Anti-Money Laundering and Combating Terrorism Financing Policy	

Document title	**Anti-Money Laundering and Combating**
Document owner	**Chief Legal Officer**
Approved by	**Risk, Compliance and Technology committee**
Issue Date	**02 May 2023**
Date Last revised	**New**
Document Type	**Policy**

1. Definitions[1]

1.1. For the purposes of this policy, the following terms shall carry the following meanings:

1.1.1. **"Activities"** means Money Laundering, Terrorism Financing, Corrupt Activities, and related topics.

1.1.2. **"Applicable Laws**" means all and any laws and regulations having force of law in the Republic of South Africa, including but not limited to applicable codes of conduct, statutes, ordinances, rules, treaties, permits, licenses, as may be promulgated or amended from time to time.

1.1.3. **"Corrupt activities"** means any behaviour, which as a result of *inter alia* the misuse of authority, or of a position within the Company, induces a person/s to act or not to act in a particular manner with the result that an entity or person benefits at the expense of others. This behaviour can involve (but is not limited to) giving or accepting or offering to give or accept any form of gratification (e.g., cash, funds, services, items)

1.1.4. "**Employees**" means anyone acting for, or on behalf of, the Company, including, but not limited to, Company officers, directors, employees, and agents.

1.1.1. [1] Legal, in consultation with external counsel, is of the view that Redefine is not an accountable institution as defined in section 1 of FICA. It may be that a subsidiary of Redefine will fall within the ambit of FICA. In these circumstances, the AML Policy in respect of the subsidiary will need to be amended to make provision for additional obligations placed on an accountable institution e.g., the appointment of an AML Compliance Officer *viz* a Board appointed compliance officer responsible for ensuring the effectiveness of the RMCP in terms of **section 42A** of **FICA. – note:** consider section 42 in particular section 42A if the AML is amended for an accountable institution.

1.1.5. **"ERM Plan**" means an organisations framework to manage and address an organisation's identified significant risks.

1.1.6. "**FICA**" means the Financial Intelligence Centre Act No. 38 of 2001, as amended from time to time.

1.1.7. **"Fraud"** means the unlawful and intentional making of a misrepresentation which causes actual or potential loss or prejudice to the organisation.

1.1.8. **"GLAA"** means the General Laws (Anti-Money Laundering and Combating Terrorism Financing) Amendment Act 22 of 2022 and the amendments to the legislation as referred to therein, including any subsequent amendments to Applicable Laws arising as a result of the GLAA.

1.1.9. ***"interalia***" means among other things.

1.1.10. **"Immediate family member"** means in relation to PEP, the spouse, civil partner or life partner, the previous spouse, civil partner or life partner, if applicable, children and stepchildren and their spouse, civil partner or life partner, parents, sibling and step sibling and their spouse, civil partner or life partner, individuals who are closely connected to a PEP, either socially or professionally, close business associates and or personal advisors, such as financial advisors or those acting in a financial fiduciary capacity for the PEP's own personal benefit, a person who is known to have a joint beneficial ownership in an entity or other legal arrangement with a PEP (e.g., a business partner or associate), any person who maintains a beneficial ownership interest in an entity or other legal arrangement that is set up by or for the personal benefit of a PEP or a person widely and publicly known to maintain a close relationship with the PEP.

1.1.11. **"Money Laundering"** means an activity which has, or is likely to have the effect of hiding, concealing, or disguising the original ownership and control, nature, source, location, disposition, or movement of the proceeds of unlawful activities or any interest which anyone has in such proceeds. For purposes of the Policy, Money Laundering shall include:

1.1.10.1 the conversion or transfer of property, knowing that such property is derived from criminal activity or from an act of participation in such activity, for the purpose of concealing or disguising the illicit origin of the property or of assisting any person who is involved in the commission of such an activity to evade the legal consequences of that person's action.

1.1.10.2 the concealment or disguise of the true nature, source, location, disposition, movement, rights with respect to, or ownership of, property, knowing that such property is derived from criminal activity or from an act of participation in such activity.

1.1.10.3 the acquisition, possession, or use of property, knowing, at the time of receipt, that such property was derived from criminal activity or from an act of participation in such activity.

1.1.10.4 participation in, association to commit, attempts to commit and aiding, abetting, facilitating, and counselling the commission of any of the above-mentioned actions.

1.1.12. **"Politically Exposed Person"** or **"PEP"** means:

1.1.10.5 Individuals who are or have been entrusted with prominent public functions by a foreign country, for example, Heads of State or of government, senior politicians, senior government, judicial or military officials, senior executives of state-owned corporations, important political party officials.

1.1.10.6 A domestic prominent influential person is an individual who holds, including in an acting position for a period exceeding six months, or has held at any time in the preceding 12 months, a prominent public function, for example, senior politicians, government, judicial or military officials, senior executives of state-owned corporations, important political party officials in the Republic.

1.1.10.7 persons who are or have been entrusted with a prominent function by an international organisation, refers to members of senior management or individuals who have been entrusted with equivalent functions, i.e., directors, deputy directors, and members of the board or equivalent functions.

1.1.10.8 An Immediate Family Member of a person referred to in 1.1.10.1 and 1.1.10.2 above; and/or

1.1.10.9 a natural person who is a close associate of a person referred to in 1.1.10.1 and 1.1.10.2 above.

1.1.13. "**POCA**" means the Prevention of Organised Crime Act, No. 121 of 1998 as amended from time to time.

1.1.14. **"Policy"** means this Anti-Money Laundering and Combating Terrorism Financing Policy.

1.1.15. **"POCDATARA"** means the Protection of Constitutional Democracy Against Terrorist and Related Activities Act, No. 33 of 2004, as amended from time to time.

1.1.16. **"PRECCA"** means the Prevention and Combating of Corrupt Activities No. 12 of 2004

1.1.17. **"Proliferation Financing"** means the provision of funds or financial services used 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.

1.1.18. **"Sanctions"** means restrictions on activities that relate to particular countries, goods and services, or persons and entities.

1.1.19. "**SOPs"** means standard business unit specific operating procedures and "**SOP**" means any one of them as the context may require.

1.1.20. **"Terrorism Financing"** means the activities which involve the collection or provision of funds for the purpose of enhancing the ability of an entity or anyone who is involved in terrorism or related activities to commit an act that is regarded as a terrorist act.

1.1.21. **"Redefine"** means Redefine Properties Limited (registration number 1999/018591/06) and "**Company**" shall bear a corresponding meaning.

1.1.22. **"Reports"** means any report in terms of Section 29 of FICA.

1.1.23. **"Tipping Off"** means a person involved in the making of a report may not inform anyone, including the customer or any other person associated with a reported transaction, of the contents of a suspicious transaction or activity report or even the fact that such a report has been made.

2. Purpose

2.1. The Company will not knowingly conduct business with any person, entity, or party whose conduct may give risk to suspicions of involvement with Activities.

2.2. The Company supports participation in, and compliance with, efforts to combat Activities.

2.3. This Policy aims to foster Employee awareness of the Activities by introducing internal policy, processes, standards, and controls to be applied by Employees to identify and prevent the occurrence of any Activities.

2.4. This Policy also aims to introduce systems and training to ensure that the Company, and its Employees, meet their statutory duties and discharge their regulatory obligations.

2.5. This Policy forms part of the Redefine Ethics Framework and is intended to be read in conjunction with the Redefine Fraud Policy, the Fraud and Corrupt Activities Framework as well as supplementary policies aimed at promoting ethical and responsible business practices.

2.6. Any failure to comply with this Policy can expose the Company to significant reputational damage, legal and regulatory risk, as well as financial loss.

3. Legal and Regulatory Framework

The Policy was formulated having regard to the legislation referred to in the table below.

FICA	creates compliance obligations which *inter alia* assist in the identification of the proceeds of unlawful activities, combats Money Laundering, and combats the financing of terrorist and related activities
GLAA	provides for the amendments of *inter alia* FICA, the Companies Act 2008, the Trust Property Control Act 1988, the Non-profit Organisations Act 1997, and the Finance Sector Regulation Act 2017, and develops a comprehensive mechanism to bring transparency to beneficial ownership
POCA	introduces measures to *inter alia* combat organised crime; Money Laundering and racketeering activities
POCDATARA	*inter alia* provides measures to prevent and combat terrorism and other offences associated with terrorist activities and to provide measures to prevent and combat Terrorism Financing
PRECCA	combats Money Laundering activities by way of *inter alia* an offence created by section 20 of PRECCA

4. Scope

4.1. The Policy is drafted having regard to the Legal and Regulatory Framework governing the Activities and is intended to establish an Activities prevention culture.

4.2. The scope of the Policy extends to understanding, identifying, avoiding, monitoring, detecting and, to the extent applicable, reacting to any Activities.

4.3. This Policy applies to all Employees of the Company, adherence to the Policy is mandatory and (i) will assist the Company in ensuring that regulatory requirements are observed and (ii) reduce the Company's exposure to reputational, operational, financial, and legal risks.

4.4. Accordingly, all departments and business units of the Company are to be guided by the Policy, and Employees are to ensure compliance with, and use of, the Policy (in conjunction with the Redefine Ethics Framework) as their point of reference.

4.5. The Policy will be supplemented by business unit specific training and SOPs. Failure by any Employee to comply with department specific SOPs *provided* will be deemed to be a breach by the Employee of the Policy.

4.6. Employees are required to fully comply with this policy at all times. Violation of this Policy will be dealt with in terms of the Company's disciplinary code and processes, in addition to any substantial fines and criminal prosecution.

5. Redefine Policy Statements

The Policy Statements recorded in this paragraph 6 are to, the extent required and applicable, to be complied with by all Employees and all provisions of this Policy *vis-á-vis* non-compliance apply to this paragraph 6 as if specifically incorporated herein.

5.1. Redefine's PEP policy statement:

Redefine's governance and compliance approach incorporates, where and when applicable, monitoring efforts to ensure the monitoring of anti-Money Laundering, Terrorism Financing, anti-bribery and Corrupt Activities. These monitoring efforts extend to including the notification and awareness of PEPs and PEP entities *and/or activities they are involved in.*

To monitor Employees that do/could fall to be classified as a PEP, Redefine has adopted a risk-based approach wherein the risk of an Employee being classified as a PEP risk has been incorporated into Redefine's ERM Plan. This risk-based approach includes:

(i) the ranking of all Employees (including both non-executive and executive directors) as high, medium, or low risk.

(ii) remedial action for the identified risk, where deemed appropriate.

(iii) The completion, by all Employees and Directors, of a mandatory annual self-declaration form to manage risks proactively. Enhanced due diligence must be applied to both PEPs and PEP entities. When dealing with a PEP entity Due Diligence must be applied to the PEP entity and the PEPs identified in the PEP entity.

5.2. Redefine's Political Donations or Contributions policy statement:

5.2.1. The Company adopts a discretionary approach when considering political donations or contributions in the countries in which it operates.

5.2.2. Employees shall not, at any time, without complying strictly with the requirements set out in this paragraph 5.2., consider making/make any political donations or contributions of any nature whatsoever.

5.2.3. Political donations must be permitted by local laws and regulations and made to a political party or a political organisation and not to individual political candidates.

5.2.4. Any political donations or contributions can only be made following the presentation of a strong business case, based on local circumstances which will include a detailed risk assessment set out in the ERM plan (as amended from time to time).

6. Policy Principles

6.1. The key principles of this Policy include:

6.1.1. identifying risks inherent in the business, implementation of department specific SOPs; facilitation of required training to enable Employee compliance with the Policy and the SOPs;

6.1.2. confirmation that the required policy principles are in place to (i) manage corruption, Money Laundering and to counter Terrorism Financing risks, and (ii) mitigate the risks of Money Laundering and terrorism financing to minimize the impacts thereof.

6.1.3. avoiding, detecting and, if applicable monitoring and reporting on Activities

6.1.4. responsibilities of the Company, senior management, and other Employees

6.2. To facilitate the policy principles:

6.2.1. the Company is:

6.2.1.1. to identify potential Company risks at a business department level to produce the required SOPs and provide the necessary training to facilitate Employee compliance with the Policy;

6.2.1.2. to ensure that the required structures and policies are in place to manage the Activities and any risk associated therewith; and

6.2.1.3. to implement and support policies in place to avoid/mitigate the risks of the Activities;

6.2.1.4. obliged to cooperate with the relevant authorities and release to them such information as required related to the proceeds of unlawful activity, Money Laundering, Terrorism Financing, Proliferation Financing, and related activities or financial Sanctions.

6.2.2. senior management is to:

6.2.2.1. implement policies and procedures to manage the Activities;

6.2.2.2. develop processes that identify, manage, and monitor Activity risks that may be incurred by the Company;

6.2.2.3. monitor the appropriateness, adequacy, and effectiveness of the Activities risk management system as well as the SOPs;

6.2.2.4. ensure that Employees adhere to policies and procedures to avoid Activities risks;

6.2.2.5. identify the vulnerability of the Company to be used to launder money or finance terrorists and to the extent necessary implement risk management controls to ensure that the Company is not used to launder money or finance terrorists;

6.2.2.6. devote appropriate resources to deal with money laundering and terrorist financing and ensure Employees receive appropriate and sufficient training;

6.2.2.7. report, where applicable, monitoring results and any other significant internally identified anti-money laundering and counter terrorism financing compliance matters to the responsible internal person;

6.2.2.8. where applicable, the immediate reporting of actual or potential Activity risks to the responsible person (the Board) in the Company and to the Financial Intelligence Centre (FIC) and inform the responsible person and provide guidance to the Employees on the reporting of suspicious transactions;

6.2.2.9. Reports of suspected money laundering and terrorist financing risks must be reported to the Board, which is responsible for reporting to the FIC.

6.2.3. Employees are to:

6.2.3.1. carry out their responsibilities according to the Policy and all procedures (including SOPs) developed to manage the Activities and risks;

6.2.3.2. ensure no transactional activity is undertaken without a clear understanding of the purpose and background of the transactional activity;

6.2.3.3. promptly report to the responsible person when they have knowledge or suspicion of any Activities or where there are reasonable grounds to know of or suspect any Activities, which includes knowledge that the Company has received, or is about to receive the proceeds of unlawful activities or property which is connected to an offence relating to an Activity; a transaction or series of transactions to which the Company is a party must, as soon as it has acquired the knowledge or the suspicion arose, report to the relevant person the grounds for the knowledge or suspicion and the prescribed particulars concerning the transaction or series of transactions.;

6.2.3.4. not tip off any person that a suspicious transaction report has been made or that their transactions are under any investigation;

6.2.3.5. assist / support Senior Management and the responsible person with any reported matters; and

6.2.3.6. complete a record of when they have received Activities training.

7. Sanction Compliance

The Company strives at all times to comply with all/any applicable sanctions and restrictive measures which may apply in the country in which it operates. Therefore, the Company will use its best endeavors to not knowingly engage in any commercial relationship or financial relationship with a sanctioned entity, and/or a restricted country.

8. Internal monitoring

An independent review of the Company's anti-money laundering and counter Terrorism Financing program must be conducted on a regular basis.

The review should be completed in accordance with the established audit and compliance procedures. Results of the reviews should be reported to the identified responsible person, including recommendations to rectify shortcomings identified.

9. Processing of Personal Information

The processing of Personal Information will take place according to the Company's Protection of Personal Information Policy.

10. Disclosure and reporting

Incidents, suspicious activities, breaches of non-compliance are required to be formally reported by the Head of Risk and Compliance periodically to the, Risk and Compliance Management Committee, and the Risk, Compliance and Technology Committee, as well as the FIC, in the prescribed manner. subject to Tipping Off-restrictions.

However, more frequent reporting may be required by management, other lines of assurance and/or the FIC.

11. Approval of policy

Approved by	Signed by	Signature	Date
Risk, Compliance and Technology	*L Sennelo Chairperson*		*2023*

16 Aug, 2023 1:48:43 AM GMT+2

Frequency of review	Next review date
Every three years or as and when required	02 May 2026