documents are requested in every stage of the cra

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. Kindly follow the Risk Assessment worksheet and Methodology policy accordingly.

**Commented [7]:** create a grid showing each stage of risk being Low medium and high what is being done and what due diligence is expected to be carried out

**Formatted:** Font color: Auto

## Onboarding of New and Prospective Customers

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

The customer on account registration, shall provide the following identification information:

- First name
- Last name
- Date of birth
- Residence address
- Email and/or mobile phone number

The KYC provided will be verified electronically to 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, an automated 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 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 approval and analysis.

### Timing of Due Diligence Measures

CDD measures are to be applied when carrying out transactions amounting to 2,000 Euro or more, whether carried out within the context of a business relationship or otherwise.

#### LEVEL 1: Customer Due Diligence (CDD)

**Commented [8]:** explain simplified due diligence there is duplication

The Company CDD Level 1 requires customers to only be able to deposit to a maximum aggregate value of less than 2,000 EUR cumulatively lifetime or in one lump sum. Level 1 consists of the provision of the:

- Customer's Email and/or Mobile number
- Basic customer information:
  - Official full name
  - Date of birth (to calculate age)
  - Permanent residential address

Upon reaching the €2,000 cumulative lifetime deposit threshold, customers are classified in risk categories according to their risk profile - low, medium or high.

#### LEVEL 2: Customer Due Diligence (CDD)

**Commented [9]:** here establish a customer profile , how much is the client going to spend? what is the SOW/F information, what is the annual salary?

The Company CDD Level 2 incorporates customers whose gross deposits reach 2,000 EUR cumulatively lifetime or in one lump sum, and the risk assessment is deemed as low risk. This stage includes the following:

- Identifying and verifying the customer's identity and address via documentation;
- Identifying the beneficial owner where this is not the customer;
- Conducting ongoing monitoring of the business relationship.

Upon the Company requesting CDD documentation, a 30-day time period will start for the provision of documentation, during which withdrawals will be suspended. Upon the lapse of the 30-day time period, and CDD documentation is not provided or not successfully completed, the customer's account will be suspended from deposits and wagers as well. A determination will be made as to whether an internal SAR/STR will be deemed to be submitted to the MLRO.

#### **Identification Verification**

The customer is subject to identity verification which shall be outsourced to a third party provider and if required also have the ID document screened against [www.edisontd.nl](http://www.edisontd.nl) 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 shall be kept within the Company. All customers entering the platform shall be subject to completion of identification including PEP, FS and NM 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 licence (must hold nationality)

For the provisions relating to identification procedures and CDD requirements, proof of identity is satisfactory if:

- It is reasonably possible to establish that the customer is the person he claims to be; and
- The person who examines the evidence is satisfied that the customer is actually the person he claims to be.

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.

An assessment of the provider's systems capabilities has been carried out, and the following criteria has been met:

**Commented [10]:** here you need to mention what information are you going to obtain from the client to further measure the risk of the client. Including also, thresholds triggers and controls

- The ability of the software to assess the KYC received for validity and that the details provided match the customer's; and
- The retention of the documents uploaded shall be held in accordance with the record keeping section hereunder.

It is pertinent that the documents are held on file for a minimum of 5 years. All documents, including any correspondence or re-uploading of documentation, shall be kept on file. The time and date of actions and uploading of documents shall also be kept on file. The records may not be altered, tampered with or manipulated upon upload completion.

#### ***Address verification***

At this stage (CDD), the customer's address shall also be verified. The address is verified by obtaining 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 (see the list of acceptable address verification documentation above);
- 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 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 (level 4).

### LEVEL 3: Enhanced Due Diligence (EDD)

The Company CDD Level 3 incorporates customers whose gross deposits reach 50,000 EUR cumulatively lifetime or in one lump sum, and the risk assessment is deemed as high risk, such as if a customer is a PEP. This stage includes the following:

- Identifying and verifying the customer's identity and address via documentation with photograph;
- Collect additional personal details;
- Collect source of wealth information and documentation;
- Identifying the beneficial owner where this is not the customer;
- Obtaining details expected level of spending; and
- Conducting ongoing monitoring of the business relationship.

Upon the Company requesting CDD documentation and/or source of wealth information, a 30-day time period will start for the provision of documentation and/or information, during which withdrawals will be suspended. Upon the lapse of the 30-day time period, and documentation and/or information is not provided or not successfully completed, the customer's account will be suspended from deposits and wagers as well. A determination will be made as to whether an internal SAR/STR will be deemed to be submitted to the MLRO.

EDD is to be applied without delay in instances where the customer is likely to pose a higher than normal ML/FT risk. EDD shall require additional measures concerning where the threat is emanating from achieved via source of wealth/funds 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; See the 'Source of Funds and Wealth' sections below for more information regarding the SOW/F process;
- 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 conducting enhanced briefing with engagement teams responsible for the customer; and

**Commented [11]:** This is not permitted, the number is nowhere stipulated in the law and shall be determined based on the profile of the client. If a client does not earn that money how can he play with that amount, the client will have to have it verified earlier.

- Obtain Senior Management approval for the continuation of the relationship in cases where the doubt has been raised on approval of the customer.

#### Mandatory Enhanced Due Diligence

EDD will be conducted in the following situations:

- The customer is determined to be a high net worth individual who has over two million (2M) Euro in total assets that shall be carried upon review.
- Customers with multiple revenue streams for which are not easily identified where the provenance of funds is emanating from for which this shall be done through an override function.
- Customers receiving funds to or from high-risk or non-reputable jurisdictions as per internal jurisdiction risk assessment for which this shall be carried out upon review of the account and an override of the CRA, leaving note that account is receiving funds from high risk or non-reputable jurisdictions.
- Customers who are from high risk or non-reputable jurisdictions as per internal jurisdiction risk assessment.
- The 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.
- If the player is a PEP or a family member of a PEP or a known close associate of a PEP, the Company, in addition to the regular CDD measures, always carries out EDD measures. These include:
  - Taking appropriate steps to find out the source of wealth and source of funds used in the context of the business relationship;
  - Applying enhanced ongoing follow-up of the business relationship and monitor activities and transactions to an increased extent; and
  - Seeking approvals from Senior Management.

Commented [12]: remove

Commented [13]: Will you be accepting PEPs ?

If the customer's SOF/SOW is not verified the account is suspended and the customer will remain on the EDD level. The customer if they wish to reactivate the account will have to provide SOF/SOW verification documentation.

- SOW/F shall be re-verified periodically according to the customer's level of risk. See the 'Ongoing and Transaction Monitoring' section below for more information.
- A manual review of the account is conducted inline with CDD and if 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.
- Accounts following CRA has resulted in a High Risk;
- Accounts with a suspicious transaction pattern upon review or game play; or
- The customer is a PEP.

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 and stop processing any further wagering and shall be effectively blocked. The case shall be raised further with the MLRO or designated individuals assigned to decide whether the case warrants further reporting to the relevant authority by analysing 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 not obligated to interrogate all customers about their financial history, but we are required to take reasonable steps to ensure that the transactions are consistent with our knowledge and profile of the customer. This is part of ongoing monitoring see the 'Ongoing and Transaction Monitoring' section below for more information.

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 Medium or High risk following a CRA;
- Negative Media Hits, especially regarding Fraud or Financial Crime;
- If a customer generates income through trading of financial assets;
- Customers who are from or 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;

- 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;
- A suspicion that a customer's activity is funded via a third party.

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/STR 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 requested to reply to the source of wealth questions.

In situations where verification is required, the customer will be required to provide supporting reliable documentation to verify the income stated in the identification process.

## Source of Wealth and Funds and Supporting Documentation

To establish 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 is in line with customers original net worth.

Below is sample documentation to be requested in the SOW/SOF process. Note for each of the funding sources below, before the 'Additional evidence, if required' bullet point the mandatory documentation required for that particular funding source is shown.

Salary income:

- 3 month bank statement(s) showing receipt of salary (Documentation is to be 3 to 6 months old).

Company profits:

- Distribution of dividends certificate.

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).

Sale of property:

- Copy of contract of sale.

Sale of the company:

- A Letter detailing company sale signed by a licensed solicitor or regulated accountant on letter-headed paper.

Inheritance:

- Copy of the deceased's will.

Loan:

- Copy of the loan agreement.

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 sale if it exceeds 6 months).

Fixed deposit – Savings:

- Savings statement.

Funds generated from gambling/gaming winnings:

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

Pension:

- Bank statement showing the release of pension payment and indicating the name of the pension fund making said payment.

## Customers Failing to Provide Due Diligence Information

Where we are unable to apply Due Diligence 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. The decision to delay Due Diligence measures must never be unilaterally decided and a note should be left with the rationale of such action.

Customers shall be given a 30-day timeframe from the date of first correspondence to respond to due diligence information requests. The customer will be allowed to deposit and wager only. No withdrawals will be allowed. These 30 day time periods 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 blocked in its entirety, and the user 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.

In relation to EDD (SOF/W) information requests, 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. If the customer does not provide within 30 days the account will be blocked accordingly and SAR/STR will be considered to be escalated to the MLRO.

#### **Ongoing and Transaction 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.

After the Company enters into a business relationship with its players, all transactions undertaken throughout the course of the relationship are monitored on an ongoing basis. The Company monitors ongoing business relationships and assesses single 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 player, 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 behaviour 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:

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

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 and not any business within the Customer Acceptance Policy and

- 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 fulfil 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 manual 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 scrutinised to establish whether any suspicious activity or transactions are occurring.

A full review of the account will be conducted as stated both on the identification and verification information and the transactions. A note shall be left on the system detailing what has been checked and the result of the checks carried out. Accounts can have their risk ratings increased via override, such will indicate that the account is to be reviewed more frequently.

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 Money Laundering Reporting Officer (MLRO) for controlling and reporting obligations. In case of deviation or suspicious activities/transactions, the customer's risk profile is also updated.

#### **Periodic Ongoing Monitoring**

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

**Commented [14]:** Insert section on customer acceptance policy - what do you deem as acceptable or not?

**Commented [15]:** Determine also the threshold currently in place, limits and controls and also an oversight of the transaction monitoring currently in Place

- High Risk: 1 year
- Medium Risk: 2 years
- Low risk : 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.

#### **SOW/F Re-Verification**

Customers will have their SOW/F identification or verification refreshed in line with periodic ongoing monitoring time scales; however, note if an account review is conducted which would re-set the periodic ongoing monitoring review timer it shall not reset the SOW/F re-verification timer unless SOW/F is re-verified.

#### **Transaction Monitoring**

Transaction monitoring is to be carried out in real-time by an internally generated system. 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.

As can be seen from the above, 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 will monitor the list of prohibited countries against transactions to ensure that no payments are acceptable from such jurisdictions.

#### **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 CRA.

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 the Compliance Officer shall consult data, information and reports [e.g. customers from countries which inadequately apply Financial Action Task Force's (hereinafter "FATF"), country assessment reports] that are published in the following relevant international organisations in order to determine the jurisdictional risk posed by a customer:

- FATF - [www.fatf-gafi.org](http://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](http://www.coe.int/moneyval)

**Commented [16]:** Kindly attach the jurisdiction risk assessment you are referring to here as annex 1

**Commented [17]:** is a jurisdiction risk assessment established. kindly share as part of the policy and make reference

- The EU Common Foreign & Security Policy (CFSP) - [http://ec.europa.eu/external\\_relations/cfsp/sanctions/list/consolidated.htm](http://ec.europa.eu/external_relations/cfsp/sanctions/list/consolidated.htm)
- The UN Security Council Sanctions Committees - [www.un.org/sc/committees](http://www.un.org/sc/committees)
- The International Money Laundering Information Network (IMOLIN) - [https://www.imolin.org/imolin/amlid/index.jsp?lf\\_id=](https://www.imolin.org/imolin/amlid/index.jsp?lf_id=)
- The International Monetary Fund (IMF) – [www.imf.org](http://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.

## 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
- 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.

## Record Keeping

The Company shall retain the following documents and information in accordance with PMLFTR Art 13 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, information, and documentation, unless otherwise instructed by the FIU or any other relevant authority.

The information and documents may be requested to be kept for an additional five-year period or if it shall be considered necessary not to jeopardise 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 as follows. All documentation is kept in electronic form.

- Policies and documentation (kept electronically on the Company's drive):
  - 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;
  - All training delivered and attendees;
  - Employee screening records.
- Customer due diligence (securely kept electronically on the Company's Back Office system):

- A copy of all documentation received by the customer;
  - A copy of any correspondence received by the customer;
  - Information on the purpose, nature and expected activity;
  - All transactions (including deposits, withdrawals, game play, bonuses);
  - Any supporting evidence and records necessary to reconstruct all transactions carried out by the customer;
  - Customer Risk Assessments.
- Related to the MLRO (securely kept electronically by the MLRO on the Company's drive):
    - 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;
    - An authority has informed the Company that such documents or data need to be retained for a longer period of time
    - Copy of any agreements with any vendor or third-party provider.

## Internal Auditing

The Company has outsourced its internal audit function that is independent and responsible for reviewing the internal guidelines, controls and procedures for complying with its obligations under the AML/CFT Regulations. Even though such function is outsourced, ultimate responsibility lies with the Company. Such function reviews and regularly assesses whether the Company's:

- Organisation, control processes, IT systems, models and procedures, and guidelines are appropriate and effective;
- Activities are being conducted in line with the Company's internal controls and guidelines;
- Internal controls are appropriate and effective;
- Other control functions are reliable and assess the quality of the work done.

The independent internal 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.

## Employee Screening

The Company carries out employee screening, based on the carrying out of interviews and the collection of certificates, references, identification documents (passport/identity card), and police conducts. The Company ensures the suitability of the persons employed to carry out tasks relevant to the prevention of ML/FT through employee screening.

The analysis of the interview and the documents collected are used to decide on employment matters. The documentation obtained prior to the onboarding of the individuals is reviewed and maintained 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.

## Employees Training

A key element of our compliance programme is ensuring that all employees are trained as to their compliance responsibility and developments in the area. The Company ensures that all individuals employed with the Company receive relevant training and information in order to fulfil the Company's obligations under the AML/CFT legislation.

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. Failure to do so without good reason constitutes a significant breach of their employment contract and may result in termination of their employment.

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.

#### Periodicity

- On employee onboarding, within 3 months.
- Once a year for relevant persons including Senior Management and Board of Directors, or whenever there is new regulation or significant development, whichever comes first.

#### Training Records

The training is documented, electronically or in paper form. The Company conducts training either on a face-to-face basis or via electronic means, depending on the location of the participants.

### Policy Review

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.

**Commented [18]:** Add section on termination of business relationship

X 

David Jose Avila Sherwood  
Director and MLRO

01.01.2024

