

RISK MANAGEMENT AND COMPLIANCE PROGRAM

**(in terms of Section 42 of the Financial Intelligence Centre Act No 38 of 2001 as
amended)**

VAN ZYL'S INC

&

VAN ZYLS ROOS INC

(hereinafter referred to as the Institutions)

Nov 2023

Version 1.2023



Contents

| | |
|--|----|
| 1. Overview..... | 3 |
| 2. Legal Framework..... | 4 |
| 3. Executive Statement of the Board of Directors | 4 |
| 4. The Legal Practise Act | 5 |
| 5. The Code of conduct for legal practitioners | 5 |
| 6. FIC Registration | 5 |
| 7. Appointment of MLCO and the MLRO | 6 |
| 8. The institution's' clients and its Approach to Risk (42b)..... | 7 |
| 9. Appointment of Employees | 9 |
| 10. Anonymous or Fictitious Clients..... | 10 |
| 11. Due Diligence Processes (42d – j)..... | 10 |
| 12. Determining whether a transaction or activity is reportable | 12 |
| 13. Proliferation Financing..... | 13 |
| 14. Activity based financial sanctions..... | 14 |
| 15. Terminating a Business Relationship..... | 14 |
| 16. Business Relationship with a client who is a Domestic Politically Exposed Person, Foreign Politically Exposed Person, or Prominent influential Person. | 14 |
| 17. How and where FICA records are to be kept | 15 |
| 18. Reportable Information..... | 15 |
| 19. Avoiding Transactions and Business Relationships with Persons and Entities identified by the United Nations Security Council..... | 16 |
| 20. Provision's that are not applicable to the institution's | 18 |
| 21. Responsibility for RMCP | 18 |
| 22. Disciplinary Action | 19 |
| 23. Review..... | 19 |
| Annexure 1: Money Laundering Compliance Officer Appointment Letter | 20 |
| Annexure 2: Client Due Diligence Questionnaire | 21 |
| Annexure 3: Enhanced Due Diligence Questionnaire (High Risk Clients only)..... | 23 |
| Annexure 4: Identification and Verification | 24 |
| Annexure 5: Public Finance Management Act..... | 26 |
| Annexure 6: Senior Management Approval Procedure | 28 |
| Annexure 7: Reporting Template | 29 |
| Annexure 8: Sanctions Screening Process | 30 |
| Annexure 9: Procedure for freezing property and transactions pursuant to the UNSCR's | 31 |
| Procedure for providing basic living expenses as contemplated in section 26C..... | 31 |
| Annexure 10: High Risk Jurisdiction | 32 |
| Annexure 11: Employee Money Laundering and Terrorist Financing Risk Questionnaire..... | 33 |
| Annexure 12: Key Definitions..... | 35 |




1. Overview

This programme forms part of the institution's internal business policies, processes and procedures. The institution's Directors and employees are required to familiarise themselves with the Risk Management and Compliance Program (RMCP) and undertake to comply with the stated processes and procedures.

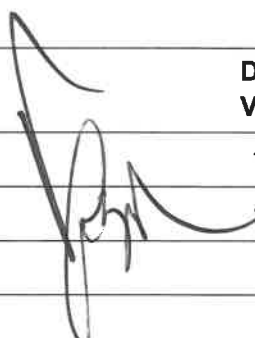

1.1. Document History

| Revision Date | Doc Version | Summary Changes | Author / Reviewer |
|---------------|-------------|-----------------|------------------------------------|
| July 2020 | 1 | Initial Policy | G Booysen |
| June 2022 | 1.2022 | Review | G Booysen |
| Nov 2023 | 1.2023 | Review | MLCO & MLRO assisted by G Booysen. |

1.2. Operational Approvals

| Name | Nature | Doc Version | Approval Signature | Date of Approval |
|----------------|--------|-------------|---|------------------|
| Francois Human | MLRO | 1.2023 |  | 05/12/2023 |

1.3. Governance Approvals

| Name | Nature | Doc Version | Approval Signature | Date of Approval |
|-------------|----------------|-------------|--|------------------|
| Mr. Roos | Director/ MLCO | 1.2023 |  | 05/12/2023 |
| Mr. Van Zyl | Director | 1.2023 |  | 05/12/2023 |

2. Legal Framework

- Financial Intelligence Centre Act ("FIC ") 38 of 2001 as amended (hereinafter referred to as "the Act")
- Prevention of Organised Crime Act ("POCA"), No. 121 of 1998
- Protection of Constitutional Democracy against terrorist and related activities ("POCDATARA"), No. 33 of 2004
- Public Compliance Communications ("PCC") issued by the FIC
- The Legal Practise Act 28 of 2014
- The code of conduct for legal practitioners

3. Executive Statement of the Board of Directors

It is the intention of the Board of Directors of the institution's to support the global fight against money laundering (ML), terrorist financing (TF) and proliferation financing activities (PF). The institution's has prioritised the implementation of anti-money laundering, counter terrorist and proliferation financing measures within the Company by adopting a Risk Management and Compliance programme (the "RMCP") for adequate prevention and control.

The Anti-Money Laundering Risk Management and Compliance programme (the "RMCP") summarizes the relevant risk areas, controls and compliance thereof, as applicable to the Company in respect of anti-money laundering and establishes the necessary procedures and guidelines to ensure full compliance with all applicable laws and regulations, including without limitation, the Financial Intelligence Centre Act.

The programme is designed to assist all employees of the institution's in adhering to policy and procedures, which, if followed diligently, will protect the institution's, its clients, its employees, facilities and activities from money laundering or other illegal activities.

The Board of Directors and Senior Managements commitment to this objective is set forth herein, which defines the risk management and compliance programme and includes procedures for the detection and reporting of activities possibly linked to money laundering or the financing of terrorist activities.

This risk management and compliance programme aims to:

- Identify;
- Assess;
- Monitor;
- Mitigate;
- Manage

any Money Laundering and terrorist financing risks that the institution's may encounter.

The legal profession is one of the non-financial sectors identified by the international anti-money laundering community as potentially highly vulnerable for money laundering, terrorist and proliferation financing (ML, TF and PF) because of services provided by the legal profession such as advising on and creating legal entities, including shell companies and trusts, property conveyancing services and the provision of client accounts.

It is for this reason that compliance with the Risk Management and Compliance Programme is integral to the institution's overall commitment to combat money laundering, terrorist financing and other crimes. The appropriate application of the RMCP requires that staff and senior management be familiar with its contents, related procedures, and norms that regulate these activities.

The following concepts and approach for the effective implementation of requirements has been introduced:

- A risk based, as opposed to "rules based" compliance management programme, based on the unique identified risks of the entity

- A range of risk-based customer due diligence ("CDD") and enhanced due diligence ("EDD") requirements when required, which are focused on understanding customers and getting to adequately "know your client" ("KYC") as opposed to simply identifying and verifying identities
- A risk-based KYC approach to ensure the efficient utilisation of resources and easier compliance for low-risk clients
- Risk management relating to relationships with Domestic Politically Exposed Persons (DPEP'S), Foreign Politically Exposed Persons (FPEP's) and Prominent Influential Persons (PIP's).
- The provision for the freezing of assets, in terms of targeted financial sanctions against persons identified by United Nations Security Council in terms of various sanctions regimes
- Procedures for the reporting of transactions where required and for co-operation with the Financial Intelligence Centre in respect of the provision of required information.
- Procedures to ensure robust record retention

The institution's is committed to the highest standards of anti-money laundering (AML) compliance and requires management and employees to adhere to these standards, and the contents of our internal policies and procedures, to prevent the use of our products and services for money laundering purposes, terrorist financing or other financial crime.

All management and staff of the institution's must therefore, at all times, comply with the institution's Risk Management and Compliance Program, which are subject to review by local regulators and/or independent external auditors, if such reviews are required by local law or regulations.

Failure to adhere to the requirements may result in disciplinary or other action as prescribed in the terms of employment and the possibility of criminal sanction.

A copy of this document shall be made available electronically to every employee and all applicable staff shall receive appropriate training.

On request from the Financial Intelligence Centre ('FIC') or a regulatory body, a copy of the document describing the Risk Management and Compliance Programme may be made available to the Financial Intelligence Centre and any other regulator.

4. The Legal Practise Act

Legal practitioners are required to act lawfully and ethically. Section 84(6) of the Legal Practice Act (the LPA) provides that the Legal Practice Council (the LPC) may withdraw a Fidelity Fund certificate and, where necessary, obtain an interdict against the legal practitioner concerned if he or she fails to comply with the provisions of this Act or in any way acts unlawfully or unethically.

5. The Code of conduct for legal practitioners

Paragraph 3.1 of the Code of Conduct requires that legal practitioners, candidate legal practitioners and juristic entities maintain the highest standards of honesty and integrity.

6. FIC Registration

6.1. FIC Registration

The MLCO will ensure that the institution's is registered as an "accountable institution" and will retain the following records pertaining to the registration process:

- The institution's "Org ID"
- The institution's particulars provided during the registration process
- The log-in particulars required to access the FIC's reporting portal ("goAML")
- The "Confirmation of Entity Registration" notification received from the FIC

The institution's must remain registered whilst operating as one of the businesses listed under Schedule 1 and/or Schedule 3 of FICA and any changes to the registration particulars of the business must be communicate to the MLCO. These changes must be submitted to the FIC within 15 days after such change.

The MLCO will update the institution's details via the FIC's website portal and will ensure that the updated information is validated within 5 business days of communicating any changes.

The MLCO will keep a record of his or her instructions to the FIC as well as any confirmation notifications received from the FIC.

7. Appointment of MLCO and the MLRO

To ensure effective money laundering and terrorist financing risk management, and in accordance with Section 42 and 43 of the Financial Intelligence Centre Act, a compliance function to assist in the discharge of compliance obligations shall be instituted, and an appropriate person or persons identified to assume responsibility for the implementation and management of this.

The Board of Directors shall assign a person with sufficient competence and seniority, at Board or senior management level, to ensure the effectiveness of the compliance function as the appointed money laundering control officer ("MLCO").

The MLCO shall be sufficiently senior, be free to act on own authority and to be informed of any relevant knowledge or suspicion of money laundering or terrorist financing identified in the business.

The MLCO shall be a person with a working knowledge of the FIC Act and its implementing regulations and a working understanding of the businesses product and service offerings. Such appointee shall have a working knowledge of applicable legislative requirements and its implementing regulations and shall be qualified by experience, knowledge and training. The MLCO shall remain skilled and up to date with any changes to the risk of the business, legislative risk or changes, or anything else which may impact the RMCP.

The Board and senior management must ensure that the MLCO has sufficient resources available to him, including appropriate staff and technology, in order to adequately fulfil his function. This should include arrangements to apply in his temporary absence.

A Money Laundering Reporting Officer (MLRO) will be appointed to assist the MLCO in carrying out his duties and will serve in his temporary absence.

The designated MLCO and MLRO is appointed in terms of a written authorisation by the Board, which template is attached as Annexure 1.

The MLCO and MLRO will constitute the internal compliance function and will notify the FIC of any change in this information within 15 days of such change, by means of the goAML online system.

The MLCO is vested with full responsibility and authority to enforce the risk management and compliance programme and is responsible for monitoring compliance with policy and procedures, including reporting to senior management on compliance and addressing any identified deficiencies. The MLCO must therefore ensure that appropriate monitoring processes and procedures across the business are established and maintained.

The MLCO will furthermore act as the "appropriate person" required to be appointed under Section 43 to receive and process internal and external reports.

The MLCO as well as any appointed Money Laundering Reported Officer (MLRO) is responsible for prompt reporting as and when required both to the Regulator and the Governing authority of on compliance matters as well as reportable instances. The MLCO must have reasonable access to information that will enable him to undertake his reporting responsibility. It is important therefore that the Money Laundering Control Officer as well as any Money Laundering Reporting Officer keep a written record of every matter reported to him, of whether or not the suggestion was negated or reported, and of reasons for any decision taken.

The annual review of FIC registration information will be conducted by the MLCO with assistance from the MLRO and will be completed annually with all necessary updates provided to the FIC within 15 business.

Irrespective of any delegation, the Board of Directors shall remain fully engaged in decision making processes and take ownership of the risk-based measures adopted, and remain accountable for the adequacy of the content and application of the Risk Management and Compliance Programme.

8. The institution's' clients and its Approach to Risk (42b)

The nature of the business is that of a person who is admitted by the High Court to practise and is authorised to be enrolled as a legal practitioner, conveyancer or notary in terms of section 24 of the Legal Practice Act, 2014 (Act 28 of 2014) and who is required to have a Fidelity Fund Certificate under section 84 of that Act.

The institution's has determined that at present it enters into single transactions and business relationships with all members of the public who wish to procure their services, their clients can be divided into the following categories:

- Conveyancing clients
- Commercial Law Services
- Debt Collection & Litigation
- Heirs of Deceased Estates

All Prospective Clients of the institution's will be subjected to the Customer Due Diligence (CDD) questionnaire attached as Annexure 2.

The institution's approach is to assess the risks involved in transacting with a client or potential client, as a part of their business activities and classifying them (low, medium, high risk) on the basis of the impact on the business. It enables the institutions to look for control measures that would help in curing or mitigating the impact of the risk and in some cases negating the risk altogether.

Risk Indicators

- The legal practitioner is located far away from the client and there is no logical or economic reason for this.
- The legal practitioner does not have the necessary experience or specialist knowledge that the client requires.
- The client is prepared to pay excessive amounts in fees and charges to the legal practitioner.
- The client has changed legal practitioners' numerous times within a short period.
- Another legal practitioner has refused to provide the services sought by the client.
- Instructions from the client to the legal practitioner are inconsistent with the size, experiences or services offered by the legal practitioner.
- There are significant differences between the declared price and the approximate actual values for immovable or movable property.
- Transactions involve large amounts of cash, inconsistent with the client profile.
- The client is represented by a third party without logical or economic explanation.
- The client makes cash payments into the legal practitioner's trust account.
- A third party pays for the client transaction with no apparent logical or economic reason.
- The transaction includes the transfer of funds to or from a foreign geographic area with no valid economical or logical reason.
- The transaction includes the transfer of funds to or from a foreign high-risk geographic area.
- The transaction involves crypto assets.
- The legal practitioner's expenditure is funded by a third-party entity or government entity.
- Payment is deferred to a later date, with no guarantee to pay later, with no logical or economic reason.
- The client requests to pay for the transaction over an excessive period (either an unusually short or long repayment period) which does not make logical or economic sense.

- The transaction involves the purchase of property with cash and soon thereafter the property is used as security for a loan.
- The client requests a change to the payment method or type with no logical or economic reason.
- The client is a recently incorporated company or established entity with large capital amounts which does not match the client's source of funds.
- The client receives excessive capital donations with no logical explanation.
- There is an excessively high or low price attached to the securities transferred regarding any circumstance indicating such an excess (e.g., volume of revenue, trade or business, premises, size, knowledge of declaration of systematic losses or gains) or regarding the sum declared in another operation.
- The transaction involves a foreign politically exposed person, a domestic politically exposed person, or a prominent influential person as beneficial owner of the client.
- Conducting business and employing staff numbers that are divergent from the industry norm.
- Conducting business with unexpected profile or abnormal business cycles or entering new/emerging markets.
- Providing incorrect or insufficient information to the attorney.

The institution's approach to AML and TF risk may be better explained by the FICA Risk Assessment attached as Annexure 11.

The following clients will be regarded as an inherent high-risk, and will be subjected to the enhanced due diligence process attached as Annexure 3.

- Persons on designated UN sanctions lists or Targeted Financial Sanctions list are a high risk of ML or TF.
- Conducting business with a DPEP, FPEP or PIP and those closely associated with or related to them. They are in influential positions and may have access to public funds, or funds from unknown sources.
- Those who want to conceal their identities
- The use of unusual source of funds to transact
- Clients cease their business relationships upon a request for customer due diligence (CDD) information.
- Obscuring the identity of beneficial owners or controlling interests through shelf or front companies or nominee shares or bearer shares.
- Enabling company formation and asset administration over different countries without any ostensible legal, tax, business, economic or other reason.
- Conducting business involving unusual and unexplained complexity in control or ownership structures without an economic purpose.
- Conducting business in unconventional circumstances considering full context.
- Conducting business using new technologies may have inherent weaknesses for exploitation by criminals.
- Operating as non-profit organisations engaging in transactions having no logical economic purpose or ostensible purpose with other parties and if the organisation makes donations to individuals or organisations outside of South Africa; or provides humanitarian, charitable, religious, educational, or cultural services outside South Africa.
- Acting on behalf of an undisclosed person.
- Entering transactions being affected mainly using virtual assets to preserve anonymity, without motivation.
- Offering unusually high levels of fees for services not warranting such a premium, except legitimate contingency fee arrangements.
- Applying for residency or citizenship in exchange for capital transfers, purchase of property or government bonds, or investment in corporate entities in that jurisdiction.
- Being suspected of being engaged in falsifying or misleading activities.
- Seeking advice for arrangements that have indicators of a tax evasion purpose.
- Transferring a company's seat to another jurisdiction without any genuine economic activity in that jurisdiction.
- Performing sudden and inexplicable activity from a previously dormant company.
- Wishing not to obtain necessary governmental approvals/filings.
- Facing criminal charges on white collar and/or unlawful income generating crimes.

The following transactions will be regarded as an inherent high-risk, and will be subjected to the enhanced due diligence process attached as Annexure 3.

- The Institutions being expected to act as a financial intermediary in a business transaction by receiving and transmitting funds through accounts under their control.
- Clients depositing funds in the Institutions' trust account which do not involve legal services rendered by the Institutions
- Clients requesting financial transactions to occur outside the Institutions' trust account, i.e.: through the Institutions' general, personal, or business account.
- Services involving the Institutions may represent or assure the client's reputation and credibility to third parties, without an appropriate knowledge of the client's affairs.
- Services facilitating the concealment of beneficial ownership from competent authorities.
- Services where the Institutions does not have expertise, unless where the matter is referred to a trained professional.
- Transfer of fixed property or other high value assets a time that is unusually short for similar transactions with no ostensible economic or other legitimate reason.
- Payments received from unfamiliar or unknown third parties and unconventional cash payments.
- Transactions involving inadequate consideration and without any legitimate reasons.
- Deceased estates involving persons who have been convicted of proceeds generating crimes.
- The use of shell companies without apparent legal, tax, business, economic or other legitimate reason.
- Legal arrangements that may lead to obscuring real ownership or economic purpose, including providing advice on a discretionary trust that empowers the trustee power to name a class of beneficiaries other than the real beneficiary.
- Settlement of default judgments or alternative dispute resolutions in unusual ways.
- Use of anonymous and/or unusual payment methods, virtual currency, and wealth transfer without a clear economic or other legitimate reason.
- Postponement of a payment for an asset or service to a distant date in circumstances where payment would ordinarily take place immediately, without appropriate assurances.
- Unexplained and unusual provisions in credit arrangements that do not reflect the commercial reality of parties.
- Transfers of unique or hard-to-value goods (e.g., precious stones, antiques, virtual assets) that are uncommon to the client, or beyond the attorney's normal course of business.
- Short and recurring capital or pecuniary contributions to the same entity with no apparent economic or other legitimate reason.
- Acquisitions of businesses in business rescue or liquidation with no apparent economic or other legitimate reason.
- Power of attorney given in unusual and for unclear or illogical reasons.
- Transactions involving closely connected persons with no rational explanations and no apparent economic or other legitimate reason.
- Commercial or conveyancing transactions to be carried out by the client with no apparent economic or other legitimate reason.
- Transactions not adequately accounted form, including incorrect invoicing of goods/services, falsely described goods/services, and multiple trading of goods/services.

9. Appointment of Employees

The institutions will screen prospective and current employees for competence and integrity periodically. This process will also include scrutinising employee information against the targeted financial sanctions and UN Sanctions lists.

Not all employees present the same level of ML/TF/PF risk. The institutions have therefore implemented an Employee Money Laundering and Terrorist Financing Risk Questionnaire attached as Annexure 11, that is completed by all prospective employees to ensure that the screening applied is proportionate to the level of ML/TF/PF risk the employee role presents and how this employee will be screened in future.

If a higher risk of ML/TF/PF is identified based upon the employee role, the institutions will screen such an employee on a more frequent basis. By following this risk based process they can mitigate and manage it's the employee's ML/TF/PF risk.

10. Anonymous or Fictitious Clients

The institutions are strictly prohibited from dealing with anonymous persons, or persons who have fictitious names.

The institution's must, by adhering to the provisions of this RMCP, ward against the risk of –

- dealing with an anonymous person by refusing to on-board as a client anybody who appears to desire or expresses a desire to transact with the institutions anonymously.
- dealing with a fictitiously named person by subjecting all Prospective Clients to the CDD procedures described in section 11, which procedures are aimed at ensuring, amongst other things, that the institution's only deals with persons who exist.

11. Due Diligence Processes (42d – j)

11.1. Identification and Verification of Clients

The institutions will, where applicable, obtain information on the:

- Source of funds of the client;
- Reasons for intended business relationship and the legal services;
- Required approvals provided by the governing board or senior management
- Controlling ownership interest, whether through controlling the management of a legal person or a hidden beneficial owner.

The due diligence questionnaire is attached as Annexure 2.

The institution's distinguishes between juristic entities and natural persons and the manner by which they will be identified and verified in terms of section 42(d) are attached as Annexure 4.

Beneficial Ownership:

The institution's realises that the concept of a beneficial owner is widely defined and would encompass a person having a controlling ownership interest would include a person(s) having the power to:

- Dispose of or control the legal entity's property;
- Amend or terminate the legal entity;
- Remove or add board members, shareholders or beneficiaries or to give another individual control over the legal entity;
- And veto specified decisions or resolutions.

The beneficial owner's identity must be established and verified by determining:

- the identity of each natural person who has a controlling ownership interest in the legal person.
- Where there is doubt as to whether the natural persons who have a controlling interest are the beneficial owners, as in the case of a warehousing agreement:
- the identity of each natural person who exercises control of that legal person through other means, such as a Trust, must be established and verified. A copy of the Memorandum of Incorporation can be checked to see whether warehousing is permitted
- Failing this, the identity of each natural person who exercises control over the management, including in his or her capacity as executive officer, non-executive director, independent non-executive director, director, or manager must be established and verified.

Verification is completed by means of the following processes:

The institution's verifies the identity of its clients by means of the following:

- On a face-to-face basis the identification document is collected, verified, and certified.
- Except for conveyancing clients, when face-to-face verification is not possible the third-party application Surge Works is used to verify the identity of said client by means of electronic photo verification that matches the client's data to various databases including those of the Department of Home Affairs.

11.2. Future Transactions with Clients

The institution's will conduct future transactions with its clients and any unusual transaction that is not consistent with our knowledge of a prospective client will be reported.

11.3. Additional due diligence in respect of Legal Persons

The additional due diligence measures conducted in terms of legal persons are described under Annexure 4.

11.4. Ongoing due diligence measures

Before receiving any value from an existing client after the implementation date, the Institutions must treat such existing client as if it were a prospective Client looking to enter into a Business Relationship with the Institutions and carry out the full range of CDD procedures in accordance with this RMCP.

The CDD procedures contemplated in this paragraph need only be conducted in respect of information and documents that the institution's does not already have its possession.

When policy amendments are requested the institution's will compare each transaction under a Business Relationship against the information provided by the Client in the CDD pertaining to the:

- nature of the Business Relationship; and
- the purpose of the Business Relationship; and
- the source of the funds that will finance the Business Relationship,
- and must update such information and any other documents originally forming part of the CDD in respect of that Client where necessary.

Whenever fulfilling the duty described above, the institution's must simultaneously consider whether the Transaction that necessitated the information update is reportable.

Monthly account monitoring is conducted by the finance person.

11.5. Complex or Unusual Transactions

The institutions will examine:

- complex or unusually large transactions; and
- unusual patterns of transactions which have no apparent business or lawful purpose

The Institutions will keep written findings of the above and if not resolved will report to the MLCO.

Factors to be considered:

The examination of the above transactions will depend on several factors, including:

- The nature of the legal services required and purpose.
- The legislation, regulatory requirements, and industry standards (or lack thereof) applicable to the transactions.

- The unusual and disproportionate amounts involved and disparate exchange of value.
- The sourcing of substantial funds from high-risk countries without any apparent linkage.
- The rendering of services or goods that are mismatched within the context.
- The use of multiple bank accounts without any apparent reason.
- Deposits of large sums of money without genuine business activities or acumen.
- Unusual payment instructions taking into consideration industry practices.
- Increase of assets or income in either local or foreign countries without plausible economic justification.
- Substantially large financial transactions for recently incorporated entities without any apparent economic reason.
- Substantially large financial transactions that are unsuitable for the prospective client's business profile or commercial status.

11.6. Doubts about the Accuracy of existing information

Where an employee has doubts about information that it previously obtained from an existing client, it must take reasonable steps to satisfy itself as to that information's accuracy or otherwise, and such reasonable steps may include (without limitation) –

- requesting from the Client an original document if a certified copy thereof was originally accepted; or
- requesting from the Client a copy that is certified more recently than the copy that was originally accepted; or
- requesting from the Client a document generated by a Governmental Authority or other independent person, where a document generated by the Client was originally accepted; or
- employing any other reasonable measure to satisfy itself as to the accuracy or otherwise of the information.

Should the measures list above –

- reveal the inaccuracy of any previously obtained information, then the affected information must be updated accordingly;
- provide no clarity regarding whether the information is accurate or not, then the MLCO of the Business must consider the importance of that information's correctness considering the institution's ML/TF risk. If, in the discretion of the MLCO, the correctness or incorrectness of the information sought has a material bearing on the ML/TF risk to which the institution's is potentially exposed, then the principles stated in section 9 shall apply, which principles must be adjusted as necessitated by the context.

12. Determining whether a transaction or activity is reportable

Subject to legal professional privilege, section 29 of the FIC Act requires any person who is employed by a business to report to the FIC suspicious and unusual transactions relating to the proceeds of unlawful activities connected to the affairs of such business.

Accordingly, a report may need to be made to the FIC where an employee knows or suspects (or ought reasonably to have known or suspected) that Institutions:

- has or is about to receive the proceeds of unlawful activities or property which is connected to an offence relating to the financing of terrorist and related activities; is party to a transaction that:
- facilitated or is likely to facilitate the transfer of the proceeds of unlawful activities or property which is connected to an offence relating to the financing of terrorist and related activities;
- has no business or lawful purpose;
- is constructed to avoid any reporting duty under the FIC Act; or
- may be relevant to the investigation of any evasion or attempted evasion of a duty to pay tax or any other duty or levy imposed by legislation administered by the Commissioner for the South African Revenue Service; or

- relates to the contravention of a prohibition under section 26B dealing with prohibitions relating to persons and entities identified by Security Council of the United Nations.
- has been or is about to be used for money laundering purposes or to facilitate the commission of an offence relating to the financing of terrorist and related activities;
- must, within the prescribed period after the knowledge was acquired or the suspicion arose, report to the FIC the grounds for the knowledge or suspicion and the prescribed particulars concerning the transaction or series of transactions.

In terms of section 1(2) of the FIC Act, a person has knowledge of a fact if:-

- the person has actual knowledge of that fact; or
- the court is satisfied that the person believes that there is a reasonable possibility of the existence of that fact; and the person fails to obtain information to confirm or refute the existence of that fact.

13. Proliferation Financing

The FATF specifically provides that an effective supervisory model in the proliferation financing context often involve several measures in the control and monitoring process, including, as far as the non-financial sector is concerned, the vulnerabilities associated with company formation, which is also applicable to lawyers.

The FAFT lists, amongst other, the following indicators of possible proliferation financing:

- A transaction that involves a person or entity in foreign country of proliferation concern;
- The client activity does not match the business profile, or the end-user information does not match the end-user's business profile;
- The transaction involves the shipment of goods incompatible with the technical level of the country to which it is being shipped;
- The transaction involves possible shell companies (e.g. companies do not have a high level of capitalisation or displays other shell company indicators);
- Transaction demonstrates links between representatives of companies exchanging goods i.e. same owners or management;
- The transaction involves persons or companies (particularly trading companies) located in countries with weak export control laws or weak enforcement of export control laws;
- The transaction involves shipment of goods inconsistent with normal geographic trade patterns; and
- The transaction involves financial institutions with known deficiencies in AML/CFT controls and/or domiciled in countries with weak export control laws or weak enforcement of export control laws.
- Cash payments as it enables anonymous transfer of funds, is easily transferable and leaves no audit trail. For these reasons cash payments to or from accounts of clients that pose a high risk from a PF perspective, is a red flag.
- False documentation or documentation that seems unusual could indicate an attempt to evade sanctions. Criminals often attempt to obscure the true nature of goods, destination of goods, beneficiary, the originator, intermediary or vessel etc. through false documentation.

The institutions will not consider the above risk categories in isolation. A holistic approach will accordingly be adopted to ensure a suitable risk assessment.

Where a client poses a higher PF risk, the institutions will conduct enhanced due diligence, and will obtain the following additional information:

- Information on the end use and end users of the controlled goods and activities; and
- Information of the authorisation of the end user, and intermediaries to the transaction.

14. Activity based financial sanctions

Activity-based sanctions include but are not limited to:

- Restrictions of activity;
- Travel restrictions;
- Trade restrictions; and
- Income prohibitions.

The institutions will not provide financial services, resources, and assistance to any designated sanctioned person or entity either directly or indirectly.

Where there is a suspicion of possible non-compliance with activity-based financial sanctions, the institutions will file a suspicious and unusual transaction report to the FIC in terms of section 29 of the FICA.

15. Terminating a Business Relationship

The MLCO and in its absence the MLRO must terminate a Business Relationship with a Client in respect of whom a CDD or ongoing CDD cannot be conducted.

An Employee who is unable to conduct the CDD or ongoing CDD must, immediately upon realising his or her inability, inform the MLCO in writing of –

- the Client involved; and
- the reason(s) for which the Employee is unable to conduct the CDD or ongoing CDD.

If the MLCO or MLRO agrees with the assessment of the Employee, then the MLCO or MLRO must advise the Client involved that –

- the institution's is terminating the Business Relationship; and
- the reason for the termination is the institution's inability to conduct a CDD in accordance with FICA and the RMCP (providing the underlying reason(s) for that inability); and not terminating the Business Relationship in these circumstances would be a serious breach of the institution's' legal duties, and shall, where practically possible, so advise the Client in writing.
- The MLCO will report such instances to the FIC in terms of Sec 29.

16. Business Relationship with a client who is a Domestic Politically Exposed Person, Foreign Politically Exposed Person, or Prominent influential Person.

The institutions must determine whether a Client is a DPEP, FPEP or PIP, by asking the Client such in the due diligence questionnaire. Where applicable, conduct an online search to determine whether a prospective client is a DPEP, FPEP or PIP.

The institutions will, before obtaining approval by senior management, attempt to establish the source of wealth and source of funds of the client, which the client may confirm. The Institutions should have an understanding of the client's wealth profile, e.g.: shares, sale of assets, inheritance and sources of income, including employment income, directors' fees, offshore accounts, etc.

The DPEP, FPEP or PIP that may procure the institution's for their services are found in the Key Definitions Annexure 12 and the Public Management Finance Act Annexure 5.

If the Client is a high-risk DPEP or PIP looking to establish a Business Relationship, then, in addition to the prescribed CDD procedures, the Employee must:

- only on-board the Client with the approval of Senior Management attached as Annexure 6;
- establish (without having to verify) the Client's source of wealth; and
- monitor the Business Relationship more closely that it would monitor any other Business Relationship.
- An enhanced due diligence should always be conducted for FPEP's.

The Enhanced Due Diligence Template is attached as Annexure 3.

17. How and where FICA records are to be kept

In respect of each Client, the Business must keep CDD records that reflect the following information:

- the name of the Client; and
- the means through which the Client's name was established; and
- the documents by which the Client's name was verified; and
- the Employee who established and verified the Client's name.

In respect of each transaction, whether in the context of a Single Transaction or Business Relationship, the Employee must keep records of the:

- amount and currency involved; and
- date; and
- parties involved; and
- nature of the Transaction
- any reports made in terms of the FIC Act; and
- underlying business correspondence.

These records will be stored as follows:

- Metro file office: Old Mutual Roseville Park, Cnr. DF Malan Drive and Moot Streets, Pretoria, Cnr. DF Malan Drive and Moot Streets, Pretoria, 008
- On the server of the institution's office in Pretoria that includes a cloud back-up facility.

The MLCO must ensure that all records kept in terms of this RMCP are stored for at least 7 (seven) years following the conclusion of a single Transaction or the termination of a Business Relationship, in such a manner that :

- they are readily retrievable should they be requested by the FIC, or any other person legally entitled to them; and they are protected, through physical and other controls, against unauthorised access thereto; and back-up records / copies of the records are stored separately from the original records.

18. Reportable Information

An Employee must immediately provide a written report to the MLCO if the employee knows or reasonably suspects that –

- the Institutions received, or is about to receive the proceeds of crime, or property associated with the financing of Terrorist Activities; or
- either of the Institutions are party to one or more transactions that –
 - facilitated, or will likely facilitate, the transfer of the proceeds of crime, or property associated with the financing of Terrorist Activities; or
 - are complex or involve abnormally large amounts of money, are not business-like, or do not appear to serve any legal purpose; or
 - were affected so as not to trigger a reporting duty on the institution's part; or
 - may pertain to an investigation into actual or attempted tax evasion; or
 - are associated with the financing of Terrorist Activities; or
 - the institutions have been, or is about to be, used for ML/TF/PF in any manner whatsoever.
 - there has been a transaction of the Institutions involving the payment of R50 000.00 (twenty-five thousand rand) or more in Cash, which payment is made to or received from a client, or the Client's Representative or Principal.

An employee must immediately provide the MLCO with a report if the employee knows or suspects an unsuccessful attempt to do anything that, if done successfully, would have resulted in any of the consequences contemplated in paragraph above.

An employee must immediately provide the MLCO with a report if the employee knows (as opposed to merely suspects) that the institution's is in possession or control of property associated with any person or entity listed on UN Sanctions list, or any person or entity involved in Terrorist Activities.

The report template is attached as Annexure 7.

The MLCO receiving a report from an Employee must, in turn, report to the FIC, on the FIC's electronic reporting platform to be found on its website www.fic.gov.za:

- within 5 (five) business days for a report made by an Employee about any property associated with terrorism; and
- within 15 (fifteen) business days for a report made by an Employee about any suspicious or unusual transactions or activities; and
- within 3 (three) business days for a report made by an Employee about Cash Threshold payments.

An Employee reporting to the MLCO, and the MLCO reporting to the FIC in terms of this section may not alert the subject of the report ("Tipping off"), whether directly or indirectly as to the fact that a report is about to or has been made to the MLCO or to the FIC (as the case may be), nor as to the content of the report.

With the exception of a report about property, the institution's may, even after making any report in terms of this paragraph, continue with or give effect to the matter in question giving rise to that report, unless the FIC instructs the institution's otherwise in writing.

19. Avoiding Transactions and Business Relationships with Persons and Entities identified by the United Nations Security Council

The institution's will avoid all transactions where it is suspected that the transaction will or may facilitate the acquisition, collection, use or provision of property or any other economic support, for the benefit of, or at the direction of, or under the control of a person or an entity identified pursuant to a resolution of the Security Council of the United Nations or the Targeted Financial Sanctions.

The institution's will take reasonable measures to establish whether a prospective client, or an existing client is indicated on the Targeted Financial Sanctions and the UN Security Council Sanction List.

Employees responsible for interacting with clients and/or maintaining client and transaction information will screen high risk clients against the Targeted Financial Sanctions and the UN Security Council Sanction list in the following situations:

- When entering a single transaction
- When establishing a new business relationship with, or
- When performing ongoing due diligence procedures on existing clients.

19.1. Sanctions screening procedure

The institution's Sanctions screening will be completed via the FIC TFS online tool and the UN1267 list as updated from time to time and all results saved (the OFAC search tool will be utilized if and when we receive confirmation from the service provider). If a positive match is made, the transaction will be paused, and a written report provided to the MLCO.

The procedure to access and screen against the UN Security Council Sanction list and the FIC TFS Online tool is DESCRIBED under Annexure 8.

If at any stage during the employee's interactions with a client or a client representative, the Employee suspects that a client is listed on the Sanction lists mentioned above; the employee will report this suspicion to the MLCO.

The MLCO will investigate all such reports and consider submitting a Suspicious or Unusual Transaction Report, a Terrorist Financing Activity Report or a Terrorist Financing Transaction Report to the FIC.

19.2. Procedure to freeze property and transactions pursuant to the UNSCRs.

When filing a report with the Centre in terms of section 28A of the FIC Act it is an offence (by virtue of section 4 of the POCDATARA Act) to continue dealing with that property in any way, whereas if a person files a report with the Centre in terms of section 29 of the FIC Act they may elect to continue with the transaction as provided for in section 33 of the FIC Act. The defence contained in section 17(6)(b) of the POCDATARA Act can be applied.

The procedure for freezing property and transactions pursuant to the UNSCR's is indicated under Annexure 9.

Procedure to give effect to the Minister of Finance's decision to provide for basic living expenses as contemplated in section 26C of the FIC Act

"(1) The Minister may, in writing and on the conditions as he or she considers appropriate and in accordance with a resolution of the Security Council of the United Nations contemplated in a notice referred to in section 26A (1), permit a person to conduct financial services or deal with property referred to in section 26B in the circumstances referred to in subsection (2)."

The procedure for providing basic living expenses as contemplated in section 26C is indicated under Annexure 9.

19.3. Submitting Suspicious or Unusual Transaction Reports within the Prescribed Time Limit

Any person who knows or ought reasonably to have known or suspected that:

- The institutions have received, or is about to receive, or if a transaction was concluded, may have received, the proceeds of unlawful activities or property which is connected to an offence relating to the financing of terrorist and related activities, or
- a transaction or series of transaction to which the institution's is a party:
 - facilitated or is likely to facilitate, or if the transaction was concluded, may have facilitated, the transfer of the proceeds of unlawful activities or property which is connected to an offence relating to the financing of terrorist and related activities, or
 - has no apparent business or lawful purpose, or
 - is conducted for the purpose of avoiding giving rise to a reporting duty under FICA, or
 - may be relevant to the investigation of an evasion or attempted evasion of a duty to pay any tax, duty or levy imposed by legislations administered by the South African Revenue Services, or
 - relates to an offence relating to the financing of terrorist and related activities, or
 - will or may facilitate the acquisition, collection, use or provision of property or any other economic support, for the benefit of, or at the direction of, or under the control of a person or an entity identified pursuant to a resolution of the Security Council of the United Nations.
 - the institutions has been used or is about to be used, or if the transaction was concluded, may have been used, in any way for money laundering purposes or to facilitate the commission of an offence relating to the financing of terrorist and related activities, must within the prescribed period after the knowledge was acquired or the suspicion arose, report to the FIC the grounds for the knowledge or suspicion.

Where an employee suspects that the institution's has been used or is about to be used, for money laundering or terrorist financing purposes, he or she will notify the MLCO of this transaction in writing within one business day of such a transaction.

The employee may not disclose his or her suspicion, or any information regarding the contents of any such notification to any other person, including the person in respect of whom the report is or must be made.

The MLCO will submit a Suspicious or Unusual Transaction Report to the FIC as soon as possible but not later than fifteen days after the employee became aware of a fact concerning a transaction on the basis of which knowledge or a suspicion concerning the transaction must be reported.

The MLCO will keep a record of all reports submitted to the FIC.

The MLCO will also keep a record of all transactions and activities which gave rise to the submittal of a suspicious and unusual transaction report, for at least five years from the date on which the report was submitted to the FIC.

19.4. Submitting Terrorist Property Reports within the Prescribed Time Limit

Where the institutions have in its possession or under its control:

- property associated with terrorist and related activities, or
- property owned or controlled by or on behalf of, or at the direction of a specific person or entity identified:
- by a notice issued by the President under Section 25 of POCDATARA, or
- pursuant to a resolution of the Security Council of the United Nations, the institution's will within the prescribed period report that fact to the FIC.

Where an employee has knowledge that any of the institution's has in its possession or under its control property associated with terrorist or related activities, he or she will notify the MLCO within one business day after he or she has established this fact.

The MLCO will submit a Terrorist Property Report to the FIC as soon as possible but not later than five days after the employee established that the institutions have property associated with terrorist and related activities in its possession or under its control.

The MLCO will keep a record of all reports submitted to the FIC.

19.5. Ensuring Compliance where Transaction or Due Diligence Records are maintained by a Third Party

Where the institution's has outsourced the recordkeeping requirements to a third party, it will ensure that:

- the institution's has free and easy access to the records,
- the records are readily available to the FIC or any other relevant supervisory body, and
- it provides the FIC with the prescribed particulars concerning the third party.

The MLCO will without delay provide the FIC with the third party's:

- Full name, if the third party is a natural person, or registered name, if the third party is a close corporation or a company
- The full name and contact particulars of the individual who exercises control over access to the records
- The address where the records are kept
- The address where the third-party exercises control over the records
- The full names and contact particulars of the individual who liaises with the third party on behalf of the institutions.

20. Provision's that are not applicable to the institution's

All provisions of section 42 of the Financial Intelligence Amendment Act apply to this institutions.

21. Responsibility for RMCP

It is the responsibility of the Board of Directors with assistance from the MLCO:

- to see to it that all Employees are properly sensitised, through appropriate training and instructional material, to their FICA duties in general, and to their duties under this RMCP in particular; and
- to publish this RMCP in such a manner that all Employees are alerted as to its existence, and can access it freely and with ease; and
- to use the UN Sanctions and FIC'S TFS Screening Tool (as updated from time to time) to screen all Prospective Clients before they are on-boarded; and
- to see to the effective implementation of this RMCP.

The institution's will provide ongoing training to its employees to enable them to comply with the provisions of FICA and the RMCP.

22. Disciplinary Action

Where a FICA related complaint or an investigation related to an infringement of FICA or the institution's' RMCP has been finalised, the institution's may recommend any appropriate administrative, legal and/or disciplinary action to be taken against any employee reasonably suspected of being implicated in noncompliance.

In the case of ignorance or minor negligence, the institution's will undertake to provide further FICA training to the employee.

Any gross negligence or the wilful non-compliance will be considered a serious form of misconduct for which the institution's may summarily dismiss the employee. Disciplinary procedures will commence where there is sufficient evidence to support an employee's gross negligence.

Examples of immediate actions that may be taken subsequent to an investigation include:

- A recommendation to commence with disciplinary action.
- A referral to appropriate law enforcement agencies for criminal investigation.
- Recovery of funds and assets in order to limit any prejudice or damages caused.

Examples of noncompliance or misconduct include:

- Failure to identify and verify
- Failure to comply with duty in regards to customer due diligence
- Failure to keep records
- Failure to conduct sanction screening

23. Review

This programme shall be reviewed annually or when required to ensure that it meets legal requirements and reflects best practice.

Handwritten signature and initials in the bottom right corner of the page.

Annexure 1: Money Laundering Compliance Officer Appointment Letter

MONEY LAUNDERING OFFICER APPOINTMENT LETTER

The following person is herewith appointed as the institution's Money Laundering Compliance Officer (MLCO) with immediate effect.

PETRUS JACOBUS ROOS

Name & Surname

VAN ZYL'S INC & VAN ZYLS & ROOS INC

Organisation

In making this appointment on behalf of the institution's, I understand that the MLCO will require the support of the institution's governing body in performing his or her responsibilities as provided for hereunder.

This appointment may at any time be withdrawn or amended in writing.

PETRUS JACOBUS ROOS

Name & Surname

Signature

05/12/2023

Date

You are entrusted with the following responsibilities:

- Keeping up to date with the requirements of FICA and Regulations and Guidance Notes issued by the FIC
- Establish and managing the institution's compliance function pursuant to the requirements of FICA
- Assisting the institution's governing body with its annual review of the RMCP
- Ensuring that the institution's is registered with the FIC and keeping a record of the institution's "goAML" log in particulars
- Monitoring of changes to the institution's contact particulars and communicating such changes to the FIC
- Periodic updating of UN Security Council Sanction List
- Monitoring compliance with the submittal and continued record keeping of all cash threshold, suspicious or unusual transaction and terrorist activity or property reports.
- Monitoring compliance with the retention and back-ups of all FICA Transaction Records and Client Due Diligence Records
- Ensuring that employees undergo annual FICA Training
- Ongoing Due Diligence and Monitoring of Existing Business Relationships
- Client random spot checks: UN Security Council List, False or Fictitious verification, DPEP's, FPEP's and PIP's and if applicable family or associate them.
- Monitoring Compliance with Additional Information on a New Business Relationship

In accepting this appointment, I understand that I must fulfil my responsibilities as the institution's MLCO.

I hereby accept the appointment as MLCO.

Signature

05/12/2023

Date

Annexure 2: Client Due Diligence Questionnaire

SECTION A: CLIENT DUE DILIGENCE QUESTIONNAIRE

If you are transacting on behalf of another person, we are required to establish and verify the identity of that other person as well as your authority to establish the business relationship or to conclude the transaction on behalf of that other person.

Details of person on whose behalf you are transacting:
(please complete this form for the Entity as well as for each natural person who is a Shareholder / Director / Member / Beneficiary and Trustee of Trust/ Partner/ Other of such entity)

CLIENT NAME _____

ADDRESS: _____

WORK TEL: _____ CELL: _____

OCCUPATION: _____

| RISK PROFILER | | | |
|---|---|---|--|
| | LOW | MEDIUM | HIGH |
| Source of Funds | Salary in bank account Savings with a financial institution, Pay contribution out of retirement funds | Other existing financial product or inheritances or sale of property | Third party payments, gambling winnings or undisclosed sources |
| Type of Services | Conveyancing Debt Collection Administration of Deceased Estates | Commercial Law Services Litigation | DPIP's FPPO's Clients on the Sanctions lists |
| Transaction value | Under R100 000 | Between R100 000 and R500 000 | Over R 500 000 |
| Onboarding | Face-to-face | Non-face-to-face | Contact through agent, third party, electronic or telephonic communication only |
| Client risk (by occupation or business) | Salaried person Natural Persons Small business | Client is consultant or earns commission Medium-sized business not in red zone | Client conducts own high risk or high cash or cross border business or occupation Client business unusual or complex structure Client does business with government, SOE's or municipalities |

| | | | |
|---|---|---|---|
| Client risk (geographical) | Client based in same city SA Citizen | Client based in same country Client based offshore (living and/or working) | Non-resident Countries involved in internal conflict, war or known as tax havens |
| Client risk (affluence) | Client has assets less than R5 million | Client assets between R5 million and R15 million | High net asset clients (over R15 million) |
| Is the Client a DPEP, FPEP, PIP or close family member or closely associated with a DPEP, FPEP or DPIP? (Annexure 5) | Not a DPEP, FPEP or PIP | | Client is a DPEP, FPEP, PIP or close family member or closely associated with a DPEP, FPEP or PIP. |

| FICA RISK ANALYSER | | L | M | H |
|---------------------------|--|----------|----------|----------|
| 1 | Source of funds | | | |
| 2 | Type of Services | | | |
| 3 | Transaction value | | | |
| 4 | Onboarding | | | |
| 5 | Client occupation or business | | | |
| 6 | Client Geographical location (local / foreign) | | | |
| 7 | Client Affluence | | | |
| 8 | DPEP, FPEP or PIP? | | | |

| RISK TABLE INDICATORS | RISK RATING |
|--------------------------------------|--------------------|
| NO RED INDICATORS | LOW |
| MAXIMUM 2 RED INDICATORS | MEDIUM |
| 3 OR MORE RED RISK INDICATORS | HIGH |

Is the client subject to enhanced due diligence: YES NO

If "YES", please complete Annexure 3.

Signed at: _____ (place) this _____ day of _____ 20__

SIGNATURE: _____ (who warrants my authority hereto)

Annexure 3: Enhanced Due Diligence Questionnaire (High Risk Clients only)

Is the client an existing client and known to you personally? If yes what is the duration of client relationship with the institution's: YES NO

Is the client on the United Nations or Targeted Financial Sanctions lists? YES NO

Jurisdiction of client? YES NO
If foreign national, is it a high-risk jurisdiction? YES NO (list of high-risk jurisdictions attached as Annexure 10)

Is this a once off transaction? YES NO

Could this type of transaction be used for the purposes of ML, TF, or tax evasion or is it suspicious or unusual? YES NO

Conclusion

Taken into consideration all the information collected on above mentioned client, do you find this client a high risk? YES NO

Motivation:

Signed at: _____ (place) this _____ day of _____ 20____

SIGNATURE: _____ (who warrants my authority hereto)

A handwritten signature in dark ink, consisting of a large, stylized 'M' or 'W' shape with a long, sweeping tail that curves upwards and to the right.

Annexure 4: Identification and Verification

BASIC IDENTIFICATION REQUIREMENTS:

NATURAL PERSON

- Full names, through identity document, driver's license or passport
- Home address, through documentary proof of residence
- Telephone/cellular phone number
- Occupation; and
- Business address, if applicable.

Prospective client acting on behalf of another person, establish and verify the client's details, as per above criteria (for individuals) and the below for the entity, together with:

- Documentary proof of authority, e.g.: power of attorney, board resolution, court order or letter of authority.

Additional due diligence required in respect of Legal Persons:

COMPANY, CORPORATIONS, CO- OPERATIVES, PARTNERSHIPS, TRUSTS, ASSOCIATIONS ETC.

Complete Section A of the CDD questionnaire for each natural person who is a shareholder.

Where a shareholder, member or beneficiary is not a natural person (such as a Company or Trust), the natural person beneficiaries of the juristic entity must be identified and Section A must be completed for each such person.

Where the shareholders cannot be identified, this needs to be noted, and the controlling person/s (executive management) need to be identified and Section A completed for each such person.

DOCUMENTS REQUIRED:

- legal name – documentation: registration certificate, letters of authority, partnership agreement, memorandum of incorporation, trust deed, letterhead, business invoice, proof of residence,
- registered address – documentation: where applicable, notice of change of address
- telephone number;
- registration certificate, letters of authority, NPO certificate, etc.; and
- proof of physical address for the entity; and
- the name, position and contact information of the individual giving you instructions on behalf of the organisation.
- The identity of every director, member, partner, trustee, beneficiary or person who exercises executive control.

ORGANS OF STATE INCLUDING GOVERNMENT DEPARTMENTS

Certain organs of state are incorporated as companies and registered with the Registrar of Companies to conduct business and must be identified as companies. In other instances, Government institutions are constituted as legal persons by statute.

Sound business practice indicates that organs of state that are neither incorporated as companies nor constituted as legal persons by a statute should be dealt with in a manner similar to that used in respect of "other legal persons". This would apply to national, provincial and local government departments; however, it is important to ensure that the requirements for identifying prominent or influential local persons is implemented.

Means to obtain further information:

The Institutions will ordinarily obtain information to determine whether:

- any conflicting interests exist; and
- the institutions are equipped to render the requested services.

The institutions will, where applicable, review the following:

- Documentary information pertaining to shareholding: memorandum of incorporation; share holders' agreement; trust deed; constitution; share certificates; minutes of shareholders' meetings;
- Annual reports, integrated reports, annual financial statements;
- Data publicly available from a public database relating to the potential client, including: the CIPC, Masters' office, Department of Social Development (NPOs) and websites

Handwritten signature and scribbles in the bottom right corner of the page.

Annexure 5: Public Finance Management Act

PLEASE NOTE: Users of this Programme must consult the most recent version of the Public Finance Management Act to obtain the most recent version of the Schedules.

Schedule Two

This includes the following entities and any subsidiary or entity under the ownership control of the following entities:

Air Traffic and Navigation Services Company, Airports Company, Alexkor Limited, Armaments Corporation of South Africa, Broadband Infraco (Proprietary) Limited, Broadband Infraco Limited, CEF (Pty) Ltd, DENEL, Development Bank of Southern Africa, ESKOM, Independent Development Trust, Industrial Development Corporation of South Africa Limited, Land and Agricultural Bank of South Africa, SA Broadcasting Corporation Limited, South African Express (Proprietary) Limited, SA Forestry Company Limited, SA Nuclear Energy Corporation, SA Post Office Limited, South African Airways Limited, Telkom SA Limited, TransCaledon Tunnel Authority, Transnet Limited

Schedule Three

This includes the following entities and any subsidiary or entity under the ownership control of the following entities:

Accounting Standards Board, Africa Institute of South Africa, Pretoria, African Renaissance and International Cooperation Fund, Afrikaanse Taalmuseum, Agricultural Research Council, AGRISSETA, Artscape, Banking Sector Education and Training Authority, Boxing South Africa, Brand SA, BreedeGouritz Catchment Management Agency, Castle Control Board, Chemical Industries Education and Training Authority, Commission for Conciliation, Mediation & Arbitration, Community Schemes Ombud Service, Companies and Intellectual Property Commission, Companies Tribunal, Competition Commission, Construction Education and Training Authority, Construction Industry Development Board, Council for Built Environment (CBE), Council for Geoscience, Council for Medical Schemes, Council on Higher Education, CrossBorder Road Transport Agency, Culture, Arts, Tourism, Hospitality and Sports Education and Training Authority (CATHSSETA), Education, Training and Development Practices SETA (ETDP), Electricity Distribution Industry Holdings (Pty) Ltd, Electronic Communications Security (Pty) Ltd, Energy and Water Sector Education and Training Authority (EWSETA), Fibre Processing Manufacturing Sector Education and Training Authority (FPMSETA), Film and Publication Board, Financial and Accounting Services SETA (FASSET), Financial Intelligence Centre, Food and Beverages Manufacturing Industry (FOODBEV), Freedom Park Trust, Health and Welfare Sector Education and Training Authority, Housing Development Agency, Human Sciences Research Council, Independent Regulatory Board for Auditors, Information Systems, Electronics and Telecommunications Technologies Training Authority, Ingonyama Trust Board, Catchment Management Agency, Insurance Sector Education and Training Authority, International Trade Administration Commission, iSimangaliso Wetland Park, Iziko Museums of South Africa, KwaZuluNatal Museum, Legal Aid South Africa, Local Government Education and Training Authority (LGSETA), Manufacturing, Engineering and Related Services Education and Training Authority, Marine Living Resources Fund, Market Theatre Foundation, Media Development and Diversity Agency, Media, Information and Communication Technologies Sector Education and Training Authority (MICTS), Mine Health & Safety Council, Mining Qualifications Authority, Municipal Infrastructure Investment Unit, National Agricultural Marketing Council, National Arts Council, National Consumer Commission, National Consumer Tribunal, National Credit Regulator, National Development Agency, National Economic, Development and Labour Council, National Electronic Media Institute of SA, National Empowerment Fund, National Energy Regulator of South Africa, National Film and Video Foundation, National Gambling Board of SA, National Health Laboratory Service, National Heritage Council (NHC), National Home Builders Registration Council—NHBRC, National Housing Finance Corporation, National Library, Pretoria/Cape Town, National Lotteries Commission, National Metrology Institute of South Africa, National Museum, Bloemfontein, National Nuclear Regulator, National Regulator for Compulsory Specifications, National Research Foundation, National Student Financial Aid Scheme, National Urban Reconstruction and Housing Agency, National Youth Development Agency, Nelson Mandela Museum, Umtata, Office of Health Standards Compliance, Office of the Ombudsman for Financial Services Providers, Office of the Pension Funds Adjudicator, Performing Arts Council of the Free State, Perishable Products Export Control Board, Private Security Industry Regulatory Authority, Productivity SA, Public Service Sector Education and Training Authority (PSETA), Quality Council for Trades and Occupations (QCTO), Railway Safety Regulator, Road Accident Fund, Road Traffic Infringement Agency (RTIA), Road Traffic Management Corporation, Robben Island Museum, Cape Town, Rural Housing Loan Fund, Safety and Security Sector Education and Training Authority (SASSETA), SA Civil Aviation Authority, SA Council for Educators, South African Diamond and

Precious Metals Regulator, SA Heritage Resources Agency, SA Library for the Blind, SA Local Government Association,

SA Maritime Safety Authority, SA Medical Research Council, SA National Accreditation System, South African Health Products Regulatory Authority (SAHPRA), South African National Biodiversity Institute (SANBI), South African National Energy Development Institute (SANEDI), South African National Parks, SA National Roads Agency, South African National Space Agency, SA Qualifications Authority, SA Revenue Service, South African Social Security Agency, SA Tourism Board, South African Weather Service, Servcon, Small Enterprise Development Agency (SEDA), Special Investigation Unit, State Information Technology Agency, State Theatre, Pretoria, The Cooperative Banks Development Agency, The National English Literary Museum, Grahamstown, The National Radioactive Waste Disposal Institute (NRWDI), The National Skills Fund (NSF), The Playhouse Company, Durban, The Social Housing Regulatory Authority (SHRA), Thubelisha Homes, Tourism and Hospitality Education and Training Authority, Transport Education and Training Authority, uMalusi Council for Quality Assurance in General and Further Education and Training, Unemployment Insurance Fund, Universal Service and Access Agency of South Africa, Universal Service and Access Fund, Urban Transport Fund, War Museum of the Boer Republics, Bloemfontein, Water Research Commission, Wholesale and Retail Sector Education and Training Authority, William Humphreys Art Gallery,

Part B: National Government Business Enterprises

Amatola Water Board, Aventura, Bloem Water, Council for Scientific and Industrial Research (CSIR), Export Credit Insurance Corporation of South Africa Limited, Inala Farms (Pty) Ltd, Lepelle Northern Water, Magalies Water, Mhlathuze Water, Mintek, Ncera Farms (Pty) Ltd, Onderstepoort Biological Products, Overberg Water, Passenger Rail Agency of South Africa, Public Investment Corporation Limited, Rand Water, SA Bureau of Standards (SABS), Sasria Limited, Sedibeng Water, Sentech, State Diamond Trader, Umgeni Water

Part C: Provincial Public Entities – as listed under the Schedule.

Part D: Provincial Government Business Enterprises – as listed under the Schedule.

Annexure 6: Senior Management Approval Procedure

| Where client has been identified as a Domestic Prominent Influential Person or Foreign Prominent Influential Person | | | | |
|---|-------------|----------|------------------|------------------------|
| Order of Approval | Name | Capacity | Telephone Number | Email Address |
| 1 st Contact | Mr. Roos | MLCO | +27 12 667 5111 | pieter@vzylinc.co.za |
| 2 nd Alternative | Mr. Human | MLRO | +27 12 667 5111 | francois@vzylinc.co.za |
| 3 rd Alternative | Mr. Van Zyl | Director | +27 12 667 5111 | @vzylinc.co.za |

Approval obtained, must be in written form.

Annexure 7: Reporting Template

REPORTING FORM

Full circumstances that gave rise to the submission of the report to be attached to this form.

DATE OF REPORT: ____/____/____

DATE ACTIVITY/ TRANSACTION/S DISCOVERED: ____/____/____

NAME OF PERSON REPORTING: _____


TYPE OF REPORT: CTR CTRA STR SAR TFAR TFTR TPR

EMAIL: _____ CELL: _____

RECEIVED BY: _____ DATE: ____/____/____

FIC REPORTABLE: YES DATE: ____/____/____ NO (reasons)

SIGNATURE: _____



Annexure 8: Sanctions Screening Process

In order for the institution's to determine if they are dealing with an undesirable person, they are required to "screen" their client(s) against these lists. The process is as follows:

Conveyancing

- The conveyancing department will receive all new applications for processing.
- Sanctions screening is then completed via the FIC TFS online tool and the UN1267 list as updated from time to time and all results saved (the OFAC search tool will be utilized when we receive confirmation from the service provider).
- A snip is taken of the search results and if there are no matches, the results are saved in the client folder.
- Should a client's name match against any of these lists, then the conveyancing department would be required to ensure that this is in fact an exact match. The conveyancing department would need to make use of the information available to them, and conduct further research if so required, to make this determination.
- If after further investigation there is still a positive match, the transaction must be placed on hold and all relevant documentation sent to the MLCO or MLRO.
- If the MLCO or MLRO agrees with the findings of the conveyancing department, they will make a report the FIC.

Litigation & Deceased Estates

- The litigation department will receive a case for processing
- Sanctions screening of the client is then completed via the FIC TFS online tool and the UN1267 list as updated from time to time and all results saved (the OFAC search tool will be utilized when we receive confirmation from the service provider).
- A snip is taken of the search result and if there are no matches, the result is saved in the client folder.
- Should a client's name match against any of these lists, then the litigation department would be required to ensure that this is in fact an exact match. The litigation department would need to make use of the information available to them, and conduct further research if so required, to make this determination.
- If after further investigation there is still a positive match, the transaction must be placed on hold and all relevant documentation sent to the MLCO and MLRO.
- If the MLCO and MLRO agrees with the findings of the litigation department, they will make a report to the FIC.
- The Procedure for freezing property and transactions pursuant to the UNSCR's follows in Annexure 9.

Annexure 9: Procedure for freezing property and transactions pursuant to the UNSCR's

Once the institutions have determined that it controls relevant property it is required to report full particulars of the type of property concerned and a description of the property in relation to which the terrorist property report is made.

Measures should therefore be in place to enable the institution's to determine the particulars and description of the property.

Please refer to the FIC user guide for uploading of a Terrorist Property Report.

Procedure for providing basic living expenses as contemplated in section 26C

- (2) *The Minister may permit the provision of financial services or the dealing with property if it is necessary to-*
- (a) *provide for basic expenses, including, at least-*
 - (i) *foodstuffs;*
 - (ii) *rent or mortgage;*
 - (iii) *medicines or medical treatment;*
 - (iv) *taxes;*
 - (v) *insurance premiums;*
 - (vi) *public utility charges;*
 - (vii) *maintenance orders;*
 - (viii) *reasonable professional fees, and*
 - (ix) *reimbursement of expenses associated with the provision of legal services;*
 - (b) *satisfy a judgment or arbitral award that was made before the date on which the person or entity was identified by the Security Council of the United Nations;*
 - (c) *make a payment to a third party which is due under a contract, agreement or other obligation made before the date on which the person or entity was identified by the Security Council of the United Nations;*
 - (d) *accrue interest or other earnings due on accounts holding property affected by a prohibition under section 26B;*
 - (e) *make a payment due to a person or entity affected by a prohibition under section 26B by virtue of a contract, agreement or other obligation made before the date on which the person or entity was identified by the Security Council of the United Nations: Provided that the payment is not directly or indirectly being received by that person or entity.*
- (3) *The Minister may permit the provision of financial services or the dealing with property under subsection (1) on his or her own initiative or at the request of a person affected by a prohibition under section 26B.*
- (4) *The Director must, by appropriate means of publication, give notice of the Minister's permission of the provision of financial services or the dealing with property under subsection (1).*
- (5) (a) *The Minister may, in writing, delegate any power conferred in terms of this section, to the Director.*
- (b) *A delegation in terms of paragraph (a)-*
 - (i) *is subject to any limitations or conditions that the Minister may impose;*
 - (ii) *does not divest the Minister of the responsibility concerning the exercise of the delegated power or the performance of the assigned duty.*
 - (c) *The Minister may vary or revoke any decision taken by the Director as a result of a delegation in terms of paragraph (a), subject to any rights that may have vested as a consequence of the decision."*

The institution's will release such funds as directed by the Minister or Director as set out in Section 26 to the sanctioned person/s.

Annexure 10: High Risk Jurisdiction

| | | |
|--------------------------|---------------------|----------------------------|
| Afghanistan | Kazakhstan | Tajikistan |
| Albania | Kenya | Tanzania |
| Algeria | Kiribati | Thailand |
| Angola | Kosovo | Togo |
| Antigua & Barbuda | Kyrgyzstan | Trinidad & Tobago |
| Argentina | Kuwait | Tunisia |
| Armenia | Laos | Turkey |
| Azerbaijan | Lebanon | Turkmenistan |
| Bahrain | Liberia | Turks & Caicos |
| Bangladesh | Libya | Uganda |
| Belize | Macedonia | Ukraine |
| Belarus | Macau | United Arab Emirates (UAE) |
| Benin | Malawi | Uruguay |
| Bolivia | Malaysia | Uzbekistan |
| Bosnia Herzegovina | Mali | Venezuela |
| Botswana | Mauritania | Vietnam |
| Brazil | Mexico | Virgin Islands (British) |
| Brunei Darussalam | Moldova | Yemen |
| Burkina Faso | Mongolia | Zambia |
| Burundi | Montenegro | Zimbabwe |
| Cambodia | Morocco | |
| Cameroon | Myanmar (Burma) | |
| Cape Verde | Namibia | |
| Central African Republic | Nauru | |
| Chad | Nepal | |
| China | Nicaragua | |
| Colombia | Niger | |
| Cote d'Ivoire | Nigeria | |
| Croatia | North Korea | |
| Cuba | Pakistan | |
| Democratic Rep of Congo | Panama (onshore) | |
| Djibouti | Papua New Guinea | |
| Dominica | Paraguay | |
| East Timor | Philippines | |
| Ecuador | Russian Federation | |
| El Salvador | Rwanda | |
| Egypt | Samoa | |
| Eritrea | San Marino | |
| Ethiopia | Sao Tome & Principe | |
| Equatorial Guinea | Senegal | |
| Gabon | Serbia | |
| Gambia | Seychelles | |
| Georgia | Sierra Leone | |
| Ghana | Somalia | |
| Guatemala | Sri Lanka | |
| Guinea Bissau | St Kitts and Nevis | |
| Guinea Republic | St Lucia | |
| Guyana | Sudan | |
| Haiti | Swaziland | |
| Honduras | Syria | |
| India | | |
| Indonesia | | |
| Iran | | |
| Iraq | | |
| Ivory Coast | | |

Annexure 11: Employee Money Laundering and Terrorist Financing Risk Questionnaire

Shortlisted Employee: _____

Employee's Role/Position: _____

Employee Competency: _____

Does the employee have the necessary skills, knowledge and expertise to perform their functions effectively?

Has the employee's previous employment history, employment references, qualifications and relevant accreditations been reviewed?

Employee risk is a combination of an employee's good-standing risk as well as the role's risk assessments.

1. Good Standing Risk:

- Employee good-standing risk assesses whether employees have been subject to criminal conviction and other adverse information.
- Employees subject to criminal conviction and other adverse information identified through screening, are considered to represent a higher ML/TF/PF risk.

Criminal check result: _____

2. Role Risk:

- Employee role risk assesses the extent to which a company employs individuals in roles that are recognised as having increased vulnerability to being used to facilitate money laundering or finance terrorism.

Employee risk is assessed through the following matrix:

- **Low:** There is some risk of a small-scale incident occurring.
- **Medium:** Risk of an incident that can make an impact but not a serious one.
- **High:** Severe events that can cause a loss of business.

| Department | Role/ Vulnerability | Risk Rating | Explanation | Comments |
|-----------------|-----------------------------|-------------|-------------|----------|
| Finance | Senior litigation Secretary | Low | | |
| Executive Suite | Director | High | | |
| Attorneys | Attorneys | Medium | | |
| Administration | Assistants | Low | | |
| | Receptionist | Low | | |

If an employee falls in the Medium to High category as per risk matrix, the following controls will be put in place:

Controls / Mitigations

Preventative:

- Ensuring fit and proper requirements are met in key positions. Managers and key personnel must comply and implement FICA, POCA, POCDATARA policies, procedures and controls to mitigate the risk of ML/TF occurring. Policies, procedures and controls implemented should effectively minimise the risk of ML/TF through effective risk assessments, monitoring, training and revision of risk assessments.
- In instances where there are concerns about employee integrity, management will act where appropriate. If the employee is also licensed under the FSCA, debarment may be considered.

Detective:

- Controls within the company largely rely on employee supervision and face-to-face interactions with the customer. The company will ensure that employees receive adequate and regular AML training and awareness of ML and TF vulnerabilities.

Employee's role risks may be re-assessed to ascertain increased levels of vulnerability and/or opportunity to facilitate laundering of money, financing of terrorism or proliferation financing when job responsibilities are amended and/or as and when required.

Senior Management

Date

Money laundering Compliance Officer

Date

Handwritten signature and initials in black ink, located in the bottom right corner of the page.

Annexure 12: Key Definitions

Definitions

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

1. Client

In relation to the institution's, means a person who has entered into a single transaction or a business relationship with the institution's.

2. Client Representative

In relation to the institution's, means a natural person who has been authorised by a client to enter into a single transaction or a business relationship with the institution's on behalf of that client.

3. Single Transaction

A single transaction means a transaction:

- other than a transaction concluded during a business relationship, and
- where the value of the transaction is not less than the prescribed amount. i.e., R5000

4. Business Relationship

Means a relationship between a client and the institution's for the purpose of concluding transactions on a regular basis.

5. Member Due Diligence Procedure

Means the reasonable steps taken by the institution's to establish and verify the identity of a client that is party to a transaction, which steps are fewer and less onerous than that of an Enhanced Due Diligence.

6. Enhanced Member Due Diligence Procedure

Means the reasonable steps taken by the institution's to establish and verify the identity of a client that is party to a High-Risk ML/TF transaction, which steps are more stringent than a standard Due Diligence.

7. Effective Control

In respect of a legal person, means the ability to materially influence or make key decisions in respect of, or on behalf of that legal person.

8. 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.

9. Money Laundering

Means 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.

10. Terrorist and Related Activities

Has the meaning assigned to it in Section 1 of the Protection of Constitutional Democracy Against Terrorist and Related Activities Act 33 of 2004 ("POCDATARA").

11. Property associated with Terrorist and Related Activities

Has the meaning assigned to it in 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.

An abbreviated list of the POCDATARA offences are:

- 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.
- The intentional seizure, high jacking, taking control, destroying, or endangering the safety of a fixed platform.
- The intentional seizure, detaining or taking of a hostage 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.
- The intentional murder, kidnap violent attack or other offence related to causing harm to an internationally protected person.
- The intentional seizure or taking of control of an aircraft by force or threat.
- The intentional seizure or taking of control of a ship by force or threat.
- The harbouring, concealing, of a person or group of persons who intend to commit, or who has committed any of the offences listed above.
- The financing of a person or group of persons to commit, or to facilitate the commission of any of the offences listed above.
- 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.

12. Cash

Cash means 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.

13. Cash Threshold Report

Means 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 i.e. R 50 000.00 is paid or received by the institution's in terms of that transaction. Split transactions that are suspicious and unusual would be reportable in terms of section 29 of the FIC Act.

14. Suspicious or Unusual Activity Report

Means 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.

15. Suspicious or Unusual Transaction Report

Means 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.

16. Terrorist Financing Activity Report

Means the report that must be submitted to the FIC where there is reasonable knowledge in respect of the financing of terrorism and related activities, 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.

17. Terrorist Financing Transaction Report

Means the report that must be submitted to the FIC where there is reasonable knowledge in respect of the financing of terrorism and related activities, and where the report relates to a transaction or a series of transactions between two or more parties.

18. Terrorist Property Report

Means the report that must be submitted to the FIC where the institution's has in its possession, or under its control property, associated with terrorist and related activities.

19. Non-compliance

Any act or omission that constitutes a failure to comply with any of FICA's provisions, regulations, and the institution's' RMCP, or any order or directive made in terms of FICA.

20. Proliferation Financing

Refers to the act of providing funds or financial services which are used, in whole or in part, for the manufacture, acquisition, possession, development, export, trans-shipment, brokering, transport, transfer, stockpiling or use of nuclear, chemical or biological weapons and their means of delivery and related materials (including both technologies and dual use goods used for non-legitimate purposes), in contravention of national laws or, where applicable, international obligations.

21. Beneficial Owner

Means a natural person who directly or indirectly; ultimately owns or exercises effective control of:

- A client of an accountable institution; or
- a legal person, partnership or trust that owns or exercises effective control of a client of an accountable institution; or
- exercises control of a client of an accountable institution on whose behalf a transaction is being conducted; and includes in respect of legal persons, each natural person contemplated in section 21B(2)(a); (ii) in respect of a partnership, each natural person contemplated in 30 section 21B(3)(b); and (iii) in respect of a trust, each natural person contemplated in section 21B(4)(c), (d) and (e)" of the Act.

22. Domestic Politically Exposed Person (DPEP)

is an individual who holds, including in an acting position for a period exceeding six months, or has held a prominent public function in the Republic, including that of:

- the President or Deputy President
- a government minister or deputy minister;
- the Premier of a province;
- a member of the Executive Council of a province;
- an executive mayor of a municipality elected in terms of the Local Government: Municipal Structures Act, 1998 (Act No. 45 117 of 1998);

- a leader of a political party registered in terms of the Electoral Commission Act, 1996 (Act No. 51 of 1996);
- a member of a royal family or senior traditional leader as defined in the Traditional Leadership and Governance Framework Act, 2003 (Act No. 41 of 2003);
- the head, accounting officer or chief financial officer of a national or provincial department or government component, as defined in section 1 of the Public Service Act, 1994 (Proclamation No. 103 of 1994);
- the municipal manager of a municipality appointed in terms of section 54A of the Local Government: Municipal Systems Act, 2000 (Act No. 32 of 2000), or a chief financial officer 10 designated in terms of section 80(2) of the Municipal Finance Management Act, 2003 (Act No. 56 of 2003);
- the chairperson of the controlling body, the chief executive officer, or a natural person who is the accounting authority, the chief financial officer or the chief investment officer of a public entity listed in Schedule 2 or 3 to the Public Finance Management Act, 1999 (Act No. 1 of 1999) attached as Annexure 5;
- the chairperson of the controlling body, chief executive officer, chief financial officer or chief investment officer of a municipal entity as defined in section 1 of the Local Government: Municipal Systems Act, 2000 (Act No. 32 of 2000);
- a constitutional court judge or any other judge as defined in section 1 of the Judges' Remuneration and Conditions of Employment Act, 2001 (Act No. 47 of 2001);
- an ambassador or high commissioner or other senior representative of a foreign government based in the Republic; or
- an officer of the South African National Defence Force above the rank of major-general; or holds, including in an acting position for a period exceeding six months, or has held the position of head, or other executive directly accountable to that head, of an international organisation.

23. Effective Control

In respect of a legal person, means the ability to materially influence or make key decisions in respect of, or on behalf of that legal person.

24. Foreign Politically exposed Persons (FPEP)

An individual who holds, or has held, in any foreign country a prominent public function including 5 that of a:

- Head of State or head of a country or government;
- Member of a foreign royal family;
- Government minister or equivalent senior politician or leader of a political party;
- Senior judicial official;
- Senior executive of a state owned corporation; or
- High-ranking member of the military.

25. Prominent Influential Persons

A prominent influential person is an individual who holds, or has held at any time in the preceding 12 months, the position of:

- Chairperson of the board of directors;
- Chairperson of the audit committee; 15
- Executive officer; or
- Chief financial officer,

of a company, as defined in the Companies Act, 2008 (Act No. 71 of 2008), if the company provides goods or services to an organ of state and the annual transactional value of the goods or services or both exceeds an amount determined by the Minister by notice in the *Gazette*.

26. Weapons of Mass Destruction

Any weapon designed to kill, harm or infect people, animals or plants through the effects of a nuclear explosion or the toxic properties of a chemical warfare agent, or the infectious or toxic properties of a biological warfare agent, and includes a delivery system exclusively designed, adapted or intended to deliver such weapons.

27. Terrorist Financing (TF)

The act of providing funds to terrorists or terrorist organizations for them to carry out terrorist acts or to benefit any terrorist or terrorist organization.

Handwritten signature or initials in black ink, consisting of a large, stylized 'A' or 'M' shape with a small circle to the left.