MUKFIN
MUKOMA FINANCIAL SERVICES
Authorised Financial Services Provider : FSP No.47905

Address:
Block G, 1st Floor Palms Office Park,
391 Main Ave Ferndale, 2194
Randburg, Gauteng, South Africa

Email: admin@mukfin.co.za
Phone: +27 11 886 0667
Web: www.mukfin.co.za

ANTI-MONEY LAUNDERING (AML) POLICY

TABLE OF CONTENTS

1. PREAMBLE

1.1 The criminal activities of money laundering and terrorist financing have become a global problem as a result of several changes in world markets.

1.2 Republic of South Africa has demonstrated a strong commitment to fight money laundering and terrorism by enacting the Financial Intelligence Centre Act 38 of 2001 ("herein FICA").

1.3 The purpose of FICA is to introduce an Anti-Money Laundering ("AML") and Counter Terrorist Financing ("CTF") regulatory framework for Republic of South Africa and to establish the Financial Intelligence Centre.

1.4 The Republic of South Africa also enacted the Protection of Constitutional Democracy Against Terrorist and Related Activities Act 33 of 2004 ("POCDATARA"), the Prevention of Organised Crime Act 121 of 1998 ("POC Act"), and became the member of FATF in 2003.

1.5 The company recognises that it has been classified as a type of institution that is more readily targeted by criminals for money laundering or terrorist financing purposes.

1.6 The governing body has therefore committed itself to comply fully with FICA's regulatory requirements in order to make it more difficult for criminals to implicate the company in these activities.

2. DEFINITIONS

2.1 The definitions provided below have been adapted to align with the Mukfin's specific requirements and may not necessarily have the exact same meaning as that of similar legal definition.

2.2 **Beneficial Owner** - In respect of a legal person, means a natural person who, independently or together with another person, directly or indirectly owns the legal person or exercises effective control over the legal person. Ultimately this refers to the "warm body", a person who enjoys the benefits of ownership even though the title to some form of property is in another name.

2.3 **Business Relationship** - Means a relationship between a client and the company for the purpose of concluding transactions on a regular basis.

2.4 **Cash** - refers to coin and paper money of the Republic of South Africa or of another country that is designated as legal tender and that circulates as, and is customarily

used and accepted as, a medium of exchange in the country of issue, and includes travellers' cheques.

2.5 **Cash Threshold Report** – refers to the report that must be submitted to the FIC where a transaction is concluded with a client, and an amount of cash in excess of the prescribed amount, that is, R24, 999 is paid or received by the company in terms of that transaction. The cash threshold also includes a series of transactions or an aggregate of smaller amounts which when combined equal the amount of R24, 999. If it appears to the company that the transactions involving those smaller amounts are linked, these transactions must be considered as fractions of one transaction.

2.6 **Client** – refers to a person who has entered into a single transaction or a business relationship with the company.

2.7 **Client Representative** – refers to a natural person who has been authorised by a client to enter into a single transaction or a business relationship with the company on behalf of that client.

2.8 **Enhanced Client Due Diligence Procedure** – refers to the reasonable steps taken by the company to establish and verify the identity of a client that is party to a High-Risk money laundering or financing terrorist transaction, which steps are more stringent than a Quick Due Diligence and a Standard Due Diligence.

2.9 **Legal Person** – refers to any person, other than a natural person, that enters into a single transaction or establishes a business relationship, with the company, and includes a person incorporated as a company, close corporation, foreign company or any other form of corporate arrangement or association, but excludes a trust, partnership or sole proprietor.

2.10 **Money Laundering** – refers to an activity which has, or is likely to have, the effect of concealing or disguising the nature, source, location, disposition or movement of the proceeds of unlawful activities or any interest which anyone has in such proceeds.

2.11 **Non - compliance** - Any act or omission that constitutes a failure to comply with any of FICA's provisions, regulations, and the company's AML and CTF RMCP, or any order or directive made in terms of FICA.

2.12 **Property associated with Terrorist and Related Activities** - meaning derived and assigned to it in terms of Section 1 of the Prevention of Organised Crime Act 121 of 1998 ("POC Act"). Property in this context means:

- money, or any
- movable, immovable, corporeal or incorporeal thing, or any
- rights, privileges, claims and securities and any interest therein and all proceeds thereof, which were acquired, collected, used, possessed, owned or provided for the benefit of, or on behalf of, or at the direction of, or under the control of an entity (or another entity that has provided financial or economic support to such an entity) which commits or attempts to commit, or facilitates the commission of a specified offence as defined in POCDATARA.

2.13 **Quick Client Due Diligence Procedure** – refers to the reasonable steps taken by the organisation to establish and verify the identity of a client that is party to a Low-Risk money laundering or financing terrorism transaction, which steps are fewer and less onerous than a Standard Due Diligence and that of an Enhanced Due Diligence.

2.14 **Single Transaction** - A single transaction, means a transaction:

- other than a transaction concluded in the course of a business relationship, and
- where the value of the transaction is not less than the prescribed amount. i.e. R5,000

2.15 **Source of Funds** - Means the origin of the funds that will be used by the client in concluding a single transaction or which a prospective client is expected to use in concluding transactions in the course of a business relationship.

2.16 **Standard Client Due Diligence Procedure**- refers to the reasonable steps taken by the organisation to establish and verify the identity of a client that is party to a Moderate-Risk ML/TF transaction, which steps are fewer and less onerous than an Enhanced Due Diligence but more stringent that a Quick Due Diligence.

2.17 **Suspicious or Unusual Activity Report** – refers to the report that must be submitted to the FIC where there is reasonable knowledge in respect of the proceeds of unlawful activities or money laundering, and where the report relates to an activity which does not involve a transaction between two or more parties, or in respect of a transaction or a series of transactions about which enquires are made, but which has not been concluded, respectively.

2.18 **Suspicious or Unusual Transaction Report** – refers to the report that must be submitted to the FIC where there is reasonable knowledge in respect of the proceeds of unlawful activities or money laundering, and where the report relates to a transaction or a series of transactions between two or more parties.

2.19 **Terrorist and Related Activities** – derived and assigned meaning to it in Section 1 of the Protection of Constitutional Democracy Against Terrorist and Related Activities Act 33 of 2004 (“POCDATARA”).

3. POLICY PURPOSE

3.1 The purpose of this policy is to confirm Mukfin's commitment to implementing an effective Anti-Money Laundering and Counter -Terrorist Financing (AML/CFT) Policy, as required by FICA.

3.2 The purpose of this AML/CTF (FICA) Policy is to enable Mukfin to identify, assess, mitigate, manage and monitor the risk that the provision by the organisation of its products or services may involve or facilitate.

3.3 The Policy has been put in place in order to protect Mukfin from money laundering and terrorism financing risks, which may result in the company facing regulatory censure, fines and adverse reputational risk.

3.4 To ensure that the governing board have an overall oversight on the implementation of the Policy.

4. POLICY STATEMENT

4.1 Mukfin commits itself to achieving the following compliance objectives in terms of FICA:

4.1.1 To protect the integrity of Mukfin through the continued management of money laundering and terrorist financing risk.
4.1.2 To apply a risk-based approach to client transactions and to understand the purpose of all business relationships entered into with clients.
4.1.3 To ensure that the company design and implement the Risk Management Compliance Plan (RMCP) in accordance with Section 42 of the Act on an on-going basis.
4.1.4 To educate employees how to identify business relationships and transactions that pose a higher risk to money laundering and terrorist financing.
4.1.5 To implement robust Client Due Diligence procedures that will make it more difficult for criminals to hide the proceeds of unlawful activities.
4.1.6 To submit to FIC relevant reports concerning all transactions that are identified as being suspicious, unusual or above the prescribed cash threshold.
4.1.7 To keep accurate records of all FICA related transactions and Client Due Diligence procedures.
4.1.8 To prevent any reputational fallout or brand damage due to noncompliance with the Act and/or Mukfin's AML/CTF Policy.
4.1.9 To prevent any civil or criminal fines or penalties due to noncompliance with the Act and/or Mukfin's AML/CTF Policy.
4.1.10 To prevent loss of sales and client confidence due to noncompliance with the Act and/or Mukfin's AML/CTF.

5. POLICY OWNER

5.1 This Policy was adopted by the governing body. Any changes to the Policy must be approved by the governing body.

5.2 Questions about the Policy and its application should be directed to the Managing Director.

6. IMPORTANCE OF THIS POLICY TO THE COMPANY

6.1 Mukfin shall ensure that the governing body, management and all employees have a high level of integrity and when exercising their duties apply the regulations established in FICA and related regulations.

6.2 The employees of Mukfin shall not give advice or provide any other assistance to individuals who attempt to violate or avoid fulfilling the laws against assets laundering and the financing of terrorism or with this Policy.

6.3 The laws against money laundering and terrorist financing apply not only to individuals who attempt to legitimize funds resulting from illegal activities but also to other business parties, and their employees who participate in such transactions.

6.4 The employees of Mukfin or business parties that suspect certain operations, and deliberately avoid inquiring further on the matter with the intention to conceal, may be considered accomplices due to voluntary blindness within the scope of the anti-money laundering laws.

6.5 The employees of Mukfin that identify suspicious operations related to money laundering and financing of terrorism should report them to the respective Compliance Officer.

6.6 Failure to comply with this Policy may cause the company to take severe disciplinary actions against the employees including the removal thereto. Any violation of the laws against money laundering and terrorist financing may also result in the imprisonment of the infringer, as well as the imposition of significant fines to Mukfin and even the cancellation of the operating license.

7. APPOINTMENT OF A MONEY LAUNDERING REPORTING OFFICER (MLRO)

7.1 Mukfin shall appoint a Money Laundering Reporting Officer (MLRO).

7.2 The MLRO shall, among other things, be responsible for:

7.2.1 Monitoring and reporting of all suspicious transactions and sharing of information as required under the Act and related regulations,

7.2.2 Overseeing and ensuring overall compliance with regulatory guidelines on AML & CFT issues from time to time,

7.2.3 Developing appropriate compliance management arrangements across the full range of AML & CFT areas (e.g. CDD, record keeping, etc.),

7.2.4 Maintaining close liaison with law enforcement agencies, other designated institutions and any other institutions, which are involved in the fight against money laundering and combating financing of terrorism.

7.2.5 To enable the MLRO to discharge his responsibilities, Mukfin shall ensure that the MLRO and other appropriate staff members have timeless access to client identification data and other CDD information, transaction records and other relevant information.

7.3 Furthermore, the company shall ensure that the MLRO is able to act independently and report directly to the governing board.

7.4 In the absence of the designated MLRO, suspicious transactions shall be reported to the most senior person, as designated, and the report should be made in confidentiality.

7.5 Mukfin shall provide the MLRO with the necessary access to systems and records to enable him/her to investigate and validate internal suspicious reports which would have been reported to him/her.

8. CLIENT DUE DILIGENCE (CDD) & KNOW YOUR CLIENT (KYC) PRINCIPLE

8.1 Mukfin is mandated to know/understand its clients and their financial dealings better, which in turn helps in identifying suspicious transactions and managing of risk.

8.2 Further, an on-going Client Due Diligence exercise should be carried out. Client due diligence includes identifying, verifying and monitoring all aspects of the client's identity, residential address, any temporary address, and includes information on the source of funds and source of wealth. It also includes information relating to any beneficial owner who has an interest in the securities, or controller who exercises influence over the investment.

8.3 Mukfin shall implement a risk-based Client Due Diligence as outlined in **Annexure 1**.

8.4 Mukfin shall implement the following procedures regarding "Know your Client": -

8.4.1 Verify and document the true identity of the clients that establish a relation, open accounts or conduct significant transactions, according to FICA and internal business procedures.

8.4.2 Obtain and document any additional information on the client based on the risk per activity.

8.4.3 Make sure that no business transactions are carried out with companies or persons whose identities cannot be confirmed, failing to provide the required information or that provide false information or containing significant inconsistencies that cannot be satisfied after a further investigation.

8.4.4 In the case of natural persons, the respective official identification document or any other reliable document should be requested to verify the identity thereto, where necessary.

8.4.5 In the case of legal persons, the company's incorporation document and any information related to its main activity, address, key controllers, among others must be obtained, where necessary.

8.5 No account under a special name shall be opened (i.e. an account using a pseudonym or number instead of the real name of the client, unless otherwise allowed by the law).

8.6 Reasonable actions shall be taken to obtain information on the true identity of the person in whose name the relation is established, or an account is opened, or an operation is carried out.

8.7 Mukfin shall periodically update client identification data, on a yearly or a need basis, if there is a continuing business relationship.

8.8 Mukfin will not accept the following clients:

8.8.1 Persons or institutions of questionable honesty, especially if they are related with drug traffic, money laundering, terrorism or any organized crime.

8.8.2 Persons or institutions with business which are difficult to know the real source of their money.

8.8.3 Accounts with false names, anonymous or pseudonym instead of the real name of the client.

8.8.4 Nominee accounts, where the details of the beneficial owners will not be provided on request or difficult to be ascertained.

8.9 Examples of documents required to identify and verify the clients, are as per **Annexure 2**. The list is not exhaustive, but provides a minimum of documents required, based on the client's risk profile and the needs of the business.

8.10 All documents required for the purposes of identifying and verifying a client should not be **more than 3 months old**, and any certified documents should be certified by a recognised certifier.

8.11 Certifiers are required to sign under seal, state is/her name in block capitals, telephone number, profession, name and address of business or official stamp, and date on which the document is being certified. The certifier should not be closely related to the person whose identity is being certified (e.g. immediate family member, spouse, etc.).

8.12 Mukfin shall, where necessary, carry out independent verifications to verify any document provided by the client for the purposes of identifying and verifying clients.

8.13 Mukfin may outsource the services of any independent party to act on its behalf, for such purposes.

8.14 Whenever Mukfin engage with an intermediary or third party to introduce business, it shall:

8.14.1 Immediately obtain the account opening information:
8.14.2 Ensure the intermediary or third party provides the key account opening documents upon request as soon as possible (should Mukfin allow the intermediary or third party to keep the documents on its behalf, Mukfin understands it will assume all the risks attendant to the decision and arrangement); and
8.14.3 Satisfy itself that the intermediary or third party is regulated and supervised for, and has measures in place to comply with FICA.

9. HIGH RISK COUNTRIES

9.1 Clients domiciled in high risk countries automatically are assigned a high-risk status, and an Enhanced Due Diligence risk assessment should be conducted.

9.2 Mukfin shall from time to time adopt and utilise, as a minimum, the FATF high risk countries list, as the basis for classifying risk countries.

9.3 This requires and sets out the following criteria for relationships requiring enhanced due diligence (among others):
9.3.1 Domicile of the contracting party, controlling person or beneficial owner in a high-risk country;
9.3.2 Nationality of the contracting party or beneficial owner in a high-risk country;

9.3.3 Business activity of the contracting party/beneficial owner in risk country; or
9.3.4 Recurring payments from and into a high-risk country.

10. PREDICATE OFFENCES

10.1 A “predicate offence” is an offence whose proceeds may become the subject of any of the money-laundering offences established under the Organized Crime Convention.

10.2 Mukfin shall consider predicate offences as shown below (list not exhaustive), and will put measures to protect the business from any exposures relating to proceeds of these offences:

- participation in an organised criminal group and racketeering;
- terrorism, including terrorist financing;
- trafficking in human beings and migrant smuggling;
- sexual exploitation, including sexual exploitation of children;
- illicit trafficking in narcotic drugs and psychotropic substances;
- illicit arms trafficking;
- illicit trafficking in stolen and other goods;
- corruption and bribery;
- fraud;
- counterfeiting currency;
- counterfeiting and piracy of products;
- environmental crime;
- murder, grievous bodily injury;
- kidnapping, illegal restraint and hostage-taking;
- robbery or theft;
- smuggling; (including in relation to customs and excise duties and taxes);
- tax crimes (related to direct taxes and indirect taxes);
- extortion;
- forgery;
- piracy; and
- insider trading and market manipulation.

11. FRAUD MANAGEMENT

11.1 Fraud is a general term for deliberate misrepresentation and may include money laundering. The problems of fraud and especially money laundering is increasing at an unprecedented rate.

11.2 Each employee, within the value chain (at every level), shall be required to be the gatekeeper to identify and manage incidences of fraud, and any other financial crimes.

11.3 To identify cases of fraud or any other financial crime, staff will be required to do the following:

11.3.1 Know the client
11.3.2 Transaction monitoring
11.3.3 Segregate responsibilities
11.3.4 Avoid conflict of interest
11.3.5 Get relevant transactional approvals
11.3.6 Request source of funds and wealth from respective clients
11.3.7 Whistle blow cases of fraud

12. RECORD OF TRANSACTIONS

12.1 Mukfin shall keep the documentation and record of the transactions carried out by client s for at least five (5) years (or the term established by the law).

12.2 In addition, the following shall be kept:

12.2.1 Client s profiles
12.2.2 Transactions
12.2.3 Reports submitted to FICA in relation to suspicious transactions of clients for possible money laundering and terrorist financing
12.2.4 Reports of the training provided to the staff
12.2.5 Any other document required by law. All the retained information must be kept in strict confidence and may not be disclosed to third persons

12.3 Mukfin shall take appropriate steps to evolve and maintain a system that allows data to be retrieved easily and quickly whenever required, or when requested by competent authorities.
12.4 In the event that Mukfin outsource the record keeping responsibility to a third party, Mukfin acknowledges that it shall assume full responsibility and risk associated with the arrangement and shall ensure that the third party provides the requested documents within seven days.

13. CONTROL OF SUSPICIOUS TRANSACTIONS AND REPORTING

13.1 All the employees of Mukfin are obliged to promptly report to the MLRO, in confidentiality, any unusual or suspicious transaction, for the corresponding evaluation and subsequent reporting by the MLRO to FIC only.

13.2 Once a transaction has been detected and qualified as suspicious by the MLRO, it should be reported promptly to the FIC, and in any case should be reported promptly.

13.3 While determining suspicious transactions, Mukfin shall be guided by the definition of a suspicious transaction as stated in the definition of terms table.

13.4 The MLRO shall write and submit a Suspicious Transaction Report (STR) to the FIC, if it has reasonable ground of believing that the transaction, including an attempted transaction, involves proceeds of crime, irrespective of the amount of transaction and/or the limit envisaged for predicate offences as defined by FICA.

13.5 The MLRO shall record his/her reasons for treating any transaction or a series of transactions as suspicious. The MLRO shall ensure that there is no undue delay in arriving at such a conclusion once a suspicious transaction activity has been identified.

13.6 An STR shall then be filed with the FIC.

13.7 It is likely that in some cases, transactions are abandoned or aborted by clients on being asked to give more details or to provide documents. In such cases, the MLRO shall report all such attempted transactions by means of an STR, even if the transaction was not completed by the client, and irrespective of the amount of cash or transaction involved.

13.8 The STR shall be reported in the format as provided by the FIC, from time to time.

13.9 Mukfin shall take reasonable measures to ascertain the purpose of any transaction in excess of R24, 999 or a series of transactions or an aggregate of smaller amounts which when combined equal the amount of R24, 999, and the ultimate destination of the funds involved in the transaction.

14. TRAINING

14.1 Mukfin shall give priority / attention to the periodic training programs to the governing board, management and employees on AML & CFT.

14.2 The training programs must consider the AML & CFT laws of the Republic of South Africa and the recent trends on the subject, as well as the established anti-laundering internal policies and procedures.

14.3 The records of all the training courses carried out should be kept, including the date, names of each of the training participants, hierarchical level and group to which the trainees belong.

14.4 All new staff shall be trained on money laundering and terrorism financing as an entry requirement.

14.5 Mukfin shall conduct an on-going employee training programme which, at minimum, ensures that members of staff are adequately trained so that they are aware of:

14.5.1 policies and procedures relating to prevention of money laundering and counter terrorist financing, and

14.5.2 the need to monitor all transactions to ensure that no suspicious activity is being undertaken under the guise of transactions.

15. POLITICALLY EXPOSED PERSONS (PEP)

15.1 PEPs are the persons who perform or have performed public positions in the Republic of South Africa or abroad, including the high Officers of the Executive,

Legislature and Judiciary, the Public Ministry, the high Military Commands, Senior Executives and State Companies Directors, the country main cities Mayors and main political parties' representatives.

15.2 **What control must be taken about PEPs clients?**

15.2.1 If during commercial relationship, a client is classified as PEP; then he/she must be registered as such in a database, and approval for keeping the said relationship must be provided by the Managing Director or by the official on whom this responsibility has been delegated.
15.2.2 Gather sufficient information on any person/client of this category intending to undertake a transaction and check all the information available on the person in the public domain.
15.2.3 Apply enhanced client due diligence when verifying the identity of the PEP and seek information about the source/s of wealth and source/s of funds before accepting the PEP as a client.
15.2.4 The decision to undertake a transaction with a PEP shall be taken by the Managing Director or by the official on whom this responsibility has been delegated. The PEP transactions should be subject to enhanced monitoring on an on-going basis.

16. IMPLEMENTATION OF RISK-BASED APPROACH TO AML&CFT

16.1 Mukfin shall perform risk based analysis, keep to date and determine where money laundering and terrorist financing is high. The risk assessment shall be based on:

16.1.1 The nature, scale and complexity of the client 's operations, including geographical diversity;
16.1.2 The initial and on-going due diligence or monitoring conducted on the client;
16.1.3 Any previous relationships with the applicant or other parties to the application;
16.1.4 Time scale, especially in relation to early encashment (whether for the current application or previous transactions);
16.1.5 The nature of the client, product, and activity profile;
16.1.6 The nature of the business relationship (i.e. occasional vs. on-going relationship);
16.1.7 The volume, frequency and size of transactions; and
16.1.8 The extent to which Mukfin is dealing directly with clients or is dealing through intermediaries, third parties or in a non-face-to-face setting.

Controls for Higher Risk Situations

16.2 The following measures and controls to mitigate the potential money laundering and terrorism financing risks for situations that are considered to be of higher risk as a result of the risk assessment shall be considered.

16.2.1 Increased levels of KYC or enhanced due diligence, such as proactive contact with the client to determine the reason for the transactions and the source of funds;
16.2.2 Increased levels of controls and frequency of reviews of client relationships;
16.2.3 Increased transaction monitoring of higher-risk products, services and channels; and
16.2.4 Enhanced systematic controls and data integrity at the points of payment, particularly at higher risk agent location.

16.3 At least the following factors shall be considered to assign the risk profiles:
16.3.1 The different categories of clients (i.e. Type of business).
16.3.2 The nature of the products and services provided.
16.3.3 The expected use by the client of the products and services rendered.
16.3.4 The location of the clients businesses.
16.3.5 The transaction channel

17. INTERNAL CONTROLS, POLICIES & PROCEDURES

17.1 The governing body shall ensure that effective internal controls are put in place, by establishing appropriate AML and CFT policies and procedures, and ensuring effective implementation.

17.2 The ultimate responsibility for AML and CFT compliance is placed on the governing body and/or senior management.

17.3 The internal controls, policies and procedures shall cover proper management oversight systems and controls, segregation of duties, training and other related matters. Responsibility shall be explicitly allocated, so as to ensure that the policies and procedures are implemented effectively.

17.4 The internal audit and compliance functions have an important role in evaluating and ensuring adherence to the AML and CFT policies and procedures.

17.5 As a general rule, the compliance function should provide an independent evaluation of the policies and procedures, including legal and regulatory requirements.

17.6 Mukfin shall not put any restrictions on payment to beneficiaries where a STR has been made. Moreover, Mukfin shall ensure that employees keep the fact of furnishing such information as strictly confidential, and there is no tipping-off to the client at any level.

17.7 Employees shall not tip off clients who are subject for any investigation or where a case of suspicion has been raised. Tipping of clients shall be a disciplinary case.

18. FINAL STATEMENT

18.1 Any effort made by Mukfin will be insufficient if there is no full commitment by the governing board, management and all the employees to enforce the policies and actions taken to prevent Mukfin from being used as an intermediary to legitimize funds obtained from illegal activities and therefore, it is necessary and extremely important that all the rules and regulations contained in this document be fulfilled.

19. ANNEXURE 1 – CLIENT DUE DILIGENCE

Low Risk	**Moderate Risk**	**High Risk**
Simplified/Reduced CDD	**Standard CDD**	**Enhanced CDD**
Apply reduced or simplified identification measures where the risk of money laundering or terrorist financing is lower	Apply standard identification measures where the risk of money laundering or terrorist financing is moderate	Intensive due diligence shall be required, especially for those whose source of funds are not clear
Low Risk where: · Information on the identity of the clients and the beneficial owner of a client is publicly available. · Adequate checks and controls exist elsewhere in national systems.	**Medium Risk where:** · There is a potential risk, but it is unlikely that these risks will be realised. · Identify client and verify identity. · Gather information to understand the nature of the business relationship.	**High Risk where:** · Information is not readily available · Involves cross border transactions dominated by non-residents · Client resides from a high-risk jurisdiction

Low risk clients	Medium risk clients	High Risk Clients
· Public companies (listed on a Stock Exchange or similar situations) that are subject to regulatory disclosure requirements; · Government ministries and parastatals or enterprises; · Beneficial owners of pooled accounts held by Designated Non-Financial Businesses and Professions (DNFBPs), provided that they are subject to AML/CFT requirements consistent with the provisions of the Act.	· For standard-risk clients, i.e. those who are permanently resident in the country, with a salaried job or other transparent source of income, only the standard information provided may need to be verified.	· Non-resident clients; · Clients from countries that do not or insufficiently apply the FATF standards; · High net worth individuals; · Politically Exposed Persons (PEPs); · non-face-to-face clients; · Clients with dubious reputation as per public information available; · Transactions involving accounts in multiple jurisdictions; · The use of front persons or entities (e.g. corporations, trusts, fiduciaries and nominee accounts); · Entities with complex corporate structures;

20. ANNEXURE 2 – KYC DOCUMENTS

Identification Document (ID)	Proof of Address (POA)
Individual · Identification Document issued by a recognised authority · Current signed Passport · 2 Passport Size Photographs – Each must be certified at the back that it is a true likeness of the individual by a notary. **Companies/ Legal Person** · Certificate of Incorporation (showing the client's incorporation or business identification number and the place of issue of its incorporation or business identification number) · Trust Deed · Constitution · Board resolution · Identification documents for key individuals and beneficial owns with more than 10% shareholding in the company/legal person.	Any one of the following valid documents reflecting client's name and physical residential address are acceptable as POA: · Utility bill, e.g. municipal water and lights account or property managing agent statement · Stamped bank statement from another bank on an official bank document or form · Municipal councillor's letter · Tax certificate /Official tax document · Recent active lease or rental agreement · Municipal rates and taxes invoice not older than three months · Account statement from a registered service provider · Telephone or cellular telephone statement · Long/short term insurance policy documents from another from a registered insurance company · Body corporate/governing body letter or statement

21. ANNEXURE 3 – LIST OF THE POCDATARA OFFENCES

21.1 The intentional delivery, placing, discharging, detonating (or making a hoax associated with these activities), of an explosive or other lethal device in, into or against a place of public use, a state or government facility, a public transport facility, a public transportation system, or an infrastructure facility.

21.2 The intentional seizure, high-jacking, taking control, destroying or endangering the safety of a fixed platform.

21.3 The intentional seizure, detaining or taking of a hostage in order to compel any third party, including a state, intergovernmental organisation or a group of persons, to do or abstain from doing any act as an explicit or implicit condition for the release of the hostage.

21.4 The intentional murder, kidnap violent attack or other offence related to causing harm to an internationally protected person.

21.5 The intentional seizure or taking of control of an aircraft by force or threat.

21.6 The intentional seizure or taking of control of a ship by force or threat.

21.7 The harbouring, concealing, of a person or group of persons who intend to commit, or who has committed any of the offences listed above.

21.8 The financing of a person or group of persons to commit, or to facilitate the commission of any of the offences listed above.

21.9 The threatening, attempting to threaten, the conspiring with any other person or the inciting of another person to commit any of the offences listed above.

22. APPROVED AND SIGNED

Approved by	Simbarashe Mukonzo – Managing Director
Signature	
Date	July 2019
Next Review Date	July 2021