Anti-Money Laundering and Countering the Financing of Terrorism Policy

Version 1.8

Effective date:

This document contains 19 pages

Approved by the Board of Trustees on 28 May 2026

SIGNED BY THE CEO:

_____ Date: 01/06/26

Table of Contents

1. Document Administration

Name	Thandi Kuzwayo
Designation	Legal and Compliance Manager
Phone Number	011 685 6610
E-mail	thandiwek@gpf.org.za

1.1. Revision Summary

Policy Name	Version	Approval date
Anti-money laundering and countering the financing of terrorism policy	1.6	31 March 2022
Anti-money laundering and countering the financing of terrorism policy	1.7	26 April 2023
Anti-money laundering and countering the financing of terrorism policy	1.8	28 May 2026

1.2. Review

Frequency of review	Next review date	Last review date
Annual	**28 May 2029**	28 May 2026

1.3. Version Control

Reviewed by	Review date (dd / mm / yyyy)
Thandiwe Kuzwayo	26 April 2023
Thandiwe Kuzwayo	28 May 2026

2. Summary of Terminology

In this policy, unless the context indicates a contrary intention, the following words and expressions bear the meanings assigned to them and cognate expressions bear corresponding meanings –

2.1. Definitions and acronyms

2.1.1 **"ABC"** means Anti-Bribery and Corruption:

2.1.2 **"AML"** means Anti-Money Laundering;

2.1.3 **"Board"** means GPF Board of Trustees;

2.1.4 **"Bribery"** means the offering, giving, receiving, or requesting of something of value or gratification for the purpose of influencing the action of a person in authority in the execution of his/her public or legal duties;

2.1.5 **"Business Relationship"** means an arrangement between a client/service provider and GPF for the purpose of concluding transactions. Specifically, in the case of GPF, a business relationship begins at the start of the investment due diligence process and forms part of any Transaction;

2.1.6 **"CDD"** means Customer Due Diligence;

2.1.7 **"CEO"** means Chief Executive Officer;

2.1.8 **"CFT"** means Countering the Financing of Terrorism;

2.1.9 **"CIV"** means Customer Identification and Verification';

2.1.10 **"Client"** means a Natural Person or Juristic Person who enters into a business relationship with GPF in terms of which GPF provides funding to that Natural Person or Juristic Person;

2.1.11 **"Competent Authorities"** means a public authority, with designated responsibilities for combating terrorist financing and money laundering that has the authority to issue financial Sanctions against Natural Persons, Groups, Juristic Persons and/or Countries to prevent and suppress terrorism, terrorism financing and money laundering;

2.1.12 "**Corruption"** as per the definition in Section 3 of the Prevention and Combatting of Corrupt Activities Act No. 12 of 2004, means an offence of any person who directly or indirectly:

2.1.12.1. Accepts or agrees or offers to accept any gratification from any other person whether for the benefit of himself or herself or for the benefit of another person; or

2.1.12.2. Gives or agrees or offers to give to any other person any gratification whether for the benefit of that other person or for the benefit of another person; in order to act personally or by influencing another person to act, in a manner that amounts to the:

1.2.12.2.1. Illegal, dishonest, unauthorised, incomplete, or biased; or

1.2.12.2.2. Misuse or selling of information or material acquired in the course of exercising, carrying out or performing of any powers, duties or function arising out of a constitutional, statutory, contractual or other legal

obligation; that amounts to the abuse of a position of authority, a breach of trust; or the violation of a legal duty or a set of rules, designed to achieve an unjustified result; or that amounts to any other unauthorised or improper inducement to do or not do anything, is guilty of the offence of corruption.

2.1.13 **"CRA"** means Customer Risk Assessment;

2.1.14 **"CTR"** means Cash Threshold Report';

2.1.15 **"DPIP"** means Domestic Prominent Influential Person:

2.1.16 **"EDD"** means Enhanced Due Diligence;

2.1.17 **"Employee"** means employees of GPF, regardless of specific roles and responsibilities, Business Unit or location shall include:

2.1.17.1 Permanent Employees;

2.1.17.2 Employees on a fixed term contract;

2.1.17.3 Secondees;

2.1.17.4 Representatives of the GPF; and

2.1.17.5 Third party contractors.

2.1.18 **"Exposure"** means an act or omission whereby GPF has not met its statutory, supervisory and/or regulatory requirements which has led to a risk event;

2.1.19 **"FATF"** means Financial Action Task Force;

2.1.20 **"FIC"** means Financial Intelligence Centre;

2.1.21 **"FICA"** means Financial Intelligence Centre Act, No. 38 of 2001 as amended by Act, No. 1 of 2017;

2.1.22 **"FPPO"** means Foreign Prominent Public Official;

2.1.23 **"GPF"** means Gauteng Partnership Fund;

2.1.24 **"Juristic Person"** for the purposes of this Policy, means a local or foreign entity (whether incorporated or not) that includes a company, close corporation, a trust, fund, organisation, a partnership etc. as opposed to a Natural Person;

2.1.25 **"LCM"** means Legal and Compliance Manager;

2.1.26 **"Management"** means a person who is an executive committee member and who is responsible for executive management and oversight over a business operation within GPF;

2.1.27 **"ML"** means Money Laundering;

2.1.28 **"Monthly"** means in terms of the respective policies and MOS', a period of 30 days, and not a calendar month. Therefore, reporting, for example, should be performed every 30 days, from the date as decided by the LCM;

2.1.29 **"Natural Person"** means a human being, as opposed to a Juristic Person;

2.1.30 **"ODD"** means Ongoing Due Diligence;

2.1.31 **"Politically Exposed Persons ("PEPs")** is defined in FICA (Sections 21F-G) and recognises two (2 categories of PEPs, namely: 1. Domestic Prominent Influential Persons ("DPIPs"); and 2. Foreign Prominent Public Officials ("FPPOs");

2.1.32 **"PRA"** means Product Risk Assessment;

2.1.33 "**PRECCA**" means the Prevention and Combating of Corrupt Activities Act, 12 of 2004;

2.1.34 "**RBA**" means the Risk Based Approach;

2.1.35 "**RMCP**" means the Risk Management and Compliance Programme;

2.1.36 **"Sanctions"** means restrictive measures imposed by competent authorities against natural persons, groups[1], juristic persons and/or countries to prevent or suppress terrorism and terrorist financing. There are 3 Sanctions categories:

2.1.36.1 Comprehensive Sanctions - blanket sanctions against the entire country, e.g. the US sanctions against Cuba;

2.1.36.2 Limited Sanctions – limited to certain subject matters of target countries e.g. political regime, arms, rough diamonds, anti-terrorism, drug-trafficking; and

2.1.36.3 Specific Sanctions – targeted at specific persons e.g. individuals/entities of specific countries e.g. Kremlin elites, oligarchs, and Russia's political and national security leaders;

2.1.37 **"Service Provider"** means third parties that are Natural or Juristic Persons with whom GPF contracts for the rendering of specific services (e.g., suppliers, sub-contracted suppliers, third parties etc.);

2.1.38 **"SOP" means Standard Operating Procedures;**

2.1.39 **"Source of Funds"** means the origination of the funds that the client expects to use in concluding transaction/s in the course of the business relationship with GPF;

2.1.40 **"Source of Wealth"** refers to the activities that have generated the total net worth of the client's activities that produced the client/service provider's wealth. Wealth of a person could be as a result of a number of different activities over a period of time.

2.1.41 **"Suspicious Transaction Report ("STR")** means a confidential report submitted to a Competent Authority for a suspicious transaction or activity by a client or service provider, in terms of Section 29 of the FIC Act 38, 2001 as amended by Act 1 of 2017;

2.1.42 **"TF"** means Terrorist Financing;

2.1.43 **"Terrorist Property Report ("TPR")** means a confidential report submitted to a Competent authority in terms of Section 28A of the FIC Act, 38, 2001, for a suspicion of a transaction involving terrorist property owned or controlled by or on behalf of a client/service provider;

2.1.44 **"Transaction"** refers to a transaction between GPF and a Client/Service Provider:

2.1.44.1 Concluded in the course of a Business Relationship, or

[1] "Groups" are inclusive of Terrorist Groups, Religious Groups, Financial Groups, etc.

2.1.44.2 Other than a transaction concluded in the course of a Business Relationship (once off/single transaction);

2.1.44.3 Specifically, a transaction from the perspective of GPF will include amongst others:

2.1.44.3.1 Capital raising where public sector funds are utilised to leverage additional funding and facilitate capital flows into integrated sustainable human settlements;

2.1.44.3.2 Project preparation where GPF performs feasibility studies in order to attract sources of capital;

2.1.44.3.3 Project financing where GPF acts as a source of finance in order to attract additional funding sources;

2.1.44.3.4 Project implementation where GPF assists by providing an oversight role on the development of any housing development project;

2.1.44.3.5 Property development where plays the role of attempting to unlock the value of land for future development.

2.1.45 **"Ultimate Beneficial Owner ("UBO")** means in respect of a Juristic Person, a Natural Person who independently or together with another Natural Person, directly or indirectly:

2.1.45.1 Owns the Juristic Person; or

2.1.45.1 Exercises effective control of the Juristic Person.

2.2 Document Inventory

Document	Purpose
Risk Based Approach (RBA) Framework	The RBA provides a framework that will enable GPF to identify, assess and understand its money laundering and terrorist financing risks in relation to its business operations, funding products, and clients.
Anti-Money Laundering, Countering the Financing of Terrorism and Sanctions Governance Framework	The purpose of the Governance Framework is to support the AML/CFT Policy, PEP Policy and Sanctions Policy by indicating AML, CFT and Sanctions ownership as well as the associated main roles and responsibilities as the basis to integrate it into an effective AML, CFT and Sanctions risk management process.
Politically Exposed Persons Policy	The aim of this Policy is to prevent GPF from being misused to facilitate money laundering and establishes specific principles that apply unilaterally across GPF in respect of PEPs.
Sanctions Policy	This Policy provides an overview of the various standards within which GPF should operate in relation to matters regarding sanctions. The Policy is intended to assist the Board and Senior Management in the fulfilment of their respective responsibilities for oversight and management of GPF's sanction risks
Anti-Bribery and Corruption Policy	The Anti-Bribery and Corruption Policy provides ways to prevent acts of bribery and corruption within the organisation as GPF is obliged to comply with domestic legislation that gives effect to the prevention of bribery and corruption, such as the Prevention and Combatting of Corrupt Activities Act No. 12 of 2004.
Anti-Money Laundering / Countering the Financing of Terrorism Standard Operating Procedures (SOPs)	This document introduces standards, structures, procedures, and internal controls to ensure that AML/CFT statutory, supervisory, and regulatory requirements are satisfied.
Sanctions Standard Operating Procedures (SOPs)	This document is designed to provide standards, structures, procedures, and internal controls to ensure that GPF employees know how to identify and manage risks associated with sanctions.

3/ Introduction

2.2. GPF recognises the need to enforce a policy that will guide the organisation to prevent the abuse of its funding products for the purpose of laundering money from the proceeds of crime or for funding terrorism or terrorist related activities. GPF therefore maintains this Anti-Money Laundering ("**AML**") / Countering the Financing of Terrorism ("**CFT**") Policy in line with the AML and CFT statutory, supervisory, and regulatory requirements of the Republic of South Africa, together with international standards and guidance on best practice, mainly the FATF Recommendations.

2.3. GPF is committed to complying with this AML/CFT Policy in order to protect GPF from risks originating from financial crimes. GPF, in line with its commitment to practical and sound risk management of its organisation, embraces its statutory, supervisory, and regulatory obligations in relation to AML and CFT.

2.4. GPF has introduced standards, procedures, and internal controls to ensure that AML/CFT requirements are satisfied. The Board and senior management are committed to ensuring that the AML/CFT control regime, which consists of GPF's AML/CFT Policy and the accompanying AML/CFT Standard Operating Procedures ("SOPs") are implemented within GPF.

2.5. This Policy provides an overview of the various standards within which GPF should operate in order to discharge any AML/CFT regulatory requirements.

3. Policy Statement

3.1. GPF is committed to:

4.1.1. Building its business based on trust and integrity for the benefit of all its stakeholders, including its clients, employees, service providers, funders, partners, and regulators;

4.1.2. Conducting its business in compliance with statutory, supervisory, and regulatory requirements;

4.1.3. Complying with AML/CFT statutory, supervisory, and regulatory requirements by preventing, mitigating, and managing Money Laundering ("ML") and Terrorist Financing ("TF") risks;

4.1.4. Setting out roles and responsibilities of all internal stakeholders in relation to AML/CFT statutory, supervisory, and regulatory requirements;

4.1.5. Implementing policies, procedures and controls that protect GPF and its employees from potential reputational damage and criminal and administrative penalties; and

4.1.6. Dealing with employee transgressions of the AML/CFT applicable policies and procedures with GPF disciplinary procedures.

4. Scope of this Policy

4.1. This Policy applies to GPF including any partnership, associations, all funding structures, or other arrangements where GPF exercises management control. GPF and any such partnerships, associations or other arrangements should:

5.1.1. ascribe and align to this policy in order to mitigate any ML, TF and sanctions risks identified; and

5.1.2. implement and apply at all times the AML/CFT measures consistent with legislation and relevant applicable Financial Action Task Force ("**FATF**") recommendations.

5. AML/CFT Control Principles

5.1. Principle 1: Risk Management and Compliance Programme

6.1.1. GPF has developed, documented, maintained and implemented a programme for AML and CFT in accordance with Section 42 of the Financial Intelligence Centre Act No. 38, 2001 as amended by Act No. 1 of 2017 ("**FICA**"). The Risk Management and Compliance Programme ("**RMCP**") outlines the related AML and CFT policies, processes and procedures that enables GPF to comply with local legislation and international best practice, (i.e., the FATF Recommendations). The development of the RMCP has been performed in line with the guidelines that were issued by the Legal and Compliance Manager (LCM).

6.1.2. The RMCP is the foundation of the organisation's efforts to comply with applicable regulatory requirements under FICA. The RMCP includes a description of the Board of Trustees or senior management's accountability and the appointment of a person with adequate seniority and experience to assist with ensuring compliance with FICA.

6.1.3. The RMCP has been communicated widely throughout GPF to increase awareness of its existence and the effectiveness of its implementation. It is reviewed at regular intervals in order for it to remain relevant to the organisation's risk management strategy and framework.

5.2. Principle 2: Due Diligence

6.2.1. GPF should conduct due diligence from an AML/CFT and Sanctions perspective as described below and should obtain client/service provider information as is stipulated in the AML/CFT S O P prior to establishing a business relationship. Conducting customer due diligence from an AML/CFT and Sanctions perspective will assist GPF in mitigating the risk of conducting a business relationship with a high-risk client/service provider who might pose the risk of ML and TF. This due diligence performed from an AML/CFT and Sanctions perspective should form an integral

part of the investment due diligence process, as an investment due diligence would not be approved should the due diligence from an AML/CFT and Sanctions perspective not meet the requirements described within this policy and the associated AML/CFT and Sanctions SOP. Additionally, before commencing a business relationship, GPF should perform screening on its clients/service providers to ensure that the client/service provider is not a sanctioned individual or a PEP[2].

6.2.2. GPF may not, as prescribed in section 20A of FICA, establish a business relationship or conclude a single transaction with an anonymous client/service provider or a client/service provider with an apparent false or fictitious name.

6.2.3. **CDD**

6.2.3.1. Customer Due Diligence ("**CDD**") refers to the knowledge about a client that should enable an organisation to assess the extent to which the client exposes it to a range of risks, which include ML and TF. This information will provide GPF with the comfort that it knows who its client is and that its products are not being used as a means to launder money or to perform any other criminal activity.

6.2.3.2. In order to obtain such knowledge, CDD requires that the organisation identify and verify a potential client/service provider by way of obtaining the most recent Customer Identification and Verification ("**CIV**") information and this information would then need to be verified. The CDD requirements extend to instances where a person is acting on behalf of the client/service provider or where GPF transacts with another entity (natural/ juristic) on behalf of the client/service provider.

6.2.4. **EDD**

6.2.4.1. Enhanced Due Diligence ("**EDD**") is a process used to mitigate and protect against reputational damage during the on-boarding of higher-risk clients. EDD reports form part of a best-practice risk-based approach and provide a critical framework during the AML and Know your Customer ("**KYC**") compliance and on-boarding lifecycle that enables an organisation to comply with all necessary regulatory requirements.

6.2.1.1. GPF should perform EDD based on the risk rating of a client/service provider and during client/service provider on-boarding where the client/service provider presents a

[2] For the purposes of all GPF policies and minimum operating standards a PEP will either refer to a Domestic Prominent Influential Person ("DPIP") or a Foreign Prominent Public Official ("FPPO").

higher ML/TF risk. The risk rating of a client/service provider is determined according to GPF's RBA. For example, EDD measures should apply when GPF establishes that the client is a PEP or where the client/service provider has a high-risk occupation.

6.2.1.2. EDD entails obtaining additional information, which includes, but are not limited to:

6.2.1.2.1. Identifying and verifying the source of funds and source of wealth of the client/service provider by means of obtaining supporting documents;

6.2.1.2.2. Identifying and recording the nature and extent of the expected business and transactional activity of the client/service provider to assist in the identification of unusual activity which may lead to an STR;

6.2.1.2.3. Performing adverse media checks on all GPF's clients/service providers; and

6.2.1.2.4. Obtaining management approval for establishing the business relationship in line with GPF's approved delegation of authority.

6.2.5. **ODD**

6.2.5.1. Ongoing Due Diligence ("**ODD**") is a continuous process of monitoring and periodic review of client information for new ML and TF risks after initial on-boarding is completed. GPF should maintain the accuracy of their client/service provider information that may change over the course of a business relationship. CDD information should be updated periodically, in line with the risk rating of the client/service provider, and screening should be performed using the updated information once it has been obtained.

6.5.5.2. As part of the ODD process, the information and documentation obtained during the CDD stage should be reviewed and updated periodically, in line with the frequencies set out in the table below, in order to ensure that the client/service provider's information and documentation held by GPF is up to date and accurate. The client/service provider should also be risk rated to determine if their original risk rating is consistent with their current risk profile. ODD should be performed on all clients/ service providers (based on their ML and TF risk rating) with higher risk clients/ service providers requiring more frequent reviews. The ODD requirements are set out in the GPF AML/CFT SOP that forms part of the set of documents listed in the document inventory in section 2.2

6.2.5.2. The frequency of reviews is set out as follows:

Client/service provider rated as high risk	ODD should be performed annually.

Client/service provider rated as medium risk	ODD should be performed every two (2) years from last review.
Client/service provider rated as low risk	ODD should be performed when there is evidence of a change in the client profile in line with the Risk Based Approach Methodology.

6.2.5.3. A trigger event may occur outside of the set review frequency that may require a review outside of the pre-determined timeframes above. Examples of trigger events are set out in the GPF AML/CFT SOP.

5.3. Principle 3: Risk-Rating of Clients / Service Providers

6.3.1. Not all clients/service providers pose the same ML and TF risk. In order to establish the risk posed by a customer, a risk assessment should be performed.

6.3.2. GPF should perform a risk assessment when on-boarding a client/service provider. As per GPF's RBA Framework, this should occur on an ongoing basis to ensure that the clients/service providers are risk rated correctly throughout their relationship with GPF. GPF should take appropriate action to ensure that appropriate and adequate resources are allocated to the different customer risk categories, i.e., high, medium, and low risk. In essence, high-risk situations will require a significant number of resources allocated due to the need to perform EDD and rigorous monitoring of transactions throughout the business relationship, whereas low risk situations will require less onerous CDD requirements. An accurate allocation of resources will assist in ensuring that risks are analysed, managed, and reported efficiently where required.

6.3.3. The risk categories, as determined by GPF, are as follows and a detailed explanation can be found in the AML/CFT SOP:

High Risk	Client/service providers should be risk rated as high if they pose significant risk of ML/TF to GPF. This, however, does not prohibit GPF from entering into a business relationship with the client/service provider. Where a client/service provider has been identified as high risk, they should be subjected to enhanced due diligence.
Medium Risk	These clients/service providers are required to be subjected to standard due diligence requirements.

Low Risk	These clients/service providers are required to be subjected to standard due diligence.

6.4 Principle 4: Reporting obligations

6.4.1. GPF's LCM should ensure that all reporting obligations are complied with, within the prescribed timeframes as set out in FICA. As an accountable institution in terms of schedule 1 of FICA, GPF is required to file the following reports, where appropriate:

6.4.1.1. Cash Threshold Reports ("**CTR**s") in terms of section 28 of FICA;

6.4.1.2. Suspicious Transactions Reports ("**STR**s") in terms of section 29 of FICA; and

6.4.1.3. Terrorist Property reports ("**TPR**s") in terms of section 28A of FICA.

6.4.2. GPF is required to register on the FIC's goAML website to file reports.

6.4.3. Reference should be made to the AML/CFT SOP, which sets out the procedure to be followed when submitting an STR report together with the relevant information on the FIC's goAML platform.

6.5. Principle 5: Responding to regulatory requests

6.5.1. GPF undertakes to co-operate fully with the FIC and all other supervisory bodies and competent authorities, and to respond promptly, immediately, to any of the following:

6.5.1.1. Directives from the FIC;

6.5.1.2. Regulatory Inquiries;

6.5.1.3. Deficiency Letters;

6.5.1.4. Notices to appear;

6.5.1.5. Requests to provide documentation; and

6.5.1.6. Any other requests from the FIC or a supervisory body or competent authority.

6.5.2. Subsequently where GPF receives a request from a supervisory body or competent authority, GPF is required to respond immediately or within the prescribed timeframes as directed by the supervisory body or competent authority. The procedures for dealing with regulatory requests are set out in the AML/CFT SOP.

6.6. Principle 6: Training and awareness

6.6.1. AML/CFT training assists organisations in mitigating the risk of non-compliance with

regulatory requirements and in implementing measures to minimise the exposure to money laundering and fines imposed by regulators for non-compliance. Employees should be made aware of their compliance responsibilities within the organisation. All GPF employees should be made aware of and have access to this Policy, AML/CFT SOP, related policies, standards, frameworks, procedures, and controls applicable to GPF. The LCM is required to provide the Board, Management, appropriate committees, and employees with all relevant AML/CFT training.

6.6.2. The LCM should ensure that the appropriate AML/CFT general awareness and role specific training is rolled out to the organisation. All GPF employees, including Board members and Management should complete the AML/CFT general awareness training. The Compliance Officer will be responsible for maintaining training records and escalating training breaches to the LCM. Reference should be made to the AML/CFT SOP which provides an in-depth overview of the training which will be conducted within GPF.

6.7. Principle 7: Records management and document retention

6.7.1. GPF is required to keep AML/CFT records of a client/service provider as per Section 22, 22A, 23, 24 and 25 of FICA as this will ensure that GPF complies with regulatory requirements and it will enable GPF to produce such records upon request by a regulator, supervisory body, or competent authority. Records must be kept for a period of 5 (five) years from the termination of the business relationship with a client/service provider. The records must be easily accessible and readily available to the FIC and relevant supervisory body or competent authority for the purpose of investigation. The records that are required to be kept are as follows:

6.7.1.1. All CDD information:

6.7.1.1.1. The client/service provider's CIV information;

6.7.1.1.2. Identity and authority of the client/service provider acting on behalf of another person;

6.7.1.1.3. Identity and authority of another person acting on behalf of the client/service provider;

6.7.1.1.4. The nature of the business relationship or transaction;

6.7.1.1.5. For a single transaction: the amount of the transaction as well as the parties involved;

6.7.1.1.6. For a business relationship: All transactions conducted across all accounts, the nature of the business relationship, the intended purpose of the business relationship and the

client's source of funds;

6.7.1.1.7. All documents or copies related to this CDD; and

6.7.1.1.8. The details of the person collecting this information.

6.7.1.2. STR reports made to the FIC (these reports should include those made on the goAML platform);

6.7.1.3. STRs that were investigated but were not reported to the FIC (including the reasons why they were not reported); and

6.7.1.4. Records relating to the training of Employees.

6.7.2. Records may be stored in electronic format. All records should be easily accessible internally and any third-party retrieval requests should be in accordance with GPF AML/ CFT SOP.

6.8. Principle 8: Disclose Exit and Prevent Re-Entry

6.8.1. GPF should document the criteria and governance arrangements to exit a client/ service provider, whilst giving due consideration to ML and TF risks as well as reputational risks. GPF should not enter into a business relationship with a client/ service provider and should terminate a business relationship with an existing client/ service provider in instances where:

6.8.1.1. GPF cannot apply the appropriate CDD, ODD or EDD standards or take appropriate measures to mitigate the risk;

6.8.1.2. The client/service provider is on a sanctions list;

6.8.1.3. The client/service provider is classified as "prohibited" in terms of GPF's risk categorisation principles as set out in GPF's RBA; and

6.8.1.4. The client/service provider poses a risk that is beyond the risk appetite of GPF.

6.8.2. If GPF decides to exit a business relationship, then GPF should consider whether or not the termination warrants the raising of an STR. The reason for exiting the business relationship should be maintained in the client/service provider's record. All client/ service provider records should be maintained for a period of 5 (five) years as mentioned in the previous principle.

6.8.3. When GPF exits or declines a business relationship for reasons relating to ML or TF risk, reasonable steps should be taken to prevent the customer from entering into a new business relationship with the organisation. GPF may re-instate a business relationship only where the circumstances of the client/service provider change and GPF can satisfy all regulatory requirements relating to the client/service provider, and where the risks originally identified no longer exist.

6.8.4. A register of all declined or exited clients/service providers should be maintained by the Compliance Officer in a centralised GPF Watchlist.

6.9. Principle 9: Management Reporting and Information

6.9.1. The LCM should report, on a quarterly basis, to the Board, Audit and Risk Committee and executive committee who deal with GPF's compliance with AML/CFT statutory, supervisory, and regulatory requirements. This report at a minimum should include:

6.9.1.1. The number of clients/service providers on-boarded, whether compliant or non-compliant (including an overview of their risk ratings);

6.9.1.2. The number of clients/service providers exited or declined, including the reasons for the exit or decline;

6.9.1.3. The number of PEPs in the respective client/service provider databases;

6.9.1.4. The total number of STRs reported including the cumulative year to date and previous year's statistics;

6.9.1.5. A list of clients/service providers for which EDD procedures have been completed in the respective month;

6.9.1.6. Training statistics and plans;

6.9.1.7. A summary of all reports made to the FIC including:

6.9.1.7.1. number of STRs reported and red flags indicating the need to report;

6.9.1.7.2. relevant products and client/service provider types which were involved in these reports;

6.9.1.7.3. the number of PEPs, if any, who were a part of these reports; and

6.9.1.7.4. An update on the monitoring plans in place and the results of such (if available at the time of reporting).

7. Breach of this Policy

7.1. It is the responsibility of every employee to comply with this policy and failure to do so could amount to gross misconduct and a material breach of the contract of employment.

8. Dispensations

8.1. A dispensation is a request to the LCM to temporarily deviate from the prescribed AML/CFT requirements. Requests for dispensation may only be granted in exceptional circumstances. Any

such requests for dispensation from AML/CFT requirements must be approved in writing by the LCM and are only valid for 30 (thirty) calendar days.

8.2. All dispensations must be recorded and maintained by the LCM in a central location for audit purposes.

9. Exemptions

9.1. An employee may request for a temporary exemption of a specific requirement of this policy from the LCM. An exemption may be appropriate where further time is required beyond the effective date for the implementation or embedment of:

9.1.1. A new policy; or

9.1.2. A material change to an existing policy; or

9.1.3. A new process/control; or

9.1.4. An amended process/control.

9.2. During the temporary exemption period, interim controls should be implemented as proposed in the temporary exemption request to the LCM.

9.3. The employee must request a dispensation in advance and prior to the relevant effective date (as specified above) from the LCM, which must be supported by a detailed action plan to show how the risks of non-compliance with the particular AML / CFT element in the dispensation or exposure will be mitigated.

9.4. GPF may only continue with business as usual with this client/service provider upon receiving written approval from the LCM. The LCM must investigate all reported exposures of the PEP policy and report such exposures to the CEO of the Board.

9.5. The granting and duration of an exemption is at the discretion of the LCM.

10. Monitoring, Review and Compliance

10.1. Policy Review

10.1.1 This policy is subject to review every three years (or whatever period which is no longer than 3 years) or earlier if deemed necessary by the GPF, to ensure alignment with applicable resolutions, regulatory requirements, and prevailing market conditions.

10.1.2. The Policy shall remain in full force and effect unit it is reviewed, amended, or revoked by GPF.

10.1.3. Confirmation of the review will be provided in line with the GPF governance process and where relevant include the Audit and Risk Committee.

10.2. Policy Amendments

10.2.1. No amendment(s) may be made to any section(s) of this policy without such amendment(s) first being discussed and validated against prevailing acts, standards, best practises, and regulations.

10.2.2. Policy amendments will need to be approved through the relevant GPF governance forums including the Audit and Risk Committee.

10.3. Policy Compliance

10.3.1. Legal and Compliance Unit will provide compliance assurance and determine whether the approved policy provisions are put in place in each Business Unit.

10.3.2. The Audit and Risk Committee will be provided with feedback on the effectiveness to which the Business Unit has implemented the requirements of the policy.

11. Approval

11.1. This policy is approved by the Board on recommendation from the Audit and Risk Committee.