United Republic of Tanzania
Ministry of Finance and Planning

AML/CFT COMPLIANCE GUIDE ON OBLIGATIONS OF DESIGNATED NON-FINANCIAL BUSINESSES AND PROFESSION(DNFBPs) JANUARY 2023

JANUARY 2023

AML/CFT COMPLIANCE GUIDE ON COMPLIANCE OBLIGATIONS DESINATED NON-FINANCIAL BUSINESSES AND PROFESSIONS (DNFBPs)

1.0 OVERVIEW

In 2022, The United Republic of Tanzania amended its anti-money laundering related legislation to incorporate Risk Based Approach to AML/CFT/CFP measures. The two legislations defined the term reporting person to include DNFBPs.

Both the AMLA and AMLPOCA empowers the FIU and regulators of specific sectors/industry, to issue guidelines with respect to AML/CFT/CFT measures. This Guide is so issued for the guidance of persons and entities operating as DNFBPs in United Republic of Tanzania and Zanzibar. The definitions of the "reporting person" in the AMLA and AMLPOCA equally apply mutatis in this Guide.

The United Republic of Tanzania National Risk Assessment (NRA) 2016 as Revised in 2022, identified the DNFBPs among the highest-risk channels used to launder the proceeds of crime. The NRA concluded that the transactions conducted by DNFBPs with financial institutions are associated with a certain level of risk that requires FIs to implement efficient risk management framework to minimize negative effects that transactions with DNFBPs may pose.

2.0 PURPOSE OF THE GUIDANCE

2.1 This Guidance is designed to provide DNFBPs with a clear and simplified overview of their AML/CFT obligations under the Anti-Money Laundering Act (Cap.423) and the Anti-Money Laundering and Proceeds of Crime Act, No: 10 of 2009 of Zanzibar including the requirement to report any transaction/activity suspected to be related with money laundering (ML) and terrorism financing (TF). This Guide reflects the provision of AML/CFT Laws and regulations made under those two laws. Moreover, since suspicious transaction reports (STRs)are a crucial preventive tool relied upon in the fight against money laundering and terrorism financing, the FIU, through this Guidance is committed to assisting DNFBPs to meet their obligations and ensure they file suspicious transaction reports of high quality.

2.2 The FIU's Compliance Department is responsible for the supervision of the compliance the AML/CFT requirements stipulated under the laws in URT and proposing administrative and financial sanctions/measures against violations of the provisions of the Laws or regulations and any relevant decisions or instructions.

3.0 TARGET AUDIENCE AND APPLICATION OF THE GUIDANCE

3.1 The Guide shall apply to all DNFBPs in the following categories:

(a) Operators of gaming activities – with respect to customers engaged in monetary transactions or activities related to gaming activities the applicable designated

threshold-

(b)

(i) a currency transaction involving Tanzanian Shillings or any foreign currency equivalent to ten thousand United States' Dollars or more in the course of a single transaction;

(ii) an Electronic Funds Transfer involving Tanzanian Shillings or any foreign currency equivalent to one thousand United States' Dollars or more in the course of a single transaction;

(c) Real estate agents – when they are involved in suspicious transactions for their client concerning the real estate business;

(d) Dealers in precious metals and dealers in precious stones – when they engage in any transaction or activity with a customer;

(e) Advocates, notaries, other independent legal professionals and accountants – when they prepare for or carry out financial transactions for or assist their client whose transaction is of suspicious in nature when:

(i) buying and selling of real estate;

(ii) managing of client money, securities or other assets;

(iii) management of bank, savings or securities accounts;

(iv) Organization of contributions for the creation, operation or management of companies;

(v) Creation, operation or management of legal persons or arrangements; and

(vi) Buying and selling of business entities.

(f) Trust and company service providers – when they prepare for or carry out transactions for a client when:

(i) acting as a formation agent of legal persons or legal arrangement;

(ii) acting as (or arranging for another person to act as) a director or secretary of a company, a partner of a partnership, or a similar position in relation to other legal persons;

(iii) providing a registered office, business address or accommodation, correspondence or administrative address for a company, a partnership or any other legal person or arrangement;
acting as (or arranging for another person to act as) a trustee of an express

trust or performing the equivalent function for another form of legal arrangement;

(g) acting as (or arranging for another person to act as) a nominee shareholder for another person

(h) Auctioneers, Motor Vehicle Dealers, Clearing and Forwarding Agencies - when they prepare for or carry out financial transactions for clients.

4.0 MONEY LAUNDERING AND TERRORISM FINANCING CRIMES

4.1 Section 12 of the Anti-Money Laundering Act (Cap. 423) in this guidelines referred to as AMLA and Section 7 of Anti-Money Laundering and Proceeds of Crime Act, 2009 [Act No:10 of Zanzibar] in this guidelines referred to as AMLPOCA stipulate that any person commits offence of money laundering if he -

(a) engages, directly or indirectly, in a transaction that involves property that is proceeds of a predicate offence while he knows or ought to know or ought to have known that the property is the proceeds of a predicate offence;

(b) converts, transfers, transports or transmits property while he knows or ought to know or ought to have known that such property is the proceeds of a predicate offence, for the purposes of concealing, disguising the illicit origin of the property or of assisting any person who is involved in the commission of such offence to evade the legal consequences of his actions;

(c) conceals, disguises or impedes the establishment of the true nature, source, location, disposition, movement or ownership of or rights with respect to property, while he knows or ought to know or ought to have known that such property is the proceeds of a predicate offence;

(d) acquires, possesses, uses or administers property, while he knows or ought to know or ought to have known at the time of receipt that such property is the proceeds of a predicate offence; or

(e) participates in, associates with, conspires to commit, attempts to commit, aids and abets or facilitates and counsels the commission of any of the acts described in paragraphs (a) to (d) of this section.

4.2 The Money Laundering crime is under both the AMLA and AMLPOCA an independent offence from the underlying predicate offence. When proving that funds are the proceeds of crime, it is not necessary that a person is convicted of a predicate offence. This means that the punishment of a person committing a predicate offence does not prevent their punishment for the money laundering crime.

4.3 The money laundering offence has the following general characteristics:

4.3.1 ML crime is an ancillary offence or a crime of consequence meaning that ML is committed following the commission of a principal/ predicate offence which generates proceeds that are placed in the financial system or is used for other economic or personal use;

4.3.2 ML offence is an independent crime from the predicate offence. The underlying predicate offence is also a criminal act and therefore it is not required that a person must be convicted of a predicate offence in order to be prosecuted for a money laundering crime;

4.3.3 The punishment for committing a predicate offence shall not prevent the punishment for the money laundering crime.

4.3.4 Any funds or proceeds may be laundered and consequently funds or assets (whether physical or non-physical, movable or immovable), including the revenue, income, or interest derived or obtained, directly or indirectly, from committing a predicate offence are related to money laundering crime.

4.3.5 The money laundering Offender may be:

(a) either the perpetrator of the predicate offence: in this case, he proceeds by his own desire or choice with concealing the true criminal source of funds; or

(b) any other person who assists (the perpetrator of the predicate offence) for the purpose of integrating the proceeds of crime into the formal economy.

4.4 Penalties/sanction for commission of ML are stipulated in section 13 of the AMLA and Section 8 and 9 of the AMLPOCA that any person who commits money laundering –

(a) if the person is an individual, shall be sentenced to a fine not exceeding five hundred million shillings and not less than one hundred million shillings or an amount equivalent to three times the market value of the property derived or proceeds obtained, whichever is greater or to a term of imprisonment not exceeding ten years and not less than five years; or

(b) if the person is a body corporate, shall be liable to a fine not exceeding one billion shillings and not less than five hundred million shillings or be ordered to pay the amount equivalent to three times the market value of the property derived of proceeds obtained, whichever amount is greater.

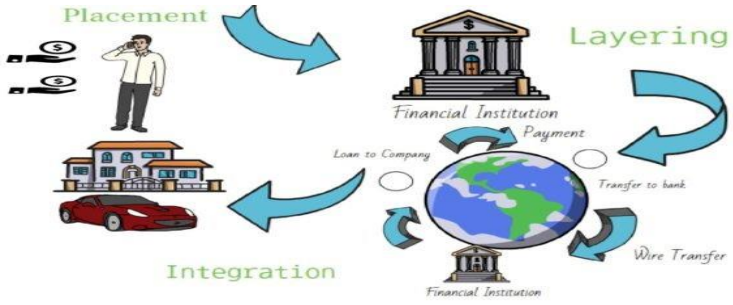
4.5 In addition to the penalties/sanction referred to in paragraph 4.4 above, the Financial Intelligence Unit or regulator of a particular DNFBPs may apply to the court for an order against a body corporate that has been convicted of an offence of money laundering-

(a) barring that body corporate from carrying on business directly or indirectly for a period not exceeding three years;

(b) placing that body corporate under supervision of the regulator; or

(c) permanently barring that body corporate from carrying on business directly or indirectly in respect of which an offence was committed.

4.6 Money laundering processes and stages are depicted in the diagram below:



4.7 Crimes such as drugs, arms trafficking, corruption and bribery can generate huge amounts of proceeds to perpetrators who seek to conceal or disguise their illicit sources through money laundering in order to benefit from such proceeds through the following money laundering stages as shown in the diagram in paragraph 4.6 above:

4.7.1 **Placement**: At this stage, the money launderer arranges the proceeds of the crime -

(a) by placing the proceeds in the financial system usually through a bank, or other financial institution-

(i) either by breaking up large amounts of cash into smaller amounts to avoid raising any suspicions and scrutiny, and then depositing such amounts into different accounts held by different persons at different times and different branches of the financial institution. This process is known as Smurfing; or

(ii) by converting banknotes with a low value to banknotes with higher value, or to foreign currencies, or financial instruments such as checks, payment orders, to facilitate their physical cross border transportation.

(b) A money launderer may place the proceeds of the crime by buying real estates and movable assets like gold, precious metals and precious stones directly and with large amounts, or by structuring the purchases to avoid raising any suspicions, in particular when the conducted financial transactions are not proportionate to the usual size or pattern of transactions of similar customers.

(c) Proceeds of crime may not always be in cash, they can include the income, interest, revenue or other product or security, whether or not it has been transferred in whole or in part into properties or investment proceeds.

4.7.2 **Layering:** After the placement of the proceeds of the crime, the money launderer disguises or conceals the illicit source by performing a series of complex operations and transfers that prevent the detection of the source of the proceeds, such as by carrying out services, concluding fictitious contracts and bills and establishing front/fictitious companies; or by selling or purchasing gold, precious metals and precious stones without a business purpose, which make traceability of the illicit source of funds very complicated.

4.7.3 **Integration:** at this stage, the money launderer injects the proceeds of the crime into legal economic activities to give them an apparently legitimate source. Following successful integration, funds can be easily demonstrated to the profits of a legitimate business, proceeds from the sale of legitimately acquired assets or properties, etc. Once integration has successfully taken place, it is very difficult and even impossible to identify funds as the proceeds of crime.

4.8 TERRORISM FINANCING

4.8.1 According to Section 13 of the Prevention of Terrorism Act (Cap. 19) of the Laws of Tanzania, financing of terrorism is a criminal offence. A person who finances terrorism or a person who willfully provides or collects, by any means, directly or indirectly, funds within or outside the United Republic with the intention that the funds may be used, or with the knowledge that they may be used, in order to carry out terrorist acts, commits an offence.

4.8.2 Section 14 of the Prevention of Terrorism prohibits collection of property or provision of property and services for commission of terrorism. According to Section 14, any person commits an offence if he directly or indirectly, collects property or provides, invites a person to provide, or makes available, property or financial or other related services-

(a) intending that they be used, in whole or in part, for the purpose of committing or facilitating the commission of a terrorist act, or for the purpose of benefiting any person who is committing or facilitating the commission of a terrorist act; or

(b) knowing that in whole or in part, they may be used by, or shall benefit, individual terrorist or a terrorist group.

4.8.3 Penalty/sanction for commission of Terrorism financing is imprisonment for a term of not less than twenty years but not more than twenty-five years.

4.8.4 In the offence of Terrorism financing, it is not necessary to prove that that the funds or other assets were actually used for financing terrorism. An attempt or link to a terrorist act is adequate to prove terrorism financing.

4.8.5 Terrorism financing offence extends to any funds, whether from a legitimate or illegitimate source, regardless of whether the funds were actually used to commit or attempt to commit a terrorist act, or are linked to a specific terrorist act and is deemed to have been committed, irrespective of whether the person charged with committing the offence is present in the same country or where the terrorist or terrorist organization is located or where the terrorist act was committed, or would be committed or in any other State**.**

4.8.6 Terrorism financing offence is considered a predicate offence for purposes of money laundering. As stated above, terrorism financing is to provide or collect funds, whether from a legal or illicit source, to be used for perpetrating a terrorist act(s) which is a predicate offence. The funds may be used by a terrorist (individual) or terrorist entity, even in the absence of any relation with a specific terrorist act(s).

4.8.7 Terrorism financing offence extends to any funds, that are assets or property of every kind, whether physical or non-physical, tangible or intangible or movable or immovable. It is important to be aware that "funds" does not just mean money. Providing anything of value to a terrorist or a terrorist group—or collecting it with the intention of providing it—is a terrorist financing crime. This can include providing food, housing, medical supplies, weapons, and computers—not just cash or electronic transfers**.**

4.8.8 Differences between ML and TF

MONEY LAUNDERING CRIME	TERRORISM FINANCING CRIME
The crime is independent of the predicate offence	The crime is a predicate offence to the money laundering crime
The crime is subsequent to the predicate offence	The crime is often prior to the terrorism crime
The laundered money is the proceeds of the predicate offence	Funds used in terrorism financing can be licit or legal (example in fundraising, etc.) or illicit (proceeds of drugs trafficking, etc.)

5.0 AML/CFT COMPLIANCE REQUIREMENTS FOR DNFBPs

5.1 Applying the Risk-Based Approach:

Risk-Based Approach constitutes a series of measures and procedures that aims at identifying, assessing, understanding and mitigating Money Laundering, Terrorism Financing risks and Proliferation financing in order to allocate sufficient resources to focus on prioritized areas such as on high-risk activities, customers or transactions, to achieve effectiveness.

Risks can be low, Medium or high as shown in the diagram below:

5.2 How should DNFBPs assess their ML/TF risks?

To comply with the AML/CFT requirements, DNFBPs are required to-

5.2.1 Conduct an Institutional risk assessment for the business.

The goal of the risk assessment is to identify, assess and understand the money laundering and terrorism financing risks. The risk assessment should be appropriate to the size and nature of the business. Larger businesses will need a more in-depth and comprehensive risk assessment.

5.2.2 In conducting an institutional Risk Assessment, DNFBPs are required to consider the following:

(a) Size of the business:
The important thing to consider is whether the business is a single person, or whether it is a single store or multiple stores in different countries, with a large staff. A larger business may have a higher risk because it is more difficult to track customer activity and to get to know your customers.

(b) Nature of the business:
Certain parts of the business have higher risks than others. Sale of motor vehicles, sale of land or houses, placing huge amount of funds at the lawyer or dealing with occasional business transactions are considered of highest risk because these ways are most attractive to criminals or illicit actors. In contrast, dealing with other reporting persons or well-established customers, is considered to be lower risk because the transactions are more unpredictable and because they are already under obligation to apply preventive measures.

(c) Risks identified in the National Risk Assessment (NRA):
The NRA discusses the primary proceeds-generating crimes as well as ways in which criminals launder the proceeds of those crimes or terrorist financiers may seek to move funds. Motor vehicle dealers, Dealers in precious metals and precious stones, Lawyers, auctioneers and real estate agents must be aware of the findings of the NRA and consider whether any of these apply to their business, including their customer base.

(d) Risk factors associated with the customer base:

The risk of the customer base may be high if many of a business customers or suppliers are high-ranking officials or one of their family members and close associates (known as politically exposed persons) or reside in high-risk jurisdictions or was not subject to the identity verification process (i.e. non-face to face transactions). Customers or suppliers may also be of higher risk are customers that are legal persons (are in the form of companies) or legal arrangements (such as trusts) whose structures or nature makes it difficult to identify the beneficial owners. In addition, a customer attempting to obscure understanding of his business or transactions through shell or front companies, or companies with a complex ownership structure or companies managed over different countries without any apparent economic reason, or a customer who is a legal person and operates a considerable part of his business in, or have branches in, countries that pose high-risk are also things to look at when conducting institutional risk assessment. In assessing customer risk, DNFBPs must consider not just their direct customers, but the people who own and control their legal person customers, known as "beneficial owners".

(e) Risk factor Associated with a business of DNFBP:

When conducting Risk Assessment, a DNFBP should also consider how well they know their business. A business that serves a small group of customers who have been using the same DNFBP for many years may have lower risk than a business that has a large and constantly changing customer base, because in the first case it is easier to know your customers' backgrounds, their businesses, and what they do with your service. However, the fact that the DNFBP knows a customer for years doesn't mean the customer is automatically low risk. A thorough assessment should be carried out by the dealer to satisfy himself of the risk posed by each customer/business the conduct.

(f) Risk factors associated with jurisdictions and geographical areas:

A business of a DNFBP may be of higher risk factors if it frequently conducts transactions associated with jurisdictions identified by credible and reliable source documents (such as by FIU, or in Financial Action Task Force (FATF) statements), as having ineffective AML/CFT regimes or high level of corruption and other criminal activities. An association with jurisdiction could mean that the business sources has affiliation, connection or relationship with that jurisdiction or works with intermediaries or customers who are based in that jurisdiction, or has business dealings there. On the other hand, the risks may be lower if the transaction is related to jurisdictions which have effective AML/CFT regime or identified by credible and reliable sources as jurisdictions with low propensity or tendency for corruption and other criminal activities or identified by reputable bodies and organizations in the mutual evaluation process.

(g) Risk factors associated with products, services, transactions and professional practices:

Certain products and services are considered to be higher risk for ML/TF because they make it easier for criminal to abuse your business. The physical characteristics of the product offered are also a factor to consider. Products that are easily portable and which are unlikely to draw the attention of law enforcement are at greater risk of being used in cross border money laundering or terrorist financing. For example, business conducted over the internet or any other arrangement in which a DNFBP never comes to face to face with the customer are considered to have high risks; products or services that favour anonymity or that are provided with conditions on no questions asked; cash transactions and transactions which involve new or developing technologies, such as accepting virtual assets (cryptocurrencies, such as Bitcoin) are all of high risks to DNFBPs.

(h) Updating the risk assessment regularly.

DNFBPs must update their risk assessment before beginning to offer new products or services or using new delivery channels or new technologies.

5.3 What is the Methodology to be adopted by DNFBPs to identify, assess, understand, address and mitigate their ML/TF risks?

5.3.1 DNFBPs must rely on an appropriate methodology to enable identification, assessment and understanding of the risks. The methodologies are many but what is required by the law is that the methodology used should also assist in addressing the risks faced. On line or self-designed methodologies may be used for this purpose so long as they are based on the following steps:

(a) **Step 1:** Provide insights about your business by providing specific information about your business and operations such as the number of employees, jurisdictions where you operate, type of customers and how you onboard customers and specifics about the products/service you offer to customers. The DNFBP is therefore required to identify certain risk categories, i.e., customers, countries or geographical locations, products, services, transactions and delivery channels. Depending on the specificity of operations of a particular DNFBP, other categories may be required to identify all segments in which money laundering or terrorist financing may emerge. The significance of different risk categories may vary from DNFBP to another. One DNFBP may decide that some risk categories are more important to it than others. DNFBPs should find out which ML/TF risks they are, or would be, exposed to as a result of entering into a business relationship or carrying out an occasional transaction. In identifying ML/TF risks associated with a business relationship or occasional transaction, it is important to consider relevant risk factors including who the customer is, the countries or geographical areas they operate in, the particular products, services and transactions the customer

requires and the channels the firm uses to deliver products, services, and transactions. Where possible, information about ML/TF risk factors should come from multiple sources, whether these are accessed individually or through commercially available tools or databases that pool information from several sources. DNFBPs should determine the type and numbers of sources on a risk-sensitive basis.

(b) **Step 2:** Schedule an interview with a Compliance Officer to go through your answers and iron out anything that might have been unclear in Step 1.

(c) **Step 3**: DNFBPs should identify the likelihood that the types or categories of risk will likely materialize. For example, with respect to customers, they may misuse the DNFBP for money laundering and terrorism financing purposes. This likelihood is for instance high if it can occur several times in a year, medium if it can occur once in a year and low if it is unlikely, but not impossible.

5.3.2 Use the answers you provided in Step 1 to map them to different risk factors and assess the likelihood of some of these risk factors happening and Likelihood of a risk factor happening may be based on the following five staged categories:

Probability of occurrence	Likelihood	Description
91-100%	Almost certainly	Occurs often during the provision of the service. Continuously experienced.
61-90%	Likely	Occurs several times during the provision of the service. Occurs frequently.
41-60%	Possible	Occurs sometime during the provision of the service. Occurs sporadically, or about half of the time.
11-40%	Unlikely	Possible to occur during the provision of the service. Remote chance of occurrence and expected to occur sometime during the provision of the service.
0-10%	Rare	Can assume will not occur during the provision of the service. Possible, but improbable. Occurs only very rarely.

(a) **The DNFBPs should also assess the impact**.

In assessing the impact, the DNFBP can for instance look at the financial damage from the crime itself or from regulatory sanctions or reputational damages to the business. These impacts can vary from minor if there are only short term or low-cost consequences to (very) major when there are high cost and long-term consequences that affect the proper functioning of the DNFBP.

The impact/severity of each risk factor happening may be expressed as follows:

Impact	ML/TF Impact	Reputation	Non-compliance
Negligible	The service cannot be used in facilitating any illegal or criminal activities.	Non-headline exposure, not at fault, no impact.	Innocent procedural breach, evidence of good faith, little impact.
Minor	The service can be used directly or indirectly to fund or support criminal activities with minor impact.	Non-headline exposure, clear fault - settled quickly.	Breach, objection/complaint lodged, minor harm with investigation.

Moderate	The service can be used directly or indirectly to fund or support criminal activities with moderate impact such as: • minor cyber-crime and scams; • small scale business fraud and tax evasion; • small scale local and street crime.	Repeated non-headline exposure, slow resolution. Results with regulatory enquiry/briefing.	Negligent breach, lack of good faith evident, performance review initiated.
Significant	The service can be used directly or indirectly to fund or support criminal activities with a significant impact such as: • serious financial crime; • organised maritime piracy; • organised environmental crime; • corruption; • extorsion; • major cyber-crime.	Headline profile, repeated exposure, at fault or unresolved complexities. Results with the involvement of the regulator.	Deliberate breach or major negligence, formal investigation, disciplinary action. Results with regulatory involvement.
Severe	The service can be used directly or indirectly to fund an illicit activity that may result in loss of lives or have a severe impact on human well-being such as: • terrorist attacks; • human trafficking; • drug trafficking.	Maximum high-level headline exposure, regulatory censure, loss of credibility.	Serious wilful breach, criminal negligence or act. Results with prosecution, dismissal and regulatory censure.

(b) **Step 4:** Having insight into the Inherent Risk of your business, you can now list down all the risk you have identified and make an assessment on likelihood of its occurrence against the impact or consequences. The inherent Risk as a function of likelihood and impact may result in any of the following rating for each risk you have identified:

Likelihood	Risk Score				
Almost certainly	Medium	Med High	Med High	High	High
Likely	Low Med	Medium	Med High	Med High	High
Possible	Low Med	Low Med	Medium	Med High	Med High
Unlikely	Low	Low Med	Low Med	Medium	Med High
Rare	Low	Low	Low Med	Low Med	Medium
Impact	Negligible	Minor	Moderate	Significant	Severe

This step can result to the following report:

Type of customer	Likelihood	Impact	Risk analysis
Domestic retail customer	Medium	Moderate	Medium
Individuals	High	Major	High
Small business	Medium	Moderate	Medium
Foreign companies	High	Moderate	Medium
PEP	High	High	High
Occasional customer	High	High	Medium High

The above risk analysis is a general one for types or categories of customers. It is important to carry out this assessment for all other categories in the AML/CFT/CPF Assessment on the products/service, channels of distribution and geographical areas.

(c) **Step 5**: Based on your understanding and knowledge obtained from steps 4 above, suggest mitigation measures that are appropriate to the risks you are facing.

(d) **Step 6**: Calculate your Residual Risk, by taking the inherent risk identified in Step 4 for each risk against the Control Effectiveness, i.e. the level to what the proposed or implemented measures reduce the risk of your business being abused for ML/TF. Note that you will reassess the level of effectiveness over time as you collect more empirical data. If the Residual Risk does not fit your risk appetite, you should repeat Step 5 until the Residual Risk is down to a level that is acceptable for you.

Residual Risk as a function of the Inherent Risk and the Control effectiveness may result into the following ratings:

Control Effectiveness	Residual Risk				
Weak	Low	Low Med	Medium	Med High	High
Adequate	Low	Low	Low Med	Medium	Med High
Strong	Low	Low	Low	Low Med	Medium
Inherent Risk	Low	Low Med	Medium	Med High	High

5.4 What should DNFBPs do with the results of their ML/TF risk assessments?

DNFBPs should:

5.4.1 Document their ML/TF risk assessments and any basic information to be able to demonstrate their basis.

5.4.2 Document the basis and sources they used to identify, assess and understand their ML/TF risks taking into consideration the National Risk Assessment and any other relevant source to identify such risks.

5.4.3 Monitor the implementation of the Risk Assessment's findings and update the risk assessment on ongoing basis.

5.4.4 Provide relevant periodic reports to the Regulator and FIU within the set timeframe and upon their request.

6.0 AML/CFT Programme

Every DNFBP should:

6.1 Develop an AML/CFT programme that contains internal policies, procedures and controls that are commensurate with the risks identified, taking into consideration the size, complexity and nature of the business. The sample of interna Policies and procedures is as set out in **Annex A.**

6.2 Implement the programme effectively to manage and mitigate the risks taking into consideration the nature and size of their businesses.

6.3 Review, update and enhance the programme, when necessary.

6.4 Apply the programme to branches and majority-owned associates, whether inside or outside the United Republic.

6.5 Provide a copy of the AML/CFT programme and the annual report of the Compliance Officer once a year to FIU and regulator (if any) and any other supporting documents that may be requested for this purpose.

6.6 What should the AML/CFT Programme include?

6.6.1 Appropriate compliance management arrangements including the appointment of a compliance officer and his Deputy at the management level.

(a) The appointed Compliance Officer responsible for overseeing and managing the compliance with the AML/CFT requirements stipulated in the AML/CFT Laws and the Regulations.

(b) The Compliance Officer is required to prepare and submit Suspicious Transaction Reports (STRs) to the FIU.

(c) The Compliance Officer is responsible for effective implementation of the AML/CFT Programme (including ensuring that appropriate policies, procedures, systems and controls are established and developed on a regular basis, risk assessments are conducted, reviews and testing are conducted to ensure the effectiveness of the programme).

(d) The Compliance Officer acts as a focal point for communication between the DNFBP, the AML/CFT Section and other competent authorities in AML/CFT related matters.

(e) Where a DNFBP conducts his activity as a commercial company, he should appoint one of the employees to act as a Compliance Officer to manage compliance with the AML/CFT requirements, particularly to prepare and file STRs with the FIU.

(f) Where a DNFBP conducts his activity as an individual business activity, he should personally undertake the senior management and the compliance officer responsibilities or may appoint one of his employees as a compliance officer.

6.6.2 Adequate screening procedures to ensure high standards when appointing employees:

(a) DNFBPs should develop adequate screening procedures to ensure high standards and integrity of their employees and officers;

(b) Enhanced screening procedures must be adopted for higher impact individuals, such as employees engaging in a direct activity with the customer or employees conducting and overseeing the financial transactions.

(c) The screening procedures should include screening of employees before appointment or employment and must, as a minimum require –

(i) obtaining and confirming references about the candidate and confirming the candidate's employment background and qualifications;

(ii) seeking and verifying information or details about any criminal convictions or regulatory actions against the candidate.

6.6.3 Ongoing training programme for employees:

(a) Dealers in Precious Metals or Precious Stones must develop and design an appropriate ongoing training programme for their officers and employees to maintain their knowledge of international and domestic AML/CFT legal frameworks; and

(b) ensure that the training programmes are up-to-date with internal policies, regulations, procedures and controls adopted to manage and mitigate ML/TF risks.

(c) Training must assist employees to keep abreast of any ML/TF patterns or trends; must ensure they are trained to make the related STRs, and must inform appropriate employees of the importance of conducting CDD measures and ongoing monitoring.

(d) Training should be tailored to the employee's role in the organization; for instance, employees on the sales unit or at front desk may need to receive somewhat different training than those in the back office.

(e) The training programme must be documented and updated on a regular basis.

6.6.4 Independent audit and review function to test Compliance with the AML/CFT systems:

(a) The testing must include in particular the AML/CFT programme, the screening procedures for employees, record making and record keeping, in addition to the ongoing monitoring in relation to customers; aiming at identifying gaps, deficiencies and shortcomings for future remedial actions.

(b) The testing must be conducted at least once every two (2) years by an independent internal or external auditor.

(c) A record of the testing results must be made and kept and a copy of this record must be provided to FIU and he regulator every two (2) years.

7.0 Customer Due Diligence (CDD)

7.1 Customer Due Diligence is a series of measures taken to ensure that DNFBPs know and fully understand their customers. It includes the following:

(a) identifying and verifying the customer's identity using reliable, independent source documents, data or information;

(b) determining whether the customer is acting on behalf of another person, and verifying if the latter is authorized to do so, including identifying and verifying his identity;

(c) understanding the pattern and nature of the customer's business activity, the purpose and intended nature of the business relationship; and

(d) establishing the legal status of the customer, whether he is a natural person or legal person or legal arrangement.

7.2 When is Customer Due Diligence required?

7.2.1 DNFBPs should conduct CDD when-

(a) establishing business relationships involving the use of cash whether as a one-off transaction or in several operations that appear to be linked.

(b) there is a suspicion of money laundering or terrorism financing irrespective of the amount of the operation or where there is doubts about the veracity and adequacy of previously obtained customer identification data;

(c) before establishing a business relationship with the customer or conducting a one-off transaction. However, CDD measures may be completed at a later stage during the business relationship in the cases specified by the law, provided that-

(i) the customer's identity is verified, as soon as practicable. This is necessary in order not to interrupt the normal conduct of business.

(ii) there is little risk of money laundering or terrorism financing and any risks are effectively managed;

(iii) and in cases of imposing restrictions with regard to the number, types and amount of transactions that may be conducted, provided that CDD is completed as soon as practicable, after contact is first established with the customer;

(iv) if the DNFBP conduct CDD measures after the establishment of the business relationship, he must document each instance and be prepared to demonstrate to the FIU or the regulator that delayed CDD was appropriate and justified in that context.

7.3 The CDD measures to be conducted by DNFBP

7.3.1 DNFBP are prohibited from keeping anonymous customer profiles or accounts in obviously fictitious names.

7.3.2 DNFBP are required to undertake CDD measures, to identify and verify the customer's identity, legal status, activities, the purpose and nature of the business relationship and the beneficial owner/s of the customer.

7.3.3 Measures referred to in paragraph 7.3.2, particularly include the following:

(a) Identify and verify the identity of customers using reliable, independent source documents, data or information.

(b) Identify the person who is acting on behalf of the customer and verify that any person purporting to act on behalf of the customer is so authorized in conformity with the relevant rules and laws.

(c) Identify the customer's beneficial owner(s) at the 20% threshold and take reasonable measures to verify the identity of the beneficial owner using reliable independent source documents, information or data, such that the DPMS are satisfied that they know who the beneficial owner is;

(d) Obtaining information on and understand the intended purpose and nature of the business relationship or transaction;

(e) Identify the nature of the customer's business; and for customers who are not individuals (such as companies), understand their ownership and control structure and verify the identity of the beneficial owner.

7.3.4 Obtaining and verifying additional information based on the risk factors associated with the customer or with the customer's businesses and transactions.

7.3.5 Review and update the records of the customer on a regular basis, to ensure that documents, data and information collected using CDD are kept up-to-date and relevant, particularly for high-risk categories of customers.

7.3.6 Scrutinize transactions conducted throughout the course of the business relationship on a regular basis, to ensure that the transactions are consistent with the DNFBP's knowledge of the customers, their business and risk profile, including where necessary, the source of their wealth and funds.

7.3.7 DNFBPs shall ensure the veracity and adequacy of previously obtained data as stated above, using reliable, independent source documents, data and information**.**

7.3.8 DNFBPs should identify and verify the identity of the customer using reliable, independent source documents, data or information, and shall at least obtain the following information:

(a) For customers that are natural persons:

(i) name of the person as registered in the official documents (full identity and photograph), residence address or domestic address, date and place of birth, and nationality. For example: name, date of birth, and nationality of the customer by verifying a valid passport or identification card with a clear photograph.

(ii) the customer's place of residence can be verified based on a leasing contract, utility bill or a letter by the employer.

(b) For customers that are legal persons or legal arrangements:
(i) name, legal form and proof of existence of the person;

(ii) the mandates, declarations, resolutions and other sources of power that regulate and bind the legal person as well as the names of the relevant persons holding a senior management position in the legal person or arrangement;

(iii) the address of the registered office and, if different, its principal place of business.

(c) For customers that are legal persons or legal arrangements, the dealer in precious metal or precious stones shall understand the customer's ownership and control structure and shall verify the identity of the beneficial owners.

7.4 Reliance on third parties to conduct CDD

7.4.1 DNFBP may rely on third parties such as financial institutions and other DNFBPs to conduct CDD measures to identify the customer, the beneficial owner and understand the nature of the business.

7.4.2 A DNFBP remains with the ultimate responsibility for the proper conduct of CDD measures.

7.4.3 When relying on third-party to perform the CDD measures the DNFBPs shall-
(a) immediately obtain from the third-party necessary information in relation to the CDD measures and identification of the Customer;

(b) ensure that the third party will provide without delay and upon request a copy of every document relating to the customer and other documents in relation to such measures that DNFBP would need if it were conducting CDD itself for the customer;

(c) verify that the third party is regulated and supervised and complies with the CDD measures requirements and maintains the records in conformity with the money laundering laws and regulations;

(d) DNFBP must have regard to any relevant findings published by international and regional organizations and foreign jurisdictions, as

well as available information on the level of risks related to ML and TF in jurisdictions where the third party operates or is located, before deciding to rely on said third party;

(e) ensure that it has received from the third party all information about the customer obtained from the CDD conducted by the third-party introducer for the customer that it would need if it had conducted the CDD itself.

7.5 What should DNFBPs do when they cannot complete CDD because the client refuses to provide the information or when they discover that the customers' data are fictitious or incomplete?

7.5.1 DNFBP should-

(a) not establish or continue the business relationship with the customer, or carry out the transaction for the customer;

(b) strongly consider filing an STR with the FIU in relation to the customer, especially if the customer refuses to provide information, backs out of the process halfway through, or provides fictitious information;

(c) be aware that providing false beneficial ownership information or concealing the interest of a Politically exposed Persons (PEP) in a transaction is a crime under the law;

7.6 What should DNFBP do when they suspect that the transactions are associated with money laundering or terrorism financing?

7.6.1 In cases where a DNFBP form a suspicion when establishing a business relationship with the customer, or in the course of such business relationship, or when carrying out occasional transactions, that those transactions are related to money laundering and terrorism financing, they should-

(a) Identify and verify the identity of the customer and the beneficial owner, even if the customer is an existing customer or an occasional customer and regardless of any exemptions or thresholds;

(b) If the DNFBP reasonably fears that asking too many questions will warn the customer of the DNFBP suspicions, the DNFBP can skip CDD but must immediately make an urgent report to the FIU.

(c) File an STR with the FIU.

8.0 Enhanced Customer Due Diligence (EDD)

8.1 When is Enhanced CDD required?

8.1.1 DNFBPs should apply Enhanced CDD-

(a) for business relationships and transactions with customers from countries identified by FIU as high-risk countries or countries subject to a FATF enhanced due diligence requirement whose information is available in FATF website;

(b) when ML/TF risks are high, especially in the following cases:

(i) complex, unusual large transactions or unusual patterns of transactions that have no apparent or visible economic or lawful purpose;

(ii) non-face-to-face purchase and sale transactions, direct or indirect, or transactions concluded using electronic means and instruments, as well as to other risks emerging from products and transactions that might favour anonymity and concealment of the source or identity;

(iii) purchase and sale transactions or transactions involving the power of attorney through non-resident customers**;**

(iv) for other cases that are identified by FIU as high ML/TF risks for DNFBPs.

8.2 Enhanced CDD to be conducted by DNFBP

8.2.1 The goal of Enhanced CDD is to learn more about the customer or transaction in order to minimize the chance that the customer or transaction is involved in ML/TF.

8.2.2 Enhanced CDD should be tailored to fit the risk of the specific customer or transaction.

8.2.3 DNFBP should generally carry out the following enhanced measures, but may add others as appropriate:

(a) increase the frequency and intensity of the business relationship monitoring;

(b) obtain additional information about the customer including profession, volume of assets and information available through public databases and open sources;

(c) update on an ongoing basis the identification data of the customer and the beneficial owner, by undertaken reviews of existing records particularly for high-risk categories of customers;

(d) obtain additional information on the purpose and intended nature of the business relationship;

(e) obtain additional information on the customer's source of wealth and funds;

(f) obtain information on the purpose of the intended transactions or the conducted transactions;

(g) obtain senior management approval before establishing or continuing a business relationship;

(h) take enhanced measures to monitor the business relationship by furthering the intensity and degree of supervision, and identifying patterns of transactions that require additional scrutiny and review;

(i) make the first payment through an account in the customer's name in a bank that is subject to similar CDD measures

8.3 Simplified Customer Due Diligence: When can DNFBP conduct simplified CDD?

8.3.1 DNFBP may conduct simplified CDD when all the following conditions are met:

(a) if the risk factors of the customer or transaction identified in the National Risk Assessment are low;

(b) if the risk factors of the customer or transaction identified in the self- institutional assessment are low;

(c) there is no suspicion of ML/TF; and

(d) there are no higher-risk factors, such as a link to a higher-risk jurisdiction, present.

8.3.2 What are the simplified CDD measures that DNFBP can conduct?

Simplified CDD consist of taking one or all of the following actions:

(a) verifying the identity of the customer and beneficial owner after the establishment of the business relationship;

(b) reducing the frequency of the customer's identification updates;

(c) reducing the intensity of ongoing monitoring and scrutiny of transactions based on a reasonable threshold;

(d) limiting the collection of information, or the conduct of specific measures, to determine the purpose and intended nature of the business relationship and inferring instead the purpose and nature from the type of transactions carried out or from the business relationship established.

8.3.3 In any case where a DNFBP carries out simplified CDD, he must document the risk assessment and be prepared to demonstrate when required by FIU or regulator, that the risk was appropriate and justified in this context.

9.0 Beneficial Ownership: Who is the Beneficial Owner?

9.1 The Beneficial Owner(s) are:

(a) the natural person who ultimately owns or controls a customer, through ownership interest or voting rights;

(b) the natural person on whose behalf a transaction is being conducted, whether by proxy, trusteeship or mandate or by any other form of representation;

(c) any natural person who holds ultimate effective control over a legal person or arrangement, including any natural person exercising ultimate effective control by any means.

9.2 What are the DNFBP s' obligations in relation to the Beneficial Owner?

9.2.1 The DNFBPs should identify and take appropriate and reasonable measures to verify the identity of the beneficial owner before establishing business relationships with the customer, using reliable, independent source documents, data or information until they are satisfied that they know who the beneficial owner is.

9.2.2 Where the customer is a legal person or legal arrangement, DNFBPs should understand the customer's ownership and control structure and verify the identity of the beneficial owner in conformity with the criteria referred to below.

9.2.3 **How to identify the Beneficial Owner?** DNFBP must identify the beneficial owner as follows:

(a) identifying the Beneficial Owner of legal persons:

(i) Identify the natural person(s) who ultimately has an effective controlling interest of at least 20% of a legal person or voting rights;

(ii) if no individual can be identified as the beneficial owner of the legal person, or there is a doubt that a natural person who ultimately owns effective control is the beneficial owner or if no natural person exerts control through ownership interests, DNFBPs must identify the natural person (s) exercising de facto or legal control in the legal person and arrangement through any means, whether directly or indirectly, over the executives, the general assembly, or the operations of the legal person, or any other control instruments;

(iii) in case no natural person is identified under paragraphs (i)and (ii) above, DNFBPs should identify and verify the identity of the relevant natural person holding a senior managing position in the legal person (e.g. the legal representative of the commercial company).

(b) Identifying the Beneficial Owner of legal arrangements:

(i) if the customer is a trust:

(aa) identifying the settlor, the trustee and the protector (if any) and the beneficiaries or class of beneficiaries, and any other natural person exercising, directly or indirectly, ultimate effective control over the trust;

(bb) for other types of legal arrangements; identify the natural person in equivalent or similar positions;

(cc) take the necessary procedures to determine whether a customer is acting as a trustee of a trust, or holds an equivalent or similar position in other types of legal arrangements.

9.2.4 Identifying Beneficial Owners when your customer is an individual, conducting CDD on that individual should give you the information you need to understand the customer and the purpose of his business with you.

9.2.4 Where your customer is a company, conducting CDD on the company alone is not enough to prevent financial crime. You need to understand the people who ultimately control the company and benefit from its actions.

Illicit actors commonly attempt to hide their identities by conducting business through companies they control.

9.2.5 The individuals who ultimately own and control a company are known as its "beneficial owners."

9.2.6 Under the Law, you are required to identify and conduct CDD on every beneficial owner who owns at least 20% of the company you're dealing with, or controls at least 20% of the voting rights. If no one meets that description, then you're required to identify and conduct CDD on every individual who controls the company in other ways. If you still can't identify anyone who meets that description, you're required to identify and conduct CDD on the company's senior managing official.

10.0 Politically Exposed Persons (PEPs)

10.1 PEPs are considered as a high-risk category of customers in relation to Money Laundering (ML) due to their influence and prominent functions entrusted to them. It is recognized that PEPs are in positions that they can abuse or misuse for their personal gain; or that the position they hold in society, allow them to misuse or misappropriate public funds.

10.2 PEPs often rely on their family members or close associates to conceal funds accruing from the misuse of their public functions. Therefore, in the United Republic of Tanzania you are required to treat the family members and close associates of PEPs as if they themselves were PEPs.

10.3 Who are the PEPs?

10.3.1 PEPs are individuals who have been entrusted with prominent public functions by the Government of United Republic or Revolutionary government of Zanzibar or by a foreign State, such as Heads of State or of government, senior politicians, senior government, judicial or military officials, senior executives of state owned companies, members of Parliaments, and important political party officials, and members of senior management, i.e. directors, deputy directors and members of the board or equivalent functions in international organizations.

10.3.2 Family members of a Politically Exposed Person shall include any natural person having blood relations or who by marriage up to the second degree including Father/ Mother, Husband/Wife, Father-in-Law/ Mother-in Law, Son/Daughter, Stepson/Stepdaughter, Grandfather/Grandmother, Brother/Sister, Brother-in Law/ Sister –in- Law, Grandson/Granddaughter.

10.3.3 Close associates of a Politically Exposed Person include any natural person who is a partner in a legal person or legal arrangement, or a beneficial owner of a legal person or arrangement owned or effectively controlled by a politically exposed person, or any person on associated with the politically exposed person through a close business or social relationship.

10.4 What are the measures that DNFBPs must adopt when the customer or the customer's beneficial owner is a PEP or a PEP's family member or a close associate?

10.4.1 DNFBP are required to put in place appropriate risk management systems to determine whether a customer or a customer's beneficial owner is a PEP, a family member or a close associate of a PEP.

10.4.2 The risk management system must include, in particular, seeking relevant information from customers, reference to publicly available information and having access to databases within the limits provided by the applicable legislations. In this case, DNFBP must adopt further CDD measures, as follows: ·

(a) obtain Senior Management approval before establishing a business relationship with a PEP, their family members, or close associates, or continuing a business relationship for existing customers who are PEPs, their family members, or close associates;

(b) take reasonable measures to establish the source of wealth and funds of customers and beneficial owners of customers identified as PEPs, their family members or close associates;

(c) conduct enhanced ongoing monitoring on business relationships with PEPs, their family members, and close associates, in addition to ongoing monitoring of transactions conducted within the business relationship while ensuring its consistency with customer's activity pattern and the risks it represents.

11.0 Record Keeping

11.1 What records should DNFBPs keep?

11.1.1 DNFBP should keep:

(a) records, documents and data on all domestic and international transactions and operations;

(b) records, documents and data obtained or collected while performing CDD;
(c) account files, business correspondence, and results of any analysis undertaken;
(d) all relevant information that enables tracing all financial transactions, when performing cash transactions or attempted transactions by the customer, and all related reports.

11.2 How long should the records be kept?

11.2.1 Pursuant to the requirements of the law, DNFBPs are required to keep and maintain all records, documents and data for all domestic and international transactions and operations, for a minimum of ten (10) years-

(a) from the date of concluding the transaction, occasional transaction or operation; or
(b) following the termination of the business relationship.

11.2.2 DNFBPs must retain records beyond the end of the ten-year period –

(a) if they have filed with the FIU a suspicious transaction report relating to the applicant for business or customer;
(b) if they know that the applicant for business or customer is under investigation by law enforcement or judicial authorities for issues related to money laundering or terrorism financing;

11.3 To whom should DNFBPs make records available?

11.3.1 DNFBPs should ensure that all CDD records, data and documents on transactions and operations are available without delay to the competent authorities upon request.

11.3.2 DNFBPs should also establish proper systems to ensure prompt response to the requests of the competent authorities.

11.4 What is the purpose of keeping records?

11.4.1 The records provide proof of compliance with AML/CFT requirements.

11.4.2 The records allow authorities to reconstruct individual transactions so as to provide, if necessary, evidence for the prosecution of criminal activity.

11.4.3 The records allow the DNFBPs to respond to requests by FIU, supervisory authorities, competent authorities, law enforcement authorities or judicial authorities.

12.0 Reporting Suspicious Transactions

12.1 DNFBPs must report promptly to FIU any suspicious financial transaction or activity or any attempt to perform such transactions or activity, regardless of the

amount of the transaction, when they suspect or have reasonable ground to suspect that the transactions are linked to or include funds that are proceeds of a predicate offence or are linked to terrorism financing.

12.2 DNFBPs should comply with the reporting obligations, when they suspect or have reasonable grounds to suspect that the transactions are linked to or involve proceeds of a predicate offence, or relating to terrorism financing, irrespective of the following:

(a) the amount of the transaction;

(b) no transaction has been conducted;

(c) the nature of the predicate offence;

(d) any attempt of money laundering or terrorism financing has failed.

12.3 The reporting obligation does not require DNFBPs to provide accurate evidence or supporting information in relation to the committed predicate offence or the need to provide the accurate legal description thereof. "Reasonable grounds to suspect" is determined by what is reasonable in the DNFBP circumstances, including normal business practices and systems within the industry.

12.4 A list of indicators of suspicious transactions regarding are set out in **Annex B** attached hereto. The said list of indicators is not conclusive. DNFBPs can identify suspicious transactions/activity involving high-risk individuals, legal entities, and transactions based on other criteria or known indicators of money laundering, terrorist financing, or a predicate offence.

12.5 What Kind of Transactions Must DNFBPs Report?

12.5.1 DNFBPs are required to file STRs if they believe that there may be a link to money laundering or terrorist financing.

12.6 How to Identify a Suspicious Transaction?

12.6.1 Transactions, whether completed or attempted, may give rise to reasonable grounds to suspect that they are related to money laundering or terrorist financing regardless of the sum of money involved.

12.6.2 There is no monetary threshold for making a report on a suspicious transaction.

12.6.3 A suspicious transaction may involve several factors that may on their own seem insignificant, but together may raise suspicion that the transaction is related to the commission or attempted commission of a money laundering offence, a terrorist financing offence, or both.

12.6.4 As a general guide, a transaction may be connected to money laundering or terrorist financing when the transaction (or a series of transactions) raises questions or gives rise to discomfort, apprehension, or mistrust.

12.6.5 The context in which the transaction or transactions occur or are attempted is a significant factor in assessing suspicion.

12.6.6 The context will vary from business to business, and from one Customer to another. DNFBPs should evaluate transactions using a risk-based approach, in an appropriate manner, within the normal practices in their particular line of business, and based on their knowledge of their customer.

12.6.7 Transactions that are inconsistent with the customer profile established at onboarding or that do not appear to be normal with industry practices may be relevant factors for determining whether there are reasonable grounds to suspect that the transactions are related to money laundering or terrorist financing.

12.6.8 An assessment of suspicion should be based on a reasonable evaluation of relevant factors, including the knowledge of the customer's business, financial history, background and behavior.

12.6.9 The DNFBPs should remember that behavior is suspicious, not people.

12.6.10 Suspicion could be based on a single factor, or it could be based on the combination of a number of factors.

12.6.11 All circumstances surrounding a transaction or series of transactions should be reviewed.

12.6.12 In determining whether or not the occasional transaction or inconsistent transaction is suspicious, the DNFBP should consider-

(a) whether the transaction has no apparent or visible economic or lawful purpose;

(b) whether the transaction has no reasonable explanation;

(c) whether the size or pattern of the transaction is not similar to the earlier size or pattern of the transactions of the same or similar customers;

(d) whether the customer has failed to provide an adequate explanation or full information on the transaction;

(e) whether the transaction involves a newly established business relationship, or is a one-off transaction;

(f) whether the transaction involves offshore accounts, companies, or structures that are not supported by the customer's economic needs;

(g) whether the transaction involves unnecessary routing of funds through third parties.

12.7 Who should submit the STR?

12.7.1 The STR should be made by the Money Laundering Reporting Officer or his deputy.

12.7.2 The DNFBP shall provide FIU with the contact information of their Money Laundering Reporting Officer or deputy and shall update FIU of any changes thereto**.**

12.8 When should an STR be submitted?

12.8.1 DNFBPs should promptly submit an STR to report any suspicious transaction or activity or on any attempt to perform such transaction or activity, irrespective of its value, when suspecting or having reasonable grounds to suspect that it is the proceeds of a predicate offence or in relation to terrorism financing, within 24 hours from the identification of the transaction as suspicious.

12.8.2 For attempted transactions, when a DNFBP receive an order from a customer to execute a transaction, and the said DNFBP suspect that the transaction's proceeds are from a criminal activity and/or are related to money laundering, or are linked to, or to be used in terrorist acts or by terrorist organizations, the STR must be submitted within twenty-four (24) hours from the date of determining that the transactions were suspicious, or on the first business day, whichever is soonest.

12.9 How to submit STRs?

12.9.1 DPMS must submit STRs through the FIU Electronic STR System.

12.9.2 The FIU Electronic STR system allow DNFBP to submit STRs electronically.

12.9.3 If electronic STR filing system is not available, the STR can be submitted by letter to the FIU Office to the following Address:
Commissioner,
Financial Intelligence Unit,
1 Madaraka Street,
P. O. Box 5145
11468 Dar es salaam
Tanzania
Tel: +255 22 2129457
Fax: +255 22 2129471
http://www.fiu.go.tz
fiutz@fiu.go.tz

12.10 STR contents

12.10.1 The DNFBP shall submit STRs to the FIU and complete all relevant fields in the standard form with as much accurate information as is available in the Suspicious Transaction Report Form adopted by the FIU.

12.10.2 The STRs are filed on a "suspicion " basis. And the suspect may be a customer or a non-customer.

12.10.3 The DNFBP shall indicate in the narrative field of the STR on the number of suspicious transactions, provide the transaction details separately and then submit it to the FIU as an STR attachment.

12.10.4 DNFBPs should disclose in any subsequent STR involving the same suspect that the suspicious transaction is related to another STR distinct from the previous one, by including the reference number of the suspicious transaction in the STR.

12.11 Reporting obligations

12.11.1 DNFBPs are protected from both criminal and civil liability for breach of any restriction on disclosure of information imposed by law or regulation or by administrative order or contract, if they report their suspicions in good faith; even if they did not know what the underlying predicate offence was, and regardless of whether the offence actually occurred.

12.11.2 DNFBPs are prohibited from disclosing to any unauthorized person whether or not a suspicious transaction report, or any other relevant

information is being or has been filed with the FIU the act which is known as tipping off.

12.11.3 Tipping off is a criminal offence subject to penalties under the law.

12.11.4 DNFBPs may share information on STRs with foreign branches and majority-owned associates to the extent that this is necessary to maintain a unified AML/CFT program.

13.0 Requests for Information by the FIU

13.1 Pursuant to the Law the FIU may request information that is deemed necessary for the performance of its duties.

13.2 The FIU may request information from any person or entity subject to reporting obligations.

13.3 The requested information shall be submitted within the timeframe and form specified by the FIU.

13.4 DNFBPs must comply with requests for information requested by the FIU with regard to suspicious transactions or information that may be associated with money laundering and terrorism financing.

14.0 Non-compliance and Tipping-Off

14.1 DNFBPs are required to comply with the requests for information received from the FIU or regulator with regard to suspicious transactions or transactions associated with money laundering and terrorism financing.

14.2 Non-compliance or non-response to the requests, compels the FIU or the regulator to adopt the following measures:

(a) following the lapse of the timeframe specified in this request to submit a report or the deadline set to comply with the request, the FIU or regulator shall issue a reminder to comply;

(b) after issuance of reminder, the FIU or regulator shall warn the DNFBP that their continued noncompliance will be result to taking further administrative measures including suspension of business;

(c) with continued non-compliance, the FIU will inform the relevant regulator to take the necessary administrative and financial measures and penalties.

14.3 DNFBPs that fail to meet their obligations under Law are subject to such financial and administrative measures and penalties.

15.0 Sanctions and Penalties Imposed on DNFBP for Breach of AML/CFT Obligations

15.1 In the event of a breach to the AML/CFT obligations, a DNFBP will be subject to the sanctions and penalties provided for in the law.

15.2 Penalties:

15.2.1 Under the law any person who contravenes any requirement under the law where no specific penalty is provided, is subject, if it is an individual person, to a fine not exceeding five hundred million shillings and not less than one hundred million shillings or be ordered to pay the amount equivalent to the total amount of money involved or market value of the property, which ever amount is greater or imprisonment for a term not exceeding three years.

15.2.2 A body corporate, it is subject to a fine of not less than five hundred million shillings or be ordered to pay the amount equivalent to the total amount of money involved or market value of the property, which ever amount is greater.

15.2.3 For body corporates, every director, manager, controller, principal officer or any person holding a similar position in a body corporate will be deemed to have committed the offence unless that person proves that, the offence was committed without his consent or connivance and that he exercised diligence to prevent the commission of the offence as he ought to have exercised, having regard to the nature of his functions in that capacity and to the circumstances pertaining to commission of the offence.

15.2.4 Contravention on undertaking risk Assessment, risk mitigation measures and allocation of resources is subject to administrative penalties to be administered by FIU or the Regulator. These may include warning and entering into an agreement for remedial measures t be taken within specified time lines.

15.2.5 Contravention against conducting CDD is subject to general penalty set out in paragraphs 15.2.1 and 15.2.2;

15.2.6 Contraventions against establishing and maintenance of records is subject to administrative or if convicted, to a general penalty.

15.2.7 Failure to file STR attracts a fine of not exceeding five million or a 5-years term of imprisonment to and individual or if a body corporate, to a fine of ten million or 3 times the market value of the property involved.

15.2.8 Failure to establish and maintain internal policies and procedures attracts a general penalty.

15.2.9 Failure to implement groupwide programmes is subject to administrative sanctions or if convicted to five hundred thousand shillings for individuals or a term of 12 months imprisonment. For companies, it attracts a five million shillings but not exceeding ten million shillings.

15.3 The administrative penalties

15.3.1 Administrative penalties that may be imposed by FIU and regulators include the following:

(a) warning or caution not to repeat the conduct which led to non-compliance;

(b) reprimand;

(c) directives to take remedial action or to make specific arrangement to remedy the default;

(d) restriction or suspension of certain business activities;

(e) suspending a business licence; or

(f) suspension or removal from office any member of staff who caused or failed to comply.

Dar es Salaam
January, 2023

Fatma A Simba
Commissioner, FIU

Annex A

SAMPLE AML/CFT POLICIES AND PROCEDURES MANUAL FOR DNFBPS

1.0 INTRODUCTION

The of the Anti-Money Laundering Act (Cap. 423) and the Anti-Money Laundering and Proceeds of Crime Act No 10 of Zanzibar, are intended to impose certain duties on institutions and other persons, businesses and professions who may be used for money laundering purposes among others. The legislations define "reporting persons" to include a number of businesses, financial institutions and professions. The legislation succinctly requires reporting persons to develop and implement policies, controls and procedures to enable the accountable person to effectively detect, manage and mitigate the identified risks in the future related to Money laundering, Terrorist Financing and Proliferation Financing activities.

The competent authorities are required not to grant licenses for any particular reporting person unless they inspect and approves the firm for compliance with the AML/CFT/CFP requirements under the law. It is based on the above requirements that this sample procedures and policy document intends to give guidance on how reporting persons can maintain sufficient response to matters of AML.

The requirements of the manual can be scalable to the size of the firm to deal with differences in the size of firms and nature of the services they provide.

2.0 GENERAL POLICY STATEMENT

ABC Company is committed to full compliance with all applicable laws and regulations regarding Money Laundering and Terrorist Financing. ABC Company has adopted and will enforce the provisions set forth in the Anti-Money Laundering & Counter Terrorist Financing Policy and Procedures Manual in order to prevent and detect money laundering, terrorist financing and other illegal activities. The Management of ABC consider Integrity as a key commitment on the part of the company to uphold strict standards of ethical conduct and hence preservation of a stable value for society confidence. These policies endorse the strict compliance with the legal framework governing the prevention of money laundering, terrorism financing and proliferation financing.

The Company's commitment to this objective is set forth in this Policy which defines the guiding policies for adequate prevention and control. It includes procedures for the detection and reporting of activities possibly linked to money laundering or the financing of terrorist or proliferation activities.

If ABC and/or its personnel are inadvertently used for money laundering or other illegal activities, ABC can be subject to potentially serious civil, criminal or administrative penalties. Therefore, the appropriate application of the Policy requires that staff of the firm be familiar with the contents herein, related procedures and norms that regulate the various activities and services of the firm as compliance with the provisions is compulsory to all the firm's staff.

3.0 POLICY STATEMENT

3.1 It is the policy of ABC that all members of staff at all levels actively participate in preventing the services of the company from being exploited by criminals and terrorists for money laundering purposes. This participation has its objectives as:

3.1.1 Complying with all Anti - Money Laundering laws and Regulations of the country requiring all Employees to prevent, detect and report to the AMLRO all potential instances in which ABC the company or its employees, its facilities or its activities have been or are about to be used for money laundering, terrorist financing, proliferation financing and other illegal activity;

3.1.2 Providing for a AMLRO who shall ensure adherence to the ABC AML/CFT/CFP Policies and Procedures;

3.1.3 Requiring all appropriate employees to attend anti-money laundering training sessions, so that all employees are aware of their responsibilities under ABC policies and procedures; these Guidelines and as affected by current developments with respect to anti-money laundering legislations.

3.2 Protecting the company and all its staff as individuals from the risks associated with breaches of the law, regulations and supervisory requirements.

3.3 Preserving the good name of the company against the risk of reputational damage presented by implication in money laundering, terrorist financing and proliferation financing activities.

3.4 It shall be the policy of this company that-

3.4.1 Every member of staff shall meet their personal obligations as appropriate to their role and position in the company.

3.4.2 Neither commercial considerations nor a sense of loyalty to clients shall be permitted to take precedence over the company's anti-money laundering commitment.

3.4.3 The company shall carry out a business-wide assessment of the risks of money laundering, terrorist financing and proliferation financing to which the company is subject and design and implement appropriate controls to mitigate and manage effectively the risks identified.

3.4.4 The company shall establish and maintain documented, proportionate policies and procedures, including controls, which outline the positive actions to be taken by staff to prevent money laundering, terrorist financing and proliferation financing in the course of their work.

4.0 POLICY AND PROCEDURE REGARDING THE ANTI MONEY LAUNDERING REPORTING OFFICER(AMLRO)

4.1 Policy

It is the policy of the company that a AMLRO shall be appointed and this shall be a person in a senior managerial position, possessing sufficient professional experience and competence.

4.1.1 The company shall notify the appointment of such a person or their cessation to the position to other staff of the company and to the relevant authorities.

4.1.2 For avoidance of doubt, in this manual, relevant authorities shall include the Financial Intelligence Authority and the sector or industry regulator;

4.2 Procedures

4.2.1 The company shall appoint a senior person in the company as the MLRO who shall from time-to-time coordinate AML activities and compliance responsibilities.

4.2.2 Any staff shall immediately notify the MLRO if he/she suspects or has any reason to suspect that any potentially suspicious activity or transaction has occurred or will occur if a transaction is completed.

4.2.3 Staff are encouraged to seek the assistance of the MLRO with any questions or concerns they may have with respect to the ABC & ASSOCIATES' Anti-Money Laundering Policies or Procedures.

4.2.4 Responsibilities of the MLRO include the following:

(a) coordination and monitoring of ABC's day-to-day compliance with applicable Anti- Money Laundering Laws and Regulations and ABC's own Anti-Money Laundering Policy and Procedures;

(b) develop and implement systems, mechanisms and procedures to ensure that the staff of the accountable person report any suspicious money laundering or financing of terrorism activity;

(c) conduct staff training programs for appropriate personnel related to the ABC's anti-money laundering policy and procedures and maintaining records evidencing such training;

(d) receive and review any reports of suspicious activity from staff;

(e) coordination of enhanced due diligence procedures regarding clients and respond to both internal and external inquiries regarding ABC' AML/CFT policies and procedures.

(f) notify the relevant authorities of any suspicious money laundering, financing of terrorism or financing of proliferation activity.

5.0 POLICY AND PROCEDURE FOR AML TRAINING PROGRAM FOR STAFF

5.1 Policy

It is the policy of ABC that recruitment of all staff will include adequate screening procedures to ensure high standards when hiring staff.

5.1.1 It is the policy of ABC that all staff who have client contact, or access to information about clients' affairs, shall

receive AML/CFT training to ensure that their knowledge and understanding is at an appropriate level, and ongoing training at least annually to maintain awareness shall be ensured.

5.1.2 It is the policy of ABC that all staff who have client contact, or access to personal data relating to clients, shall receive training on the law relating to data protection to ensure that their knowledge and understanding is at an appropriate level, and ongoing training at least annually to maintain awareness and ensure that the company's legal obligations are met.

5.1.3 It is the policy of the company that all staff are required to reconfirm their awareness of the contents of this Compliance Manual by signing the acknowledgement form annually, or more frequently, as required by the MLRO.

5.1.4 The MLRO shall ensure that training is made available to staff according to their exposure to ML, TF and PF risks, and that steps are taken to check and record that training has been undertaken and that staff have achieved an appropriate level of knowledge and understanding.

5.2 Procedure

5.2.1 All staff are required –

(a) at a time specified by the MLRO, to undertake training programs on anti-money laundering policies and procedures;

(b) to get trained in how to recognize and deal with transactions which may be related to ML.TF and PF;

(c) to timely escalate and report the matter to the MLCO;

(d) to get themselves acquainted and comply with Anti Money Laundering laws and Regulations.

5.2.2 The MLRO will, evaluate alternative AML/CFT training methods, products and services in order to make suitable training activities available to all members of staff who have client contact, or access to information about clients' affairs.

5.2.3 The training programme will include means to confirm that each individual has achieved an appropriate level of knowledge and understanding, whether through formal testing, assessment via informal discussion, or other means.

5.2.4 The MLRO will keep records of training completed, including the results of tests or other evaluations demonstrating that each individual has achieved an appropriate level of competence.

5.2.5 The MLRO will assess the effectiveness of the programme completed and update the training information to match with the changes in laws, regulations, guidance and practice as a way of considering relevant continuity of the training programme.

6.0 POLICY AND PROCEDURE FOR CLIENT IDENTIFICATION

6.1 Policy

6.1.1 It is the policy of DNFBPs AML/CFT/CFP policies and procedures that, prior to accepting funds from Clients, all reasonable and practical measures are taken to confirm the clients' identities and to verify that any third party upon whom DNFBPs relies for client identification, adheres to the same standards.

6.2 Procedure:

6.2.1 These Client Identification Procedures are based on the premise that the DNFBPs will accept funds from a new and existing Client only after:

(a) DNFBPs has confirmed the client's identity and that the client is acting as a principal and not for the benefit of any third party unless specific disclosure to that effect is made; or
(b) if the client is acting on behalf of others, DNFBPs has confirmed the identities of the underlying third parties.

6.2.2 The Client Identification Procedures shall be reviewed in light of the specific characteristics presented by a client and in any instance the MLRO may determine to apply Enhanced Due Diligence (EDD) measures where the client

pose high ML/TF/PF risks.

6.2.3 As a reference tool, an Individual Client KYC Checklist shall be used at DNFBPs and all Staff are encouraged to provide the MLRO with any revisions they consider appropriate.

6.2.4 The MLRO shall retain copies of all documents reviewed or checklists completed in connection with its Client Identification Procedures in accordance with DNFBPs Client Records Retention policies.

6.2.5 The member of staff conducting verification of identity will complete the process by checking that the client is not the subject of sanctions or other statutory measures, using the screening methods set out by the MLRO.

6.2.6 The company's MLRO will maintain a list of acceptable documents or information obtained from a reliable source which is independent of the client.

6.2.7 In cases where a client cannot produce acceptable documents, the responsible staff will make a risk-based decision on accepting the documents that are available, and shall immediately consult the MLRO whether or not to onboard the client.

6.2.8 Where the client is not the beneficial owner of assets involved, the responsible staff will take the necessary steps to determine who the beneficial owner is, and take reasonable measures to verify their identity accordingly.

6.2.9 The MLRO will prepare a format for use by the responsible staff in requesting verification of identity and beneficial ownership information from relevant corporate entities and trustees, and a procedure for following up when requests are not met within the statutory period.

6.2.10 If all possible means of identifying the beneficial owner of a client entity have been exhausted without success, and recorded, the responsible staff will seek the approval of the MLRO, to be given on a risk-sensitive basis, to treat as its beneficial owner the natural person who exercises ultimate effective control over the client entity.

6.2.11 In all cases assessed as presenting a higher money laundering risk, where enhanced client due diligence is required, the MLRO will consult with the Executive or Managing Director to decide on additional steps to verify the client's identity.

6.2.12 All verification of identity processes as well as actions taken to verify the identity of corporate entities will be recorded and will include keeping photocopies of documents produced, or in exceptional cases with the approval of the Managing director, recording information about where copies are held and can be obtained.

7.0 CLIENT IDENTIFICATION PROCEDURES FOR NATURAL PERSONS

7.1 Policy:

7.1.1 DNFBPs shall take reasonable steps to ascertain satisfactory evidence of an individual client's name, details of the residential address, the telephone contact including the mobile telephone, e-mail address, date and the source of the client's funds.

7.2 Procedure:

7.2.1 In order to confirm the identity of the client, copies of the following documents will be obtained and retained for DNFBPs records:

(a) the client's national identification card or an any other officially recognized identification document, whichever is applicable;

(b) an introductory letter from the employer or a senior government official attesting to the identity of the person;

(c) in the case of a student, an introductory letter from the school and a copy of the student's identity card;

(d) a summary of the nature of business activities the person is engaged in.

7.2.2 Additional information which may be requested for includes:

(a) utility bills including electricity and water bills;

(b) details on occupation or employment;

(c) details of source of income;

(d) income tax identification number, where applicable.

7.3 Procedures for Corporations, Partnerships, Trusts and Other Legal Entities

7.3.1 DNFBPs shall take reasonable steps to ascertain satisfactory evidence of an entity client's name and address, its authority to make the contemplated investment.

7.3.2 DNFBPs will obtain certainty of the following, as appropriate under the circumstances:

(a) the name of the entity, and where applicable its registered name and registration number;

(b) a copy of the constitutive document or trust deed or the power that binds the entity ;

(c) details of the registered address or principal place of business or office;

(d) the names, date and place of birth, identity card number or passport number, tax identification number and address of persons managing the entity;

(e) the financial statements of the immediate last year in case of partnerships; and

(f) the full name of the trustee, beneficiaries or any other natural person exercising control over the trust; and

(g) the founder, sponsor or protector of the trust in case of a trust

7.3.3 Where the client is a corporate entity such as a private limited company, the responsible staff will check that the entity is appropriately incorporated and registered, and take the necessary steps to determine who are the principal beneficial owners, and the people with significant control, and their identity will be verified according to this procedure.

7.3.4 DNFBPs shall follow identification requirements as prescribed by the Regulations to establish the identity of foreign nationals, entities and local entities and other bodies.

8.0 POLICY AND PROCEDURE FOR MONEY LAUNDERING RISK ASSESSMENT

8.1 Policy:

8.1.1 It is the policy of the company to identify and assess the money laundering, terrorist financing and proliferation financing risks represented by the business the company conducts so that the company can mitigate that risk by applying appropriate levels of client due diligence.

8.1.2 It is the policy of the company that the MLRO will from time to time update a list of the types of clients that the company considers to be of 'high risk,' such that enhanced due diligence procedures are warranted compared to the routine client identification procedures.

8.2 Procedures:

8.2.1 The company shall assess the money laundering risk represented by our clients and the business conducted according to three levels:

(a) the range normally dealt with by the company, requiring the company's normal level of client due diligence;

(b) an exceptionally high level of risk requiring an enhanced level of client due diligence;

(c) a negligible level of risk requiring only simplified or reduced due diligence measures.

8.2.2 The company shall identify and maintain lists of risk factors (including those required by the Regulations) relating to our clients, products or services, transactions, delivery channels and geographic areas of operation.

8.2.3 The company shall update the risk assessment annually to ensure new and emerging risks are addressed, and new information supplied by our regulatory authority is reflected.

8.2.4 The money laundering, terrorist financing and proliferation risk represented by each client will be assessed:

(a) during the new client acceptance process and/or during client continuance process for continuing clients;

(b) whenever the company's process of ongoing monitoring indicates that a change in the business or operating environment of an established client may represent a change in money laundering risk.

8.2.5 Client risk assessment shall be carried out by the responsible staff who will determine appropriate due diligence measures in respect of each client based on:

(a) the company's business-wide risk assessment;

(b) assessment of the level of risk arising in any particular case.

8.2.6 A record must be made of the assessment of individual client relationships, confirming that the company's business-wide risk assessment has been taken into account, and any other relevant factors considered.

8.2.7 The following are the examples of clients who pose a high money laundering risk:

(a) a political figure, any member of a political figure's immediate family, and any close associate of a senior political figure;
(b) any client resident in, or organized or incorporated under the laws of, a non-Cooperative Jurisdiction or high-risk countries;
(c) any client who gives the MLRO any reason to believe that its funds originate from, or are routed through, an account maintained at an "offshore bank", or a bank organized or chartered under the laws of a non-cooperative jurisdiction; and
(d) any client who gives the MLRO any reason to believe that the source of its funds may not be legitimate or may aid terrorist activities.

8.2.8 **Client Identification Procedures For 'High-Risk' Natural Persons**

Enhanced Client Identification Procedures shall be conducted for 'high risk' natural persons and such procedures shall include, but are not limited to, the following:

(a) assessing the client's business reputation through review of financial or professional references, generally available media reports or by other means;

(b) considering the source of the client's wealth, including the economic activities that generated the client's wealth and the source of the particular funds intended to be used to make the investment;

(c) reviewing generally available public information, such as media reports, to determine whether the client has been the subject of any criminal or civil enforcement action based on violations of anti-money laundering laws or regulations or any investigation, indictment, conviction or civil enforcement action relating to financing of terrorists;

(d) The enhanced due diligence procedures undertaken with respect to 'high risk' clients must be thoroughly documented in writing, and any questions or concerns with regard to a 'high risk'.

9.0 POLICY AND PROCEDURE FOR KNOWING THE CLIENT'S BUSINESS AS PART OF CUSTOMER DUE DELIGENCE (CDD)

9.1 Policy

9.1.1 It is the policy of this company to obtain information enabling us to assess the purpose and intended nature of every client's relationship with the company.

9.1.2 It is the policy of the company to keep any information obtained during a CDD for a minimum period of five years from the date the relevant business or transaction is completed with the client.

9.1.3 It is the policy of this company not to offer its services, or to withdraw from providing its services, if a satisfactory

understanding of the nature and purpose of the client's business with us cannot be achieved.

9.2 Procedures

9.2.1 The responsible staff will obtain Know Your Client's business information from clients:

(a) on acceptance of a new client;

(b) on receipt of a new instruction from a client whose arrangements are of a one-off nature;

(c) on any significant change in the client's arrangements such as the size or frequency of transactions, nature of business conducted, involvement of new parties or jurisdictions;

(d) as an ongoing exercise throughout the client relationship.

9.2.2 Know Your Client's information sought from clients will include, but not be limited to-

(a) the client's reason for choosing this company;

(b) the purpose and business justification behind the services the client is asking the company to provide;

(c) the provenance of funds introduced or assets involved in the client's arrangements;

(d) the nature, size, frequency, source and destination of anticipated transactions;

(e) the counter-parties and jurisdictions concerned.

9.2.3 The information will be obtained by interview between the company's staff and the client's representative and this information shall be recorded on the client file, to assist with future monitoring of the client relationship.

9.2.4 The information volunteered by the client shall be corroborated for consistency with any publicly accessible information to the best extent possible.

9.2.5 Where answers given by the client are implausible, or inconsistent with other information, or where the client is unwilling to provide satisfactory answers to due diligence enquiries, the responsible staff will consider whether the company should withdraw from the relationship.

10.0 POLICY AND PROCEDURE FOR INTERNAL REPORTING OF SUSPICIOUS TRANSACTIONS

10.1 Policy;

10.1.1 It is the policy of this company that every member of staff shall remain alert for the possibility of money laundering, and shall pay attention to and report all complex, unusual or large transactions, whether completed or not, and to all unusual patterns of transaction which have no apparent economic or lawful purpose and every suspicion for which they believe there are reasonable grounds, following the company's procedure.

10.1.2 It is the policy of the company that every member of staff shall pay attention to and report to the MLRO:
(a) any transactions made on behalf of a person whose identity has not been established;
(b) business relations and transactions with persons in jurisdictions that do not have adequate systems to prevent or deter money laundering, financing of terrorism or proliferation financing; and
(c) electronic funds transfers that do not contain complete originator information.

10.1.3 The expectation placed on each individual member of staff in responding to possible suspicions shall be appropriate to their position in the company.

10.2 Procedures:

10.2.1 Every member of staff must be alert for the possibility that the company's services could be used for money laundering purposes, or that in the course of their work they could become aware of criminal or terrorist property.

10.2.2 A member of staff becoming aware of a possible suspicion shall gather relevant information that is routinely available to them and decide whether there are reasonable grounds to suspect money laundering.

10.2.3 Any additional CDD information acquired, in particular any explanations for unusual instructions or transactions, shall be recorded on the client file in the routine manner, but no mention of suspected money laundering is to be recorded in any client file.

10.2.4 The requirement to gather relevant information does not extend to undertaking research or investigation, beyond using information sources readily available within the company.

10.2.5 If after gathering and considering routinely available information, the member of staff is entirely satisfied that reasonable grounds for suspicion are not present, no further action shall be taken otherwise where there are reasonable grounds for suspicion, the staff shall raise the matter with the MLRO.

10.2.6 Where a member of staff based on their own observations decides that there are reasonable grounds to suspect money laundering, he or she shall submit a suspicion report to the MLRO, in the format specified by the MLRO for that purpose and such internal suspicion report does not breach client confidentiality.

10.2.7 A member of staff who forms or is aware of a suspicion of money laundering shall not discuss it with any outside party, or any other member of staff unless directly involved in the matter causing suspicion.

10.2.8 No member of staff shall at any time disclose a money laundering suspicion to the person suspected, whether or not a client, or to any outside party and

10.2.9 where the circumstances arise that may cause difficulties with client contact, the member of staff must seek and follow the instructions of the MLRO.

11.0 POLICY AND PROCEDURE FOR ONGOING MONITORING OF CLIENTS' ACTIVITIES POLICY

11.1 Policy:

11.1.1 It is the policy of this company to put in place policies, controls and procedures for monitoring the implementation of policies, controls and procedures to address the risks relating to money laundering and terrorism financing, and where necessary, enhance them on a regular basis.

11.1.2 It is the policy of the company to maintain a system of regular, independent reviews to understand the adequacy and effectiveness of the Money laundering, terrorist financing and proliferation financing systems and any weaknesses identified.

11.1.3 It is the policy of this company to monitor clients' instructions and transactions to ensure consistency with those anticipated and with the client risk profile.

11.2 Procedures

11.2.1 All staff will maintain alertness for clients' instructions and transactions which represent a significant divergence from those anticipated for the client and feedback shall be communicated to the MLRO.

11.2.2 The company shall employ a suitable mechanism for monitoring clients' transactions, according to their number and the involvement or otherwise of members of staff in their execution.

11.2.3 Where a client's instruction or transaction is not consistent with what is anticipated, an explanation will be sought, if appropriate by contacting the client.

11.2.4 The involvement of unexpected jurisdictions or organization will be checked with the company's MLRO for possible alerts or sanctions-

(a) if a satisfactory explanation is found, the client file will be updated to record that explanation and to reflect the change in anticipated client activities;

(b) if no satisfactory explanation is found, the matter will be brought to the attention of the MLRO, who will consider whether there are grounds to suspect money laundering, terrorist financing or proliferation financing.

11.2.5 The MLRO will consider whether there is cause to carry out a re-assessment of money laundering, TF or PF risk, and if so, will carry this out.

11.2.6 Irrespective of whether specific incidents have caused a re-assessment of money laundering risk, every client

file will be reviewed periodically to check that-

(a) the information held is still adequate, correct and up to date;
(b) (b) the level of client due diligence being applied is still appropriate.

11.2.7 Periodic review of client files will be conducted at the following intervals:

(a) for high-risk clients – every six months; and

(b) for all other clients – annually.

11.2.8 As part of their improvement efforts, the company shall monitor publicly-available information on best practice in dealing with Money laundering, terrorist financing and proliferation financing risks.

12.0 POLICY AND PROCEDURE FOR KEEPING RECORDS OF CLIENT DUE DILIGENCE INFORMATION

12.1 Policy

12.1.1 It is the policy of this company to establish and maintain systems to keep records of enquiries made and information obtained while exercising client due diligence for AML purposes, and to ensure that these records are retrievable as required for legal and regulatory stipulations.

12.1.2 It is the policy of this company to ensure that principles of customer due diligence are adhered to at the start of a new business relationship, at appropriate points during the lifetime of the relationship and when an occasional transaction is to be undertaken.

12.2 Procedures:

12.2.1 When information is being collected for AML/CFT/CFP client due diligence, the responsible staff will ensure that-

(a) information collected is recorded in a consistent manner in the client file, or other appropriate place;

(b) all instances are recorded where information requested has not been forthcoming, or where explanations provided have not been satisfactory.

12.2.2 The company shall have systems to routinely archive CDD records along with the company's accounting records to ensure their availability for a minimum of ten years from the date of the completion of the transaction or enquiry.

12.2.3 The company shall have data retrieval systems which facilitate full and rapid retrieval of all relevant CDD records by authorized staff, in order to respond fully to enquiries from financial investigators.

12.2.4 The company shall have procedures to ensure that any personal data obtained for CDD purposes is processed only for the purposes of preventing money laundering, terrorist financing and proliferation financing.

12.2.5 The company shall provide new clients with the statement prior to establishing a business relationship that any personal data received from the client will be processed only for the purposes of preventing money laundering, terrorist financing and proliferation financing.

12.2.6 The company shall have a procedure to earmark relevant personal data for deletion at the end of the ten-year retention period unless-

(a) it is required for court proceedings;

(b) the data subject has given express consent to the retention of that data.

12.2.7 For clients who have been the subject of a suspicion, relevant records will be retained separately from the company's routine archives, and not destroyed, even after the ten-year period has elapsed, without confirmation from the MLRO that they are no longer required as part of an enquiry.

12.2.8 In recording and documenting money laundering, terrorist financing and proliferation financing suspicion reports, the MLRO shall at all times protect the company's position in accordance with any data protection law.

13.0 POLICY AND PROCEDURE FOR FORMAL DISCLOSURES TO THE AUTHORITIES

13.1 Policy:

13.1.1 It is the policy of this company that the MLRO shall receive and evaluate internal suspicion reports, and decide whether a formal disclosure is to be made to the authorities.

13.1.2 When so deciding, the MLRO will make the formal disclosure on behalf of the company, using the appropriate mechanism.

13.2 Procedure:

13.2.1 On receipt of a money laundering suspicion report from a member of staff, the MLRO shall acknowledge its receipt in writing, referring to the report by its date and unique file number, without including the name of the person(s) suspected and this shall be a confirmation to the member of staff that their legal obligation to report has been fulfilled.

13.2.2 The MLRO shall open and maintain a log of the progress of the report which shall be held securely and shall not form part of the client file.

13.2.3 Following receipt of a report, the MLRO shall gather all relevant information held within the company, and make all appropriate enquiries of members of staff anywhere in the company, in order properly to evaluate the report. The MLRO shall then decide whether they personally believe there are reasonable grounds for suspicion, and make a decision on the company's obligation to make a formal disclosure to the authorities.

13.2.4 All members of staff, anywhere in the company, shall respond in full to all enquiries made by the MLRO for the purposes of evaluating a suspicion report. Information provided to the MLRO in response to such enquiries does not breach client confidentiality/professional privilege, and no member of staff shall withhold information on those grounds.

13.2.5 If deciding that a formal disclosure to the authorities is required, the MLRO shall make such disclosure by the appropriate means.

13.2.6 The MLRO shall document in the report log the reasons for deciding to make or not to make a formal disclosure.

13.2.7 The MLRO shall where appropriately inform the originator of the internal report whether or not a formal disclosure has been made.

13.2.8 The MLRO shall inform all those, and only those, members of staff who need to be aware of the suspicion in order to protect them and the company from possible money laundering offences in connection with any related business.

13.2.9 Following a formal disclosure, the MLRO shall take such actions as required by the authorities in connection with the disclosure.

14.0 POLICY AND PROCEDURE FOR STOPPING/CONTINUING WORK FOLLOWING A SUSPICION REPORT

14.1 Policy

14.1.1 It is the policy of this company that from the moment a suspicion of money laundering arises, no further work will be carried out on the matter that gave rise to the suspicion.

14.1.2 It is also the policy of the company that neither commercial considerations nor the difficulty in responding to the client's enquiries on the matter shall be permitted to take precedence over the company's legal obligations.

14.1.3 Further, it is the policy of the Company that in the circumstances stated in paragraph 15, the MLRO shall act with all possible speed to enable work to continue, or if appropriate to withdraw from the client relationship, and assist staff in any communications with the client affected.

14.2 Procedures

14.2.1 As soon as a member of staff forms or becomes aware of a suspicion of money laundering, terrorist financing or proliferation financing, no further work is to be done on the matter giving rise to suspicion.

14.2.2 If there is any likelihood of the client becoming aware that work has stopped, for example because an anticipated transaction has not gone through, the member of staff concerned must contact the MLRO for instructions on how to handle the matter with the client.

14.2.3 On receipt of a suspicion report, the MLRO shall-

(a) instruct the originator of the report and any other staff involved to cease work on the matter giving rise to suspicion;

(b) decide in the shortest possible time whether all work for the client concerned should be stopped, or whether other work that is not the cause of suspicion may continue, and advise relevant staff accordingly;

(c) assist all affected staff in handling the matter with the client so that no tipping off offence is committed.

14.2.4 When work for a client has been stopped, the MLRO shall carry out the evaluation of the suspicion report as quickly as possible to decide whether a disclosure must be made to the authorities or not.

15.0 POLICY AND PROCEDURE FOR THE MONITORING AND MANAGEMENT OF COMPLIANCE

15.1 Policy

15.1.1 It is the policy of this company to monitor our compliance AML/CFT with legal and regulatory requirements and conduct an annual independent AML/CFT compliance audit, the findings of which are to be considered and appropriate recommendations for action set out.

15.1.2 The company's owner shall provide the necessary authority and resources for the ongoing implementation of a compliant AML regime.

15.2 Procedures

15.2.1 The MLRO will monitor continuously all aspects of the company's AML/CFT policies and procedures, together with changes and developments in the legal and regulatory environment which might impact the company's business-wide risk assessment.

15.2.2 Any deficiencies in AML/CFT compliance requiring urgent rectification will be dealt with immediately by the MLRO, who will report such incidents to the company's owner when appropriate and request any support that may be required.

15.2.3 The MLRO will facilitate and assist the Regulatory review team when conducting mandatory inspections on the company.

16.0 POLICY AND PROCEDURE FOR REVIEW OF THE MANUAL

16.1 Policy

16.1.1 It is the policy of this company to review the manual to keep it updated with the amendments in laws and regulations and also accommodate best practices

16.2 Procedure

16.2.1 A regular review of the program shall be undertaken to ensure that it is functioning as designed and such a review shall be performed by external or internal resources, and shall be accompanied by a formal assessment or written report.

16.2.2 If and when regulations are amended concerning reporting of suspicious activities, the company will amend this Manual to comply with those regulations.

Annex B

INDICATORS OF SUSPICIOUS ACTIVITY

The following as some indicators for red flags for ML/TF/PF in various sector in which DNFBPs operate

1.0 For jewelry dealers in precious stones and metals:

The following are common red flags a dealer in precious metals and stones take note and file STR/SAR.

(a) When the customer purchases items of high value without selecting any particular specifications or with no clear justification;

(b) When the customer's purchases items of high value which do not correspond with what is expected of him upon the identification of his profession or the nature of his business;

(c) When the customer regularly purchases high value commodities or large quantities of a specific commodity in a way that does not suit the usual deals carried out by the customer or the usual pattern of the business for his income or appearance;

(d) When the customer attempts to recover the amount of new purchases without a satisfactory explanation or when the customer tries to sell what he recently bought at a price that is much less than the purchasing price;

(e) When the customer attempts to sell items of high value at a price much less than their actual or market value;

(f) When the customer is willing to pay any price to obtain items of high value of extravagant amounts without any attempt to reduce or negotiate the price; and

(g) When the customer engages in any cash transactions equal to or above threshold ($10,000) or equivalent amount.

2.0 For lawyers and accountants, the following are common red flags or indicators of ML/TF/PF:

(a) When the customer appoints a lawyer in financial or commercial transactions and requests the concealment of the customer's name in any of these transactions;

(b) When the customer resorts to lawyers to create companies, particularly international business companies, from outside the country (offshore) in a way that shows that the objective of creating the company is to conceal the illicit source of the funds;

(c) When the customer resorts to lawyers to invest in the real estate market but the purchase or sale prices are not commensurate with the real estate value;

(d) When the customer requests, upon hiring a lawyer to incorporate a company, to transfer/deposit the incorporation fees or the capital to/in the bank account of the lawyer through multiple accounts that he has no relation to without a reasonable justification;

(e) When the lawyer manages investments portfolios, in countries allowing such conduct, and receives instructions from the customer to make buying and selling transactions that have no clear economic reason;

(f) When customers desire to create or buy a company that has a suspicious objective, does not realize profits or does not seem to be connected to his/her usual profession or related activities, without being able to submit sufficient explanations to the notary;

(g) When a customer sells assets or real estate properties repeatedly without realizing any profit margin or submitting a reasonable explanation in this respect;

(h) When the customer who creates or wishes to create different companies in a short timeframe for his own interest or the interest of other persons, without reasonable financial, legal or commercial grounds;

(i) When the customer uses another person as a facade to complete a transaction without any legitimate financial, legal or commercial excuse;

(j) When the customer does not indicate concern in incurring losses or realizing extremely low profits in comparison with persons engaged in the same business, or when the customer remains persistent in pursuing his activities;

(k) When the volume of foreign transfers from/to the client's accounts is high or when the sudden increase of the revenue and cash amounts he obtains is not consistent with his usual income and this activity lacks justification;

(l) When the customer receives cash money or high value checks, which do not suit the volume of his/her work or the nature of his/her activity, particularly if the transactions come from persons who are not clearly or justifiably connected to the client;

(m) When unjustified amounts in or deposits to the customer's account whose origin or cause is difficult to identify are made;

(n) When the customer transacts disproportionate amounts, and the frequency and nature of his transactions are not consistent with the nature of his business, profession or known and declared activity, particularly if these transactions are carried out with suspicious countries that are not connected to his apparent business domain; and

(o) When cash transactions in large amounts, including foreign exchange transactions or cross-border fund movement, if such types of transactions are not consistent with the usual commercial activity of the customer.

3.0 For all Designated Non-Financial Businesses and Professions (DNFBPs), the following red flags are common to suspicion of ML/TF/PF:

(a) When the customer has an unusually comprehensive knowledge of money laundering and terrorism financing issues and the AMLA, and the Terrorism Financing Law without any justification, as when the customer points out he wishes to avoid being reported;

(b) When the customer attempts to divide the amounts of any operations below the applicable designated threshold of reporting to the competent authorities;

(c) When the customer has an unusual interest in the internal policies, controls, regulations and supervisory procedures and unnecessarily elaborates on justifying a

transaction;

(d) When a customer has accounts with several international banks or has lately established relationships with different financial institutions in a specific country without clear grounds, particularly if this country does not apply an acceptable AML/CFT/CPF measures;

(e) When the customer is reserved, anxious or reluctant to have a personal meeting;

(f) When the customer uses different names and addresses;

(g) When the customer requests or seeks to carry out the transactions without disclosing his identity;

(h) When the customer refuses to submit original documentation particularly those related to his identification;

(i) When the customer intentionally conceals certain important information like his address (actual place of residence), telephone number or gives a non-existent or disconnected telephone number;

(j) When the customer uses a credit card issued by a foreign bank that has no branch or headquarters in the country of residence of the client while he does not reside or work in the country that issued said card;

(k) When the customer conducts cash transactions where banknotes with unusual denominations are used;

(l) When the customer conducts unusual transactions in comparison with the volume of the previous transactions or the activity pursued by the customer;

(m) When the customer conducts unnecessarily complex transactions or those that may not be economically feasible; and

(n) When the customer's transaction involves a country that does not have an efficient AML/CFT regime, or is suspected to facilitate ML or TF operations. or where drug manufacturing or trafficking are widespread.

(o) The customer is transacting without any purpose, economic justification, or underlying legal or trade obligation; purpose, or economic justification;

(p) The customer is transacting an amount that is not commensurate to the business or financial capacity of the customer or deviates from the profile of that customer;

(q) The customer might have structured transactions to avoid being the subject of a Covered Transaction Report;

(r) The customer has been or is currently engaged in any unlawful activity; or

(s) Raises suspicions that an intermediary is being used to circumvent anti-money laundering compliance measures.