

**RISK MANAGEMENT AND COMPLIANCE PROGRAMME ("RMCP")
IN TERMS OF SECTION 42 OF THE FINANCIAL INTELLIGENCE CENTRE
ACT, NO 38 OF 2001
FOR PLATINUM LIFE (PTY) LTD, FSP 5394**

1. DEFINITIONS

- "FICA" means the Financial Intelligence Centre Act, Number 38 of 2001, as amended from time to time.
- "FIC" means the Financial Intelligence Centre, a juristic person created under chapter 2 of FICA.
- "RMCP" means the Risk Management and Compliance Programme contained in this document, which has been designed in response to section 42 of FICA.

2. INTRODUCTION

- 2.1. Platinum Life is an accountable institution and subject to the provisions of FICA.
- 2.2. The purpose of this RMCP is to identify and assess the risk to Platinum Life of policy owners seeking to launder money or to finance terrorism.
- 2.3. Platinum Life is obliged to be on the lookout for such illegal practices and to report any instances of such activity or any other suspicious activities.
- 2.4. Platinum Life's obligations also extend to monitor, mitigate and manage the risk of its products and services being utilized for these illegal practices.
- 2.5. This document seeks to set out how Platinum Life intends to comply with these obligations, and other related matters.

3. OVERVIEW OF PLATINUM LIFE

- 3.1. Platinum Life offers risk-only life insurance products to natural persons.
- 3.2. The likelihood of Platinum Life being used for money laundering and or terrorist financing activities is low.
- 3.3. The premiums received for Platinum Life products are received by debit order only and no single premiums are allowed.

- 3.4. In the event that a Platinum Life policy owner pays a premium or premiums by Electronic Fund Transfer (“EFT”) and the premium balance of the policy is in credit by more than R 2,000.00, the amount of premium in excess of R2,000.00 is refunded to the policy owner.
- 3.5. All premiums are received directly by the insurer which is Guardrisk Life.
- 3.6. Platinum Life markets its products to prospective policy owners referred to the company by persons already on the Platinum Life database, or to persons who have responded to social media advertising.
- 3.7. All prospective policy owners are risk rated.
- 3.8. All Platinum Life products are sold by means of outgoing telemarketing and no inbound product requests are accepted.
- 3.9. Platinum Life’s Head Office is situated in Illovo, Johannesburg, with accompanying sales centres in Potchefstroom, Centurion, and Roodepoort.

4. RISKS IDENTIFIED

- 4.1. Platinum Life could potentially be used for money laundering or the financing of terrorism in the event that:
 - 4.1.1. a claimant successfully submits a fraudulent claim for a risk-only life insured event with the use of false identification and false medical information, or
 - 4.1.2. a policy owner successfully submits a fraudulent claim for a refund of premiums, or
 - 4.1.3. the banking details of a supplier is fraudulently changed.
- 4.2. Should additional risks become apparent, this list shall be updated.

5. THE ESTABLISHMENT AND VERIFICATION OF THE IDENTITY OF PERSONS

- 5.1. Every prospective policy owner’s identity number is obtained and recorded when he or she agrees to enter into an agreement of sale.
- 5.2. Every policy owner’s identity number is verified should he or she wish to make any beneficiary change to a policy.
- 5.3. Each claimant’s identity number is verified before any benefit is paid.
- 5.4. If a person is mandated to act on behalf of a policy owner, the identity of such a person is verified, as is the mandate.

6. ONGOING DUE DILIGENCE

- 6.1. Platinum Life is obliged to continue to monitor existing policy owners and to take note when the policy owner behaves in a manner inconsistent with its previous knowledge of that policy owner.
- 6.2. Policy owners are contacted every six to eight months and offered an upgrade on their existing policy. Should the policy owner accept such an upgrade, all the personal information of the policy owner will again be confirmed.

7. COMPLEX OR UNUSUALLY LARGE TRANSACTIONS, UNUSUAL PATTERNS OR TRANSACTIONS WHICH HAVE NO APPARENT BUSINESS OR LAWFUL PURPOSE

- 7.1. In the event that Platinum Life is asked to become party to, or to facilitate, any complex or unusually large transactions, it must be especially vigilant about the possibility that the parties involved might be attempting to launder money or finance terrorism. These transactions and the parties involved must be properly identified and investigated and records of such findings must be kept.
- 7.2. Any suspicious activity must be reported to Senior management, the Company's Head of Compliance, FICA Compliance Officer or Money Laundering Reporting Officer

8. APPOINTMENT OF FICA COMPLIANCE OFFICER

- 8.1. Platinum Life's FICA Compliance Officer is Robbie Stutterheim.
- 8.2. Platinum Life's Money Laundering Reporting Officer is Raymond McIntyre.
- 8.3. Platinum Life's Compliance Head is Terisha Nareen.
- 8.4. Any suspicion can be reported to the Company's Compliance Head at compliance@platinumlife.co.za

9. RETENTION OF RECORDS

- 9.1. Platinum Life is obliged to keep records of every transaction had with a policy owner.
- 9.2. Such records ("FICA records") must reflect the following:
 - 9.2.1. the amount involved and the currency in which it was denominated,
 - 9.2.2. the date on which the transaction was concluded,
 - 9.2.3. the parties to the transaction,
 - 9.2.4. the nature of the transaction,

- 9.2.5. business correspondence,
 - 9.2.6. the intended purpose of the business relationship, and
 - 9.2.7. copies of, or references to, information provided to or obtained by the accountable institution to verify a person's identity.
- 9.3. By their very nature, personal information pertaining to policy owners are privileged records and must be protected.
- 9.4. No FICA records are to be deleted for any reason without the authority of the FICA Compliance Officer and no such records are to be made available to any third party without the consent of the policy owner to whom they relate, unless required by law.
- 9.5. All policy owner details, and information is stored on Pinotage, an in-house insurance management system. All data is backed up and is secured with strict access control. Further information can be found in Platinum Life's Records Retention policy.

10. DUTY TO REPORT SUSPICIOUS AND UNUSUAL TRANSACTIONS

- 10.1. Every employee of Platinum Life has a duty to report any suspicious transaction that Platinum Life may be involved in, or become involved in, to the Company's Head of Compliance, FICA Compliance Officer or Money Laundering Reporting Officer.
- 10.2. The duty to report is triggered when an employee has knowledge or a suspicion that Platinum Life:
- 10.2.1. has received or is about to receive the proceeds of unlawful activities,
 - 10.2.2. is a party to a transaction that is likely to result in the transfer of proceeds of unlawful activities,
 - 10.2.3. appears to have no business or lawful purpose,
 - 10.2.4. is constructed to avoid a duty to report,
 - 10.2.5. related to an attempt to evade tax or other duty or levy administered by SARS,
or
 - 10.2.6. has been or is about to be used for money laundering purposes.
- 10.3. Platinum Life is aware of the risks as detailed in the table set out below paragraph 10.4, and which risks have been identified with reference to Guidance Note 4 on Suspicious Transaction Reporting (Notice 301 of 2008). These risks have been assessed and evaluated based on the likelihood of the risk occurring, as well as the impact should the risk occur. Risks are rated from high to low with high having a major impact and low having a minor impact. Implemented controls are those used to mitigate and minimise these risks.

10.4. For the purposes of this clause 10.4 and clause 11.1, the likelihood assessment is defined as follows:

- 10.4.1. “Possible” means that there is a conceivable chance of the risk occurring.
- 10.4.2. “Unlikely” means that there is an improbable chance of the risk occurring.
- 10.4.3. “Highly Unlikely” means it is practically inconceivable that the risk will occur.
- 10.4.4. “Not Applicable” means that the risk is not applicable given the nature of our business and products sold.

Risk	Likelihood Assessment	Risk Rating	Implemented Controls
Unusual business identified	Possible	High- Major Impact	FICA Training and Employee Reporting (Quality Control)
Deposits of funds made with a request for their immediate transfer elsewhere	Possible	High - Major Impact	FICA Training, Employee Reporting (Quality Control) and Managerial oversight
Unwarranted and unexplained international transfers	Unlikely	High – Major Impact	Senior Managerial oversight
The payment of commissions or fees that appear excessive in relation to those normally payable	Highly Unlikely	High – Major Impact	Senior Managerial oversight
The lack of concern about high commissions, fees, penalties etc. incurred as a result of a transaction or particular method of transacting	Highly Unlikely	High – Major Impact	FICA Training, Employee Reporting (Quality Control) and Senior Managerial oversight
Transactions that do not appear to be in keeping with normal industry practices	Unlikely	High – Major Impact	FICA Training, Employee Reporting (Quality Control) and Senior Managerial oversight

Risk	Likelihood Assessment	Risk Rating	Implemented Controls
Purchase of commodities at prices significantly above or below market prices	Highly Unlikely	High – Major Impact	Senior Managerial oversight
Unnecessarily complex transactions	Unlikely	High – Major Impact	Senior Managerial oversight
Buying or selling securities with no apparent concern for making a profit or avoiding a loss	Highly Unlikely	High – Major Impact	Senior Managerial oversight
Unwarranted desire to involve entities in foreign jurisdictions in transactions	Highly Unlikely	High – Major Impact	FICA Training, Employee Reporting (Quality Control) and Senior Managerial oversight
A customer attempts to convince employee not to complete any documentation required for the transaction	Possible	Low – Minor Impact	FICA Training and Employee Reporting (Quality Control)
A customer makes inquiries that would indicate a desire to avoid reporting	Possible	Low – Minor Impact	FICA Training and Employee Reporting (Quality Control)
A customer has unusual knowledge of the law in relation to suspicious transaction reporting	Possible	Low – Minor Impact	FICA Training and Employee Reporting (Quality Control)
A customer seems very conversant with money laundering or terrorist activity financing issues	Possible	Low – Minor Impact	FICA Training and Employee Reporting (Quality Control)

Risk	Likelihood Assessment	Risk Rating	Implemented Controls
A customer is quick to volunteer that funds are clean or not being laundered	Unlikely	Low – Minor Impact	FICA Training and Employee Reporting (Quality Control)
A customer provides insufficient vague or suspicious information concerning a transaction	Unlikely	Low – Minor Impact	FICA Training and Employee Reporting (Quality Control)
Accounts that show unexpectedly large cash deposits and immediate withdrawals	Not Applicable	Not Applicable	Not Applicable
Involvement of significant amounts of cash in circumstances that are difficult to explain	Not Applicable	Not Applicable	Not Applicable

10.5. Once an employee becomes aware of a suspicious or unusual transaction, it must be reported immediately. Every employee has a duty to approach Platinum Life’s Head of Compliance, FICA Compliance Officer or Money Laundering Reporting Officer and to make a full disclosure of the facts and circumstances giving rise to such belief that a report to the FIC is required. Any documentation related to these facts and circumstances must also be brought to the attention of the Company’s Head of Compliance, FICA Compliance Officer or Money Laundering Reporting Officer.

10.6. No employee is allowed to disclose any details about the suspicious or unusual transaction to anyone else, unless this is required in terms of the FICA, or for the purposes of legal proceedings or in terms of an order of court. Employees are specifically not entitled to disclose any details about the report to the person who is the subject of the report. If by some coincidence, an employee becomes aware that another employee has made a report about a suspicious or unusual transaction, the duty of confidentiality is the same as if that employee had made the report himself.

10.7. On suspicion of any unlawful activity, a Suspicious and Unusual Transaction Report (STR), Cash Threshold Report (CTR) or Terrorist Property Report (TPR) will be completed and submitted to the FIC by Platinum Life's FICA Compliance Officer.

11. STANDARDISED COMPLIANCE RISK AND IMPLEMENTED CONTROLS

11.1. Platinum Life has identified compliance risks considering its compliance objectives and obligations. The compliance risks have been assessed and evaluated based on the likelihood of the risk occurring, as well as the impact should the risk event occur. Risks are rated from high to low with high having a major impact and low having a minor impact. Implemented controls are those used to mitigate and minimise these compliance risks:

Compliance Risk	Likelihood Assessment	Risk Rating	Implemented Controls
Failure to report suspicious or unusual transactions	Possible	High- Major Impact	FICA Training and Quality Control (Employee Reporting).
FICA Customer Due Diligence measures are not conducted	Possible	High - Major Impact	FICA Training and managerial oversight. Ongoing customer due diligence
FICA Record keeping requirements are not met	Possible	High – Major Impact	Annual review of RMCP and continuous update when required
FICA requirements are not implemented, reviewed and maintained	Unlikely	High – Major Impact	Annual review of RMCP and managerial oversight
Reputational or brand damage where FICA awareness training of employees is not conducted	Unlikely	High – Major Impact	FICA Training and managerial oversight

12. THE INABILITY TO CONDUCT DUE DILIGENCE AND THE TERMINATION OF BUSINESS RELATIONSHIPS

- 12.1. Should Platinum Life be unable to comply with its FICA and other due diligence obligations in respect of a policy owner, and as described in this RMCP, it may not enter into a business relationship or conclude a single transaction with such a policy owner. More specifically:
 - 12.1.1. should a prospective policy owner refuse to provide his or her identification number, no transaction may be concluded with such person,
 - 12.1.2. should a claimant refuse to provide proof of his or her identification number, no benefit may be paid to such claimant.
- 12.2. In the event that the inability to conduct such due diligence comes about as a result of suspicious or unusual behaviour in suspicious or unusual circumstances, Platinum Life will be obliged to terminate the business relationship and report the person concerned to the FIC.

13. SANCTION SCREENING

- 13.1. All prospective policy owners are sanction-screened against the Consolidated UN Security Council's Sanctions list prior to sales stage. Should any matches be detected by the Company's Data Co-ordination and Analysis Department ("DCA"), such matches will be reported to the FIC by the FICA Compliance Officer.

14. FOREIGN POLITICALLY EXPOSED PERSONS, DOMESTIC POLITICALLY EXPOSED PERSONS AND PROMINENT INFLUENTIAL PERSONS, THEIR FAMILY MEMBERS AND THEIR KNOWN CLOSE ASSOCIATES

- 14.1. Should Platinum Life determine that a prospective policy owner is a domestic politically exposed person, a prominent influential person or a foreign politically exposed person, who is deemed a higher risk, the Company will first obtain senior management approval before entering into a business relationship with such a prospective policy owner. Reasonable measures will be taken to determine the source of wealth and verification of identity.

15. THE IMPLEMENTATION OF THIS RMCP

- 15.1. All staff members in all branches are to be made aware of the existence of this RMCP and each staff member will sign the declaration contained in their employment documentations confirming that they have read the RMCP and furnishing the undertaking to enforce its terms when dealing with all policy owners.
- 15.2. All staff members complete an annual FICA training tutorial which is accompanied by a quiz to test the staff member's knowledge.

16. APPROVAL OF THE RMCP

- 16.1. This RMCP, and all amendments hereto, is approved by the Company's EXCO.

17. OFFENCES AND PENALTIES

- 17.1. Failure to comply with this RMCP and/or the Financial Intelligence Centre Act is an offence punishable by an internal sanction of this company and by harsh fines and prison sentences in terms of the Act.

18. REASSESSMENT OF RISK

- 18.1. This RMCP shall be updated and reviewed annually. This shall however not detract from the duty of management to update and amend this RMCP as and when additional risks, or risk management steps are identified.