
	<b>REALESTATE GROUP</b>		
	<b>ANTI-MONEY LAUNDERING (AML), COUNTER-FINANCING OF TERRORISM (CFT) AND COUNTER FINANCING OF PROLIFERATION (CFP) POLICY</b>		
	Approved on 29 November 2022	<b>Version 2.0</b>	

## APPROVAL

Date	29 November 2022 (Update)
Approved by Board Representative	Nicola R Milne
Reviewed by Executive Chairman	Guido R Giachetti
Reviewed by Chief Executive Officer	Jacopo Pari

## KEY STAKEHOLDERS

Governing Body	Board of Directors
Audit and Risk Committee	Committee delegated to oversee, review and make recommendations for the Group's Governance
Executive Chairman	Guido R Giachetti
The Manager, The Management Company	Property and Asset Management Limited, so long as the current management agreement with RDC continues, and its successor should it be terminated, and /or its subsidiaries or outsourced service providers.
Management Team – “The Manager”	Management and Staff of the Manager

### 1. Policy Statement

- 1.1 This Policy and the procedures documented herein apply to all employees, directors, partners and contractors of the RDC Properties group of companies (“RDCP” or “the Group”). This includes all majority owned subsidiaries of the Group whether in country or in foreign jurisdictions.
- 1.2 The main purpose of the Group is “**to own and manage strategic property assets that add value to the communities we serve**”. The Group has a responsibility to maintain its integrity and the public's confidence by ensuring it conducts business in line with the laws, industry norms, regulations, standards and codes of good practice and the principles of being a good corporate citizen.
- 1.3 The group is strongly committed to preventing the use of its products, services and systems for the commission or perpetration of financial crimes such as money laundering (ML), terrorism financing (TF) or the financing of proliferation (PF).
- 1.4 To this end, the Group has devised a policy for anti-money laundering (AML), counter-financing of terrorism (CFT) and counter-financing of proliferation (CFP) of arms of war and Nuclear, Biological and Chemical (NBC) weapons in line with the country's anti-money laundering, counter-financing of terrorism and counter-financing of proliferation legislation, as well as international standards aimed at combatting ML, TF and FP.

### 2. Objectives of the Policy

The objectives of the policy are as follows:

- 2.1 To prevent the Group's products, services and systems from being used for money laundering, terrorism financing or the financing of proliferation.
- 2.2 To establish a framework for adopting appropriate AML/CFT/CFP procedures and controls in the operations/business processes of the Group.

- 2.3 To liaise and assist law enforcement agencies with regards to any investigations.
- 2.4 To monitor customer transactions to identify suspicious activity and report such activity to the Financial Intelligence Agency.
- 2.5 To maintain and comply with the legislative and regulatory requirements relating to record keeping and record retention periods.
- 2.6 To protect the Group's reputation.

### **3. Regulatory and Legislative Framework**

- 3.1 The Group adheres to legislation in Botswana and applicable international initiatives aimed at combating financial improprieties.

This AML/CFT/CFP compliance policy is based on the following key legislation:

- Financial Intelligence Act No. 2 of 2022
  - Financial Intelligence Regulations
  - Counter Terrorism Act 2014
  - Proceeds and Instruments of Crime Act 2014 (with amendments thereon)
  - Corruption and Economic Crimes Act 1994
  - Trust Property Control Act 2018 (With amendments thereon)
  - Any other relevant legislation
- 3.2 In addition, the Group subscribes to international standards such as the Financial Action Task Force 40 recommendations, including observance of Targeted Financial Sanctions (TFS) under the auspices of The United Nations Security Council resolutions and any other sanctions regimes such as The Office of Foreign Assets Control (OFAC), and The European Union amongst others.

### **4. Definitions**

Money laundering is generally defined as engaging in acts designed to conceal or disguise the true origins of criminally or terrorism derived proceeds so that the proceeds appear to have been derived from legitimate origins or constitute legitimate assets. Such acts also include depositing of proceeds into bank accounts and spending of proceeds. Money can generally be laundered through a three-step process, but it is important to note that a laundering scheme will not necessarily include all stages, nor is it limited to these three steps. Every act committed during each stage may constitute a laundering offence in a particular jurisdiction.

#### **4.1 Placement**

This is the initial stage where cash generated from criminal activities enters the financial system and, in general, includes actions such as deposits and transfers to a financial institution. Given the nature of the Group's operations whereby it does not conduct cash transactions with its clients, with its operations being through bank transfers and sometimes cheques, it is highly unlikely that the Group and investee companies would be used at this stage.

#### **4.2 Layering**

This is the stage where funds are transferred or moved into other accounts or other financial institutions to further separate the money from its criminal origin. Complex layers of financial transactions are created to disguise the audit trail. This stage is the most ingenious and often the most complex. This is the stage where RDCP needs to be vigilant as it can be used through transfers from unknown sources.

#### 4.3 Integration

If undetected so far, this is the stage at which laundered funds are reintroduced into the legitimate economy, appearing to have originated from a legitimate source. Integration is the final stage of the process, whereby criminally derived property that has been placed or layered is returned (integrated) to the legitimate economic and financial system and is assimilated with all other assets in the system. Integration of the “cleaned” money into the economy is accomplished by the launderer making it appear to have been legally earned. At this stage, it is extremely difficult to distinguish legal and illegal wealth.

### 5. **Minimum Requirements**

#### 5.1 Identification Procedures

With reference to international best practice and KYC procedures, all our potential clients and investee companies shall be subjected to these procedures and their identity verified. In addition, all monetary transactions with the potential clients and investee companies shall be from and to a bank account with a reputable bank acceptable to the Group. The identification means to identify the corporate bodies, individual investors, origin of the funds and legitimacy of the bank accounts are presented below.

##### *Individuals*

- Certified copies of IDs or Passport;
- Proof of address (ie, water bill, telephone bill, title deed, lease agreement, affidavit of residence, etc)

##### *Companies*

Identification documents include, but are not limited to the following:

- Constitutional documents of the company.
- Details of registered office and place of business.
- Company’s board of directors’ resolutions on authorized signatories.

Shareholders should be identified and provide the following information:

##### *For Individual Shareholders*

- Copy of valid national identity card or passport and relevant permits (for non-citizens).
- Proof of residential address - copies of utility bills or by other means.
- Details of bankers.

##### *For Corporate Body Shareholders*

- Company registration documents (i.e. certificate of incorporation and extract from CIPA).
- Company registered office and place of business.
- Details of bankers.
- Identify the natural persons behind the company.

The bank account held in a reputable bank acceptable to the Group shall be verified by a bank statement or a bank reference letter.

#### 5.2 Suspicious Transactions Reporting (STR)

Employees and directors of the Group and directors of RDC shall promptly report to the Group CFO/Compliance Manager or the CEO all cases where the individual becomes aware, has knowledge or suspects or has reasonable grounds to believe, that an employee of the Group or director of RDC, Group’s potential client, investee company or other partner has been or is involved in an illegal activity or crime or is in breach of provisions in this policy for further investigation and report to the FIA.

STRs must be filed when the customer:

- Presents fake documents.
- Is reluctant to provide identifying information or provides minimal or seemingly fictitious information.
- Is suspected of involvement in illegal activity (eg, wanted persons, etc).
- Is involved in identity theft, (ie, presents a fake identity card to impersonate someone else in order to have access to a transaction.

### 5.3 Employee Monitoring

There shall be zero tolerance for employees who engage in fraudulent activities. Such persons shall be deemed unfit to work with the Group and their appointment terminated.

### 5.4 Dissemination of Anti-Money Laundering Information

All employees (temporary and permanent) shall receive information related to AML/CFT/CFP as part of the orientation programme for newly employed staff. Updated information will be disseminated as required by any changes to the relevant legislation.

### 5.5 Confidentiality of Customer Data

All information about customers and their transactions that is obtained in the course of fulfilling AML/CFT/CFP obligations is considered confidential. Therefore, employees are encouraged to avoid disclosure to other parties or to the customer of any suspicions identified, investigated, or reported.

## **6. Roles and Responsibility for the Policy**

- 6.1 The Board of Directors shall approve the AML/CFT/CFP policy.
- 6.2 The Board of Directors, through the Audit and Risk Committee, shall oversee compliance with this policy and all other statutory and regulatory AML/CFT/CFP obligations.
- 6.3 Management is responsible for ensuring that all employees, directors, key representatives of the investee companies and partners are made aware of and understand this policy.
- 6.4 Employees and directors of the Group will assist in minimising potential losses derived from fraudulent transactions as well as combating crime in general when this policy is implemented well.

## **7. AML/CFT/CFP Programme**

- 7.1 The key elements of the AML/CFT/CFP programme encompass the following:
  - Board approved AML/CFT/CFP Policy and Procedures.
  - Designated Money Laundering Reporting Officer (MLRO), which is the Chief Financial Officer.
  - ML/TF/PF risk assessments.
  - Independent testing.
- 7.2 The programme is underpinned by the following key elements:
  - Customer due diligence including ongoing due diligence and enhanced due diligence.
  - Sanction Screening of customers and transactions.
  - Suspicious Transactions and Threshold Transactions Reporting.
  - Monitoring and reporting of Complex, Unusual and High Risk Transactions.
  - Risk-Based Approach using policies, procedures, processes, systems, and controls to identify, manage and mitigate money laundering and terrorism/proliferation financing risks.
  - Ongoing employee training and customer education.

- Continuous review and updating of the AML/CFT/CFP Policy and its corresponding AML/CFT/CFP Standards as threats and international standards evolve to prevent and detect ML, TF, or PF risks.
- Independent testing performed by the external auditors of the Group and individual companies. Recommendations and findings from the auditors will form the basis of further procedures.

## 8. Record Keeping

The Group will keep all relevant records on the identity and transactions of their clients, both locally and internationally, for seven years, or longer if required by the FIA.

### 8.1 Time Limits

The Group will observe the following time limits in order to facilitate the investigation of any audit trail concerning the transactions of their customers:

- *Entry records* – The Group shall keep all account opening records, including verification documentation and written instructions for a period of at least seven years after termination.
- *Ledger records* - The Group shall keep all account ledger records for a period of at least seven years following the date on which the relevant transaction or series of transactions is completed.
- *Supporting records* – The Group shall keep records in support of ledger entries including cheques, for a period of at least seven years following the date on which the relevant transaction or series of transactions is completed.

Notwithstanding that the prescribed period for retention of records may have lapsed, the Group may be requested to keep records until further notice, where an investigation into a suspicious transaction has been initiated. Even in the absence of such a request, the group shall not destroy any relevant records without the prior approval of FIA, even though the prescribed period of retention may have lapsed.

## 9. Monitoring and Review of the Policy

Management will monitor the effectiveness and review the implementation of this policy. The suitability, adequacy and effectiveness of the policy will be compared to the FIA guidelines, as well as international guidelines and regulations, every three years at a minimum. Improvements in the policy shall be made as soon as the need is identified and/or when there is a change to the enabling legislation.

## 10. Approval Signatures

  
\_\_\_\_\_  
Governing Body Representative

  
\_\_\_\_\_  
Chief Executive Officer

  
\_\_\_\_\_  
Executive Chairman