



AML: RISK MANAGEMENT & COMPLIANCE PROGRAMME

THE PRIME FINANCIAL SERVICES GROUP

28 PETER PLACE
LYME PARK
SANDTON
2060



CONTENTS

1. APPLICATION OF THE RISK MANAGEMENT & COMPLIANCE PROGRAMME	2
2. PURPOSE & SCOPE OF RISK MANAGEMENT & COMPLIANCE PROGRAMME	2
3. DEFINITIONS.....	2
4. PRACTICAL IMPLEMENTATION OF THE RISK MANAGEMENT COMPLIANCE PROGRAMME	3
BASIS OF PREPARATION & IMPLEMENTATION	3
ANONYMOUS CLIENTS & PERSONS ACTING UNDER FICTITIOUS NAMES.....	4
IDENTITY ESTABLISHMENT & VERIFICATION PROCESSES	4
FUTURE TRANSACTIONS & CLIENT REVIEW	6
ADDITIONAL DUE DILIGENCE MEASURES & ULTIMATE BENEFICIAL OWNERSHIP.....	6
ONGOING DUE DILIGENCE	7
COMPLEX AND UNUSUAL TRANSACTIONS	7
DOUBTS CONCERNING THE VERACITY OF CUSTOMER DUE DILLIGENCE INFORMATION.....	8
INVESTIGATING AND REPORTING SUSPICIOUS TRANSACTION ACTIVITY	8
TERMINATING BUSINESS RELATIONSHIPS	9
DETERMINATION OF PEP STATUS	9
APPLICATION OF SIMPLIFIED DUE DILIGENCE MEASURES.....	9
RECORD KEEPING	9
OTHER REPORTABLE ACTIVITIES	10
REPORTING TO THE FIC AND PROVIDING NECESSARY INFORMATION.....	11
IMPLEMENTATION OF THE RISK MANAGEMENT COMPLIANCE PROGRAMME.....	12
ANNEXURE 1: CLIENT RISK ASSESSMENT	13
ANNEXURE 2: ACCEPTABLE SUPPORTING DOCUMENTATION	17
ANNEXURE 3: RISK ASSESSMENT & ONBOARDING PROCESS OVERVIEW	28
ANNEXURE 4: SAMPLE INTERNAL DISCLOSURE FORM FOR SUBMISSION TO THE MLRO.....	29
ANNEXURE 5: SECTION 42 BREAKDOWN.....	31
ANNEXURE 6: GUIDANCE NOTES INCLUDED IN RMCP	34
ANNEXURE 7: OWNERSHIP, APPROVAL & REVISION HISTORY.....	35
POLICY OWNER	35
POLICY APPROVAL.....	35
POLICY REVISION.....	35

1. APPLICATION OF THE RISK MANAGEMENT & COMPLIANCE PROGRAMME

- 1.1 This Risk Management & Compliance Programme is applicable to the legal entities within the Prime Financial Services Group (hereinafter referred to as “the Group”), as shown on the Group’s corporate organogram and amended from time to time.

2. PURPOSE & SCOPE OF RISK MANAGEMENT & COMPLIANCE PROGRAMME

- 2.1 The purpose of the Risk Management & Compliance Programme as contained herein is to formally document the Group’s commitment to compliance with the Financial Intelligence Centre Act of South Africa as amended from time to time as well as compliance with the requirements of any associated Anti-Money Laundering and Counter-Terrorism Financing legislation.

3. DEFINITIONS

- 3.1 **Accountable Institution:** An accountable institution is any person or entity as described in Schedule 1 of the Financial Intelligence Centre Act No. 38 of 2001 who must ensure adherence to the legal requirements and responsibilities as set out therein.
- 3.2 **Act:** Financial Intelligence Centre Act No. 38 of 2001 (also known as “FICA”), as amended from time to time, including the FIC Amendment Act of 2017.
- 3.3 **AML:** Anti-Money Laundering.
- 3.4 **CTF:** Counter-Terrorism Financing.
- 3.5 **Customer Due Diligence:** The steps and procedures taken to identify and verify clients. For the purposes of abbreviation, it is also referred to as “CDD”.
- 3.6 **Financial Action Task Force:** The Financial Action Task Force is an intergovernmental organization founded in 1989 on the initiative of the G7 to develop policies to combat money laundering. In 2001, its mandate was expanded to include terrorism financing. For the purposes of abbreviation, it is also referred to as “FATF”.
- 3.7 **Financial Intelligence Centre:** The Financial Intelligence Centre is South Africa’s national centre for gathering, analysis and dissemination of financial intelligence. It was established to identify proceeds of crime, combat money laundering and the financing of terrorism and, in so doing, has a primary role to protect the integrity of South Africa’s financial system. For the purposes of abbreviation, it is also referred to as “FIC”.
- 3.8 **Law enforcement Agencies:** Financial Intelligence Centre, South African Police, National Prosecuting Authority, National intelligence agencies, South African Revenue Services, the Independent Police Investigative Directorate, Special Investigative Units, and supervisory bodies including the Financial Sector Conduct Authority and Prudential Authority.
- 3.9 **MLRO:** Money Laundering Reporting Officer.
- 3.10 **Money Laundering:** Any process which gives the proceeds of unlawful activities the appearance that they originate from a legitimate source.
- 3.11 **Non-Investment Related Business:** This term is used to refer to business relationships between the Group and other entities and/or natural persons (including suppliers, service providers and non-investment business) which enable the Group to pursue its core business as a financial services provider.

3.12 **PEP¹**: Politically Exposed Persons refer to any individuals who are or have in the past been entrusted with prominent functions in a particular country. The prominent function in question is determined by definitions contained within the Act and any subsequent amendments thereto published by the Financial Intelligence Centre from time to time. The definition includes those who have held prominent functions within the Republic of South Africa (i.e. Domestic Politically Exposed Persons) and those who have held prominent functions internationally (i.e. Foreign Politically Exposed Persons). A PEP status can also be extended to the family members and close associates of such a person, and can include:

- i) A spouse, civil partner or life partner;
- ii) A previous spouse, civil partner or life partner (if applicable);
- iii) Children and step children;
- iv) Parents;
- v) Siblings and step siblings;
- vi) Sexual partners outside the family unit (i.e. girlfriends, boyfriends and/or mistresses);
- vii) Prominent members of the same political party, civil organisation, labour or employee union;
- viii) Business partners and associates (especially those that share in beneficial ownership); and
- ix) Any individual who has sole beneficial ownership of a corporate vehicle set up for the PEP.

3.13 **POPIA**: Protection of Personal Information Act No. 4 of 2013

3.14 **RMCP**: Risk Management & Compliance Programme.

3.15 **SAR**: Suspicious Activity Report

3.16 **STR**: Suspicious Transaction Report.

4. PRACTICAL IMPLEMENTATION OF THE RISK MANAGEMENT COMPLIANCE PROGRAMME

BASIS OF PREPARATION & IMPLEMENTATION

4.1 As required by Section 42 of the Act, the Group has designed and implemented an RMCP to identify, assess, monitor, mitigate and manage the money laundering or financing of terrorism risks associated with its products and/or service offerings. The information to follow will detail the practical implementation of the RMCP in pursuit of this goal across its operating environment.

ESTABLISHMENT OF BUSINESS RELATIONSHIPS

4.2 When engaging with prospective clients to establish a business relationship (be it a continuous or once-off in nature)², the Group will establish and verify the identity of such prospective clients and will take additional due diligence measures as necessary when dealing with legal persons, partnerships, and trusts.

4.3 Should a client act on behalf of another person, the Group, will establish and verify the identity of that other person and the client's authority to establish a business relationship or conclude single transactions on their behalf.

4.4 If another person is acting on behalf of a client, the Group will establish and verify the identity of that person and the person's authority to act on behalf of the client.

¹ While South African legislation currently stipulates a different approach for the identification of PEPs, the Group has chosen to apply the FATF standard whereby if a person has held a domestic or foreign prominent position, this position (whether past or present) will always be taken into account when the respective potential client is subjected to the Risk Assessment Model.

² Given the nature of the Group's business activity, both long-term clients and those who wish to conclude a once-off transaction/investment are subject to the same processes.

- 4.5 The Group will only establish a business relationship with prospective clients or other persons once the client diligence and risk rating process is completed. Should any prospective client or any other person refuse to provide CDD documentation, the Group will not establish a business relationship or conclude a transaction, and the refusal of the client or any other person to provide CDD documentation will be reported to the MLRO for investigation and possible suspicious and unusual transaction reporting.

ANONYMOUS CLIENTS & PERSONS ACTING UNDER FICTITIOUS NAMES

- 4.6 The Group will not establish a business relationship or conclude a single transaction with an anonymous client or a person who transacts under an apparent false or fictitious name.
- 4.7 While not specifically addressed within South African legislation, the Group and its Associates shall have no dealings with “shell banks”. Defined as a local or foreign banking institution with no physical address, the Group does not deal directly with such institutions and such institutions will not be able to pass the Group’s CDD requirements.

IDENTITY ESTABLISHMENT & VERIFICATION PROCESSES

4.8 Risk Assessment Model

The Group shall perform a risk assessment on every prospective client and/or other person, assigning them a risk rating. The Group has chosen a point scoring system to facilitate the risk assessment, allowing for the weighting of various risk parameters. The cumulative score of a risk assessment will determine the risk rating of a prospective client and the CDD measures implemented thereafter.

- 4.9 The risk assessment requires prospective clients to complete an application form (including the provision of any supporting documents thereto), which will provide many of the key data points critical to the risk assessment methodology, namely:
- i) **Nature of Person:** The nature, size, and complexity of the client and/or other person.
 - ii) **Type of Product:** The risks associated with the products being offered.
 - iii) **Transaction Amount:** The higher the amount, the higher the risk.
 - iv) **Sources of Funds:** Legitimate vs. illegitimate sources.
 - v) **Jurisdiction:** The geographical jurisdiction of the client and/or other person.
 - vi) **Status & Sanctions:** Confirmation of PEP status and any sanction list data (via DocFox).³
 - vii) **Adverse Media:** Review of any adverse media on the prospective client (via DocFox)

- 4.10 Once finalised, a risk assessment will culminate in a risk rating, which will determine the CDD measures (including any enhanced CDD measures) to verify the identity of a prospective client and/or other person.
- 4.11 Any prospective client and/or other person who receives a “High Risk” classification will be automatically subject to enhanced CDD measures. Such measures will include verification of both “source of funds” and “source of wealth” and final acceptance of any High-Risk client will be subject to the approval of the Board of Directors. Further information on the Risk Assessment Model and the application thereof to different types of clients, please refer to [Annexure 1](#).

4.12 Client Due Diligence

Once a prospective client and/or other person has received their final risk rating, they will also need to provide all necessary CDD information and/or documents to verify their identity. Base document requirements are outlined in the applicable application previously provided by the prospective client or their appointed broker. Dependent on the risk rating assigned, additional documentation may be required. [Annexure 2](#) provides a list of acceptable CDD documents which the prospective client can provide.

³ During the sanction screening process (which includes screening against proliferation financing), if any prospective client is identified against a sanction list (facilitated through DocFox), such a client will not be onboarded. If an established client is identified against a sanction list at any time after onboarding, the Group shall freeze the assets of such a client, cease all business with the same, and file the necessary reports with the Financial Intelligence Centre

- 4.13 If a prospective client and/or other person receives a “High Risk” classification, enhanced CDD measures must be undertaken, and documentation requested. These measures are designed to mitigate and manage the higher risk of potential money laundering and terrorist financing activity.
- 4.14 Enhanced due diligence procedures will be undertaken on a case-by-case basis and will include obtaining additional information concerning the following:
- i) **Source of Funds:** This refers to the origin of particular funds or assets which are the subject of the business relationship between the Group, the prospective client and the transactions that the Group are required to undertake on the client’s behalf (e.g. the amounts being invested or redeemed). The additional information provided will verify where such monies are coming from.
 - ii) **Source of Wealth:** This refers to the origin of the prospective client’s financial or total net worth (i.e. the activities which have generated and contributed to the client’s funds, properties and assets). The additional information provided will verify both the origin of the clients wealth and provide insight into the nature of activities generating the same.
- 4.15 Further information on enhanced and ongoing due diligence measures shall be discussed in paragraphs 4.25 to 4.26.
- 4.16 **Third Party Reliance: Look Through Principal**
In cases where a prospective client is a regulated financial institution applying AML standards that are at least equivalent to that of the Republic of South Africa⁴ and they are acting on behalf of underlying investors in pooled investment vehicles (e.g. collective investment schemes, protected cell companies, nominees or other similar structures where underlying investors do not exercise control over the client), the following processes are implemented:
- i) **Provision of KYC Information:**
The client institution (acting in its capacity as an accountable institution) can collect KYC information concerning the underlying investors and provide such information to the Group for risk assessment in line with our established Risk Assessment Models. Such information must include (as necessary):
 - a. Identification of the underlying investor and other required particulars
 - b. Verification of the underlying investor and other required particulars
 - c. Additional information concerning source of funds, source of wealth and geographic location.
 - ii) **Conduct Risk Assessment in terms of the RMCP:**
The Group shall use the information provided by the client institution to conduct its own risk assessment on the underlying investor as an accountable institution. Such risk assessments will be conducted on the underlying investors when any of the following “trigger” events:
 - a. Opening new accounts
 - b. Purchasing new products (in addition to those previously purchased)
 - c. Changing banking particulars
 - d. Changing debit order arrangements
 - e. Changing previously established withdrawal arrangements
- 4.17 In addition to providing a written confirmation, the Group will ensure that it has free and easy access to the underlying investor CDD documentation and that such documentation is readily available to the FIC and other supervisory bodies (as needed) to facilitate their necessary functions in terms of the Act.

⁴ In cases where the prospective client (acting on behalf of underlying investors) resides in a foreign jurisdiction, the Group will review AML risk of that jurisdiction. Countries with strategic deficiencies in the fight against money laundering and the financing of terrorism (e.g. countries identified by FATF, vulnerable to corruption or politically unstable) shall be subject to a higher degree of scrutiny and CDD requirements.

4.18 **Rejection of Applications**

Following a prospective client receiving a final risk score and providing the necessary CDD documentation, their application is assessed and either rejected or accepted. Should the application be rejected for reasons other than suspicious circumstances and/or activity, the prospective client will be advised of the reasons for the rejection and a copy of such communication will be noted in the application record.

4.19 Should a prospective client's application be rejected because of suspicious circumstances and/or activity, the matter, the MLRO will be consulted before any further action or communication is taken. Should a communication of rejection be issued to the prospective client, such communication will not reference the reasons for the application's rejection (i.e. the suspicious circumstances and/or activity).

4.20 **Acceptance of Applications & Onboarding**

Following a prospective client receiving a final risk score and providing the necessary CDD documentation, if a prospective client's application is accepted, the client will be onboarded as follows:

- i) **Low/Medium Risk Clients:** Low and Medium Risk clients are onboarded in line with standard processes.
- ii) **High Risk Clients:** High Risk clients are onboarded after receiving written approval from management confirming the client's acceptance.

4.21 **Summarised Process Overview**

For ease of reference, a graphical summary of the complete Risk Assessment & Onboarding process is available in [Annexure 3](#).

FUTURE TRANSACTIONS & CLIENT REVIEW

4.22 Given the nature of the Group's business activity, being the investment and administration of client funds into various investment vehicles (including collective investment scheme portfolios and retirement vehicles), it is accepted that clients engage the Group for these same services. When such services are no longer required, it is typical for clients to disinvest their funds from the associated products and take their investment business elsewhere. Nevertheless, a comprehensive review process has been implemented by the Group as follows:

- i) When clients are accepted, their initial risk classification (which includes the basis for the business relationship and the product(s) the client may invest in) provides the basis for determining client review periods as follows:
 - a. **Low Risk:** Every 5 years (60 months).
 - b. **Medium Risk:** Every 3 years (36 months).
 - c. **High Risk:** Every year (12 months).
- ii) During the review, the client's financial needs are reassessed, the final risk score adjusted as needed, and the necessary due diligence conducted, and KYC documentation obtained.

ADDITIONAL DUE DILIGENCE MEASURES & ULTIMATE BENEFICIAL OWNERSHIP

4.23 As required by the Act, the Group has implemented several additional due diligence measures when obtaining KYC documentation from various legal entities to determine the ultimate beneficial ownership of such entities.

4.24 Ultimate beneficial ownership of a legal entity is determined as follows:

- i) **Shareholding:** The shareholding⁵ in a given legal entity provides a good indication of beneficial ownership. Within the financial services industry, it is generally accepted that any person holding 25% or more in a legal entity exercises sufficient control to be deemed an ultimate beneficial owner and shall be subject to further KYC measures as per [Annexure 2](#).
- ii) **Managerial Control:** In cases where no person holds at least a 25% shareholding in the legal entity, ultimate beneficial ownership is deemed to be the person or persons exercising effective managerial control over the entity. Such persons shall be subject to further KYC measures as per [Annexure 2](#).

ONGOING DUE DILIGENCE

- 4.25 The Group will conduct ongoing due diligence in respect of all its clients. Due diligence will include the monitoring of transactions undertaken by clients throughout the course of their business relationship with the Group and ensuring that all client-related information is kept current and up-to-date.
- 4.26 In addition to maintaining CDD documentation, ongoing due diligence shall also encompass the following:
- i) Review client transactions to ensure that these are consistent with known knowledge of the client and their risk profile.
 - ii) Ensuring that additional CDD measures are applied to higher risk business relationships, which can include any of the following:
 - a. Undertaking additional KYC reviews to those prescribed by the risk profile.
 - b. Updating KYC more frequently.
 - c. Subjecting KYC to a higher degree of scrutiny and analysis.
 - d. Applying lower monetary thresholds for reporting to client transactions and activity.
 - e. Facilitating KYC reviews through persons not involved in the client relationship.

COMPLEX AND UNUSUAL TRANSACTIONS

- 4.27 While conducting due diligence, the Group shall monitor client activity for any complex, large or unusual transactions. Such activity presents a higher risk and while there is no fixed definition for such transactions, several “red flags” have been identified which would be indicative of a transaction requiring further scrutiny. These “red flags” include (but are not limited to) the following:
- i) Transactions not in keeping with a client’s typical business activity (e.g. abnormally large transaction size and frequency or the involvement of a new and unknown third party).
 - ii) Transaction funds originating from or destined for an unusual location in the context of the client business relationship.
 - iii) A sudden surge of transaction activity after a period of relative dormancy.
 - iv) Transactions linked with “advisory” or “consulting” services that have no connection with the client’s business activities.
 - v) The involvement of charitable / political donations or sponsorships.
 - vi) Transactions connected with countries or jurisdictions that have significant levels of corruption or are linked to the financing and supporting of terrorist activities.

⁵ For the purposes of this section, the term “shareholding” will be used when referring to various legal entities and encompasses the concept of holding shares, partnership interest, member contribution and any other form of interest that gives another person (both legal and natural) voting rights in the legal entity.

- 4.28 If such transactions are noted, the Group will compile all relevant and written information related thereto and, after further assessment, a decision will be made whether or not to report the activity as a suspicious transaction. The reporting of suspicious transactions shall be discussed further in paragraphs 4.32 to 4.39.

DOUBTS CONCERNING THE VERACITY OF CUSTOMER DUE DILLIGENCE INFORMATION

- 4.29 If the Group at any time should doubt the veracity of CDD provided by a prospective client during onboarding or during a CDD review of an established client, the Group reserves the right to request new CDD documentation from the client in question.
- 4.30 If doubts concerning the veracity of CDD documentation persist even after the client has provided new documents, the client shall be classified as “High Risk” and shall be subject to enhanced due diligence procedures and documentation requirements as per [Annexure 2](#).
- 4.31 If a client at any time refuses to comply with a request for new CDD documentation, this will result in the immediate rejection of a client application (in the case of a prospective client), the halting of any transactional processing (in the case of an established client), and the possible filing of an SAR and/or STR (in both cases).⁶

INVESTIGATING AND REPORTING SUSPICIOUS TRANSACTION ACTIVITY

- 4.32 Suspicious transactions are transactions (either actual, proposed or attempted) which give rise to reasonable suspicion that they may:
- i) Involve the laundering of money or the proceeds of criminal activity.
 - ii) Involve funds and/or property linked to or used for the terrorist financing.
 - iii) Have no apparent economic justification, business purpose or lawful objective.
 - iv) Facilitate the avoidance of reporting obligations as set out in the Act.
 - v) Be linked to a tax evasion investigation.
 - vi) Be linked to persons and entities prohibited under the Security Council of the United Nations.
- 4.33 As previously highlighted in this policy document, other circumstances (such as the refusal to provide CDD documentation, or the inclusion of complex and large transactions) may also give rise to suspicion. In such circumstances, the following processes are implemented:
- 4.34 **Internal Investigation & Disclosure**
When a transaction or activity related thereto, the Group will launch an internal investigation, subjecting the transaction or activity to scrutiny. In doing so, the Group may apply enhanced CDD measures, provided that such action does not alert the associated client (prospective or otherwise).
- 4.35 Once the transaction or activity has been scrutinised, and if suspicions persist despite further investigation, an Internal Disclosure Report (as contained in [Annexure 4](#)) detailing the pertinent details of the transaction or activity will be filed with the MLRO.⁷
- 4.36 Following the receipt of an Internal Disclosure Report, the MLRO will make a final assessment of the matter, assessing whether the transaction or activity is indeed suspicious and therefore necessitating disclosure to the applicable AML/CTF Regulatory Authorities.

⁶ These outcomes also apply to instances where prospective or existing clients refuse to provide personal or special information (as defined by the Protection of Personal Information Act) necessary to comply with the provisions of the Act, as communicated by the FIC on the 30th of November 2022.

⁷ While the MRLO is ultimately responsible for the review of Internal Disclosure Reports and the reporting of suspicious transactions or activity to the applicable AML/CTF Regulatory Authorities, in the event of their absence, the deputy MLRO may discharge these same duties.

4.37 Filing of Suspicious Transaction Reports (STRs) and Suspicious Activity Reports (SARs)

STRs and SARs shall be lodged with the applicable AML/CTF Regulatory Authorities in the prescribed form and within the prescribed time limits. Such submissions shall include the following information (as required):

- i) The identified party / parties to the transaction and/or activity.
- ii) The financial amount and nature of the transaction and/or activity.
- iii) The circumstances which gave rise to suspicion.
- iv) The business relationship between the suspected party and affected institutions or professions.
- v) A voluntary disclosure as to the origin, source and/or destination of the financial proceeds.
- vi) The impact of the suspicious transaction and/or activity on the financial soundness of the Group.
- vii) The names of all Group employees, agents or officers dealing with the transaction and/or activity.

4.38 All STRs and SARs must be filed as soon as practicable with the applicable AML/CTF Regulatory Authorities, but no later than 15 working days from the date on which the MLRO became aware of the transaction and/or activity, which they had reason to view as suspicious.

4.39 Execution of Reported Transactions

The Group may continue to facilitate and execute a suspicious transaction, and unusual transaction, or a transaction exceeding the prescribed cash threshold / cash conveyance limits, unless the FIC provides directives to the contrary. Such direction to cease or withhold the transaction may not exceed 10 business days and is intended to provide the FIC with additional time to make all necessary enquiries and, where deemed appropriate, inform investigating authorities and/or the National Director of Public Prosecutions.

TERMINATING BUSINESS RELATIONSHIPS

4.40 Should the Group be unable to establish and/or verify the identity of a prospective client (prospective or otherwise) or any other relevant person (which includes the application of ongoing due diligence), the Group will terminate the business relationship (in the case of established clients and/or persons) or refuse to establish such a relationship or facilitate even a single transaction (in the case of prospective clients and or persons). In both cases, the Group reserves the right to file a SAR and/or STR with the applicable AML/CTF Regulatory Authorities.

DETERMINATION OF PEP STATUS

4.41 As previously discussed in paragraph 4.9, the Group utilises the services of DocFox, a credible information service that facilitates the confirmation of a person's PEP status against several global databases.

APPLICATION OF SIMPLIFIED DUE DILIGENCE MEASURES

4.42 As previously noted in paragraph 4.12, the extent of CDD collection and verification is ultimately dictated by a person's final risk rating (i.e. Low Risk, Medium Risk and High Risk). Since "Low Risk" clients (limited to natural person) pose a low level of money laundering and/or terrorist financing risk, the additional CDD documentation (as detailed in [Annexure 2](#)) is simplified.

4.43 Should a Low-Risk client's risk profile change at any time after the commencement of the business relationship, additional CDD documents will be obtained and enhanced due diligence measures will be applied (as necessary dependent on the client's new risk rating).

RECORD KEEPING

4.44 In keeping with the requirements of the Act, the Group will keep records of all CDD documentation, as detailed in [Annexure 2](#). In so doing, the Group will ensure the following:

4.45 Record Contents

Records pertaining to a transaction (be it a single transaction or several transactions concluded over the course of an established business relationship, shall include a reasonable amount of information to enable the reconstruction of a transaction if required. Such reasonable information shall include:

- i) The amount of the transaction.
- ii) The currency denomination of the transaction.
- iii) The parties to the transaction.
- iv) The nature of the transaction.
- v) The particulars of all accounts (e.g. account numbers) and files related to the transaction.
- vi) Any related business correspondence.

4.46 Time Period for which Records must be Kept

The Group shall retain the necessary aforementioned records for a minimum period of seven years. This minimum period will begin on the date that the business relationship is terminated, or the single transaction concluded.⁸

4.47 Records may be kept in Electronic Format & by Third Parties

Should record keeping at any point be facilitated through a third party on behalf of the Group, the Group will ensure that it retains free and easy access to the records and that such records are readily available to the FIC and other relevant supervisory bodies for the purposes of performing their functions in terms of the Act.⁹

4.48 Records may be kept in an electronic form, provided that these are capable of being reproduced in a legible format.

4.49 While the Group retains the right to appoint a third party to facilitate record keeping requirements prescribed by the Act on its behalf, the Group remains responsible for ensuring that such requirements are met.

4.50 Admissibility of Records in Court Proceedings

All records kept in the terms of the Act, or any certified extract of any such record, or a certified printout of any extract of an electronic record, is on its mere production admissible as evidence in a court.

OTHER REPORTABLE ACTIVITIES

4.51 In addition to the reporting of suspicious transactions and activities (previously discussed in paragraphs 4.32 to 4.39), the Group will report on the following activities:

- i) **Cash Transactions Above the Prescribed Limit:** In respect of a cash transaction, when such a transaction exceeds the prescribed amount (i.e. R50 000.00 or more), the Group shall file a Cash Threshold Report.
- ii) **Cash Transactions Above the Prescribed Limit:** If and when an amount of cash (or a bearer negotiable instrument) in excess of the prescribed amount (i.e. R50 000.00 or more) is conveyed to or from the Republic of South Africa, the Group shall on demand, report the prescribed particulars concerning that conveyance to a person authorised by the Minister for this purpose and will provide a copy of such a report to the FIC.
- iii) **Conveyance of Cash to or from the Republic of South Africa:** If and when an amount of cash (or a bearer negotiable instrument) in excess of the prescribed amount (i.e. R50 000.00 or more) is

⁸ In cases where a single transaction triggers a STR and/or SAR, the minimum record keeping period of seven years will begin from the date when the STR and/or SAR were submitted to the applicable AML/CFT Regulatory authorities.

⁹ The Group shall inform the FIC and other relevant supervisory bodies if it appoints a third party to facilitate any record keeping requirements on its behalf.

conveyed to or from the Republic of South Africa, the Group shall on demand, report the prescribed particulars concerning that conveyance to a person authorised by the Minister for this purpose and will provide a copy of such a report to the FIC.

- iv) **Electronic Transfers of Money to or from the Republic of South Africa:** If and when sending or receiving money via electronic transfer in excess of the prescribed amount (i.e. R50 000.00 or more) on behalf of or on the instruction of another person (whether the funds are leaving the Republic of South Africa or being received from another jurisdictional location), the Group shall make the required reports in the prescribed format and submit the same (along with all relevant particulars) to the FIC.
- v) **Property associated with Terrorist & Related Activities and/or Financial Sanctions:** If and when the Group becomes aware that it is in possession of property linked with terrorist or related activity, or property controlled by sanctioned persons, the Group shall take all necessary action to freeze such property, cease business activity with the associated persons and file the necessary reports to the FIC within the prescribed periods.

REPORTING TO THE FIC AND PROVIDING NECESSARY INFORMATION

4.52 Reporting Duty to the FIC

The Group acknowledges that it has a legal duty to make reports to the FIC. This includes providing the FIC with information at its request, and can encompass any of the following:

- i) Confirmation of a person's client status (past or present) with the Group.
- ii) Confirmation of a client's type of business relationship with the Group and current status thereof.
- iii) Confirmation of a person's authority to act on behalf of a client of the Group.
- iv) Confirmation of the Group's authority to act on behalf of a client or other person.

4.53 No duty of secrecy, confidentiality, or any other restriction on the disclosure of information, whether imposed by legislation (e.g. The Protection of Personal Information Act), the common law, or through agreements, affects the Group's duty and commitment to making the necessary reports prescribed by the Act. Furthermore, no legal action (civil or criminal) can be brought against the Group or any of its employees and representatives for complying in good faith with the reporting requirements and obligations imposed by the Act.

4.54 Access to Necessary Records

The Group acknowledges that the FIC and its authorised representatives has the right to access any client records, CDD records and the like during ordinary business hours and that such representatives may examine, take extracts from or make copies of such records for the purpose of obtaining further information in respect of reports that have been made (or out to have been made) in terms of the Act.

4.55 The Group shall fully cooperate with the FIC and its representatives, provided that (except in the case of public records) the FIC's right to access information is exercised by virtue of a warrant, in accordance with the requirements of the Act.

4.56 Reporting Procedures & Furnishing of Additional Information

The Group will submit all reports required by the Act in the prescribed form and manner, as directed by the FIC. The Group also acknowledges that once a report has been filed, the FIC may request additional information relating thereto, including transactional activity, supporting documentation and the grounds for making such a report.

4.57 Protection of Persons Making Reports

Any person who has made, initiated, or contributed to a report in terms of the Act is competent, but not compellable, to give evidence in criminal proceedings arising from such a report. No evidence concerning the identity of such a person in terms of the Act (or persons who provided additional information concerning such a report) or the grounds for the report itself are admissible as evidence in criminal

IMPLEMENTATION OF THE RISK MANAGEMENT COMPLIANCE PROGRAMME

4.58 The practical implementation of the Risk Management Compliance Programme (as contained in this document) and any amendment thereto, remains the ultimate responsibility of the Board of Directors. While the compliance department (specifically the MLRO and their deputies) are primarily charged with assisting the Board to meet the duties and responsibilities of the Act, the following measures have been implemented across the Group:

i) **Regular Reviews:**

Given the evolving nature of money laundering and terrorist activity, the Group's RMCP is regularly reviewed (at least annually) by the appointed MLRO, senior management officials or other qualified employees.

ii) **RMCP Access:**

The Group's RMCP is readily available to all employees via the Group's Intranet (hosted through Microsoft SharePoint) or upon written request from the Corporate Governance and/or Compliance departments.

iii) **Training:**

To aid in the creation of AML/CTF awareness, the Group provides regular training which, among others, includes information on the RMCP, the implementation thereof and amendments or improvements thereto. Training materials are designed internally and made available to all Group employees through the Global Learning platform (hosted through Microsoft Teams). Training initiatives are held on a regular basis and AML/CTF training forms part of the induction programme provided to all new employees.

iv) **RMCP Distribution to Authorised Agencies:**

The Group shall, upon request, make its RMCP available to the FIC and other authorised regulatory and/or supervisory bodies and agencies.

ANNEXURE 1: CLIENT RISK ASSESSMENT

The Risk Assessment Model is facilitated through an automated calculator utilising a third-party system provider (currently DocFox) functionality. Assessments are completed and stored electronically. The actual risk rating process considers a number of risk exposure elements to arrive at a final risk rating for each client. Should a client utilise numerous services or products the highest scores will be used for a cumulative calculation. Where applicable, the related parties to a juristic entity will be individually rated as though they were individual clients. The highest risk rating out of the related parties will serve as the final risk rating for the juristic entity as a whole.

In order to facilitate the Risk Assessment process, the Group has prepared several standardized models, which provide the point allocations in line with various weighted risk and other factors. The models are as follows:

Risk Rating Framework: Natural Persons		
Type of Product	Living Annuity	1
	Retirement Funds	1
	Endowment	4
	Tax Free Savings	3
	Investment Plan	4
	CIS / Mutual Funds	4
Investment Amount (IA) per annum	IA < R5 000	1
	R5 000 < IA < R25 000	2
	R25 000 < IA < R1M	3
	R1M < IA < R10M	4
	IA > R10M	5
Source of funds	Savings or Investment	1
	Salary or Income	1
	Bonus	1
	Inheritance	1
	Sale of property	1
	Other legitimate source – confirmation provided	1
	Other – no confirmation	100
Investor Jurisdiction	Local Investor	1
	Foreign Investor	2
	High Risk Jurisdiction	15
Investor Status	Domestic Prominent Influential Person	100
	Foreign Prominent Public Officials	100
	Sanction List Hits – NTU	100
	N/A	0

Risk Bucket	Lower Bound	Upper Bound	Renewal Period
Low Risk	1	8	5 years / 60 months
Medium Risk	9	17	3 years / 36 months
High Risk	18	100	12 months

Risk Rating Framework: Juristic Persons		
Type of Investor	Partnership	3
	Closed Corporation	3
	Sole Proprietor	3
	Unlisted Company	3
	Societies	3
	Foundations	3
	Non-Profit Organisation	5
	Trusts	5
	Other	5
Type of Product	Endowment	4
	Investment Plan	4
	CIS / Mutual Funds	4
Investment Amount (IA) per annum	IA < R5 000	1
	R5 000 < IA < R25 000	2
	R25 000 < IA < R1M	3
	R1M < IA < R10M	4
	IA > R10M	5
Source of funds	Savings or Investment	1
	Income	1
	Sale of Property	1
	Other legitimate source – confirmation provided	1
	Other – no confirmation	100
Investor Jurisdiction	Local Investor	1
	Foreign Investor	2
	High Risk Jurisdiction	15
Investor Status	Domestic Prominent Influential Person	100
	Foreign Prominent Public Officials	100
	Sanction List Hits – NTU	100
	N/A	0

Risk Bucket	Lower Bound	Upper Bound	Renewal Period
Low Risk	1	8	5 years / 60 months
Medium Risk	9	17	3 years / 36 months
High Risk	18	100	12 months

Risk Rating Framework: Low Risk Entities		
Type of Investor	Registered Retirement Fund	1
	Regulated Financial Services Business	1
	Listed Company	1
Type of Product	Endowment	1
	Investment Plan	1
	CIS / Mutual Funds	1
Investment Amount (IA) per annum	IA < R5 000	1
	R5 000 < IA < R25 000	1
	R25 000 < IA < R1M	1
	R1M < IA < R10M	1
	IA > R10M	1
Source of funds	Investment	1
	Income	1
	Sale of Property	1
	Other legitimate source – confirmation provided	1
	Other – no confirmation	100
Investor Jurisdiction	Local Investor	1
	Foreign Investor	2
	High Risk Jurisdiction	15
Investor Status	Domestic Prominent Influential Person	100
	Foreign Prominent Public Officials	100
	Sanction List Hits – NTU	100
	N/A	0

Risk Bucket	Lower Bound	Upper Bound	Renewal Period
Low Risk	1	8	5 years / 60 months
Medium Risk	9	17	3 years / 36 months
High Risk	18	100	12 months

Risk Rating Framework: Non-Investment Related Business Relationships		
Type of Relationship	FSP	1
	Representative or KI	1
	Related party to FSP	1
	Service Provider to Group entity	3
	Client utilising our Group services	3
	Any other business relationship	10
Monetary Amount (MA) per annum	FSP commission payments	1
	R0 < MA < R25 000	2
	R25 000 < MA < R5M	5
	A > R5M	100
Source of funds	Legitimate source	1
	Other / no confirmation on legitimacy	100
Jurisdiction	Local Person	1
	Foreign Person	10
	High Risk Jurisdiction	100
Additional Risk Status	Domestic Prominent Influential Person	100
	Foreign Prominent Public Officials	100
	Sanction List Hits – NTU	100
	N/A	0

Risk Bucket	Lower Bound	Upper Bound	Renewal Period
Low Risk	1	10	5 years / 60 months
Medium Risk	11	20	3 years / 36 months
High Risk	21	100	12 months

ANNEXURE 2: ACCEPTABLE SUPPORTING DOCUMENTATION

Format of Documentation

Financial institutions must maintain records of all transactions undertaken on behalf of a client during the course of a business relationship, either in the form of original documents or copies. Where copies of the original identification documents (passports, national ID, drivers' licence or any acceptable form of identification) are maintained, these copies should be duly certified in accordance with the CDD measures in place. Certified copies will not be required where documents are digitally verified through the use of third-party verification software.

Timeframe of Documentation Collection

Due to the wide range of products available and the large client pool (encompassing natural persons, legal persons and Non-Investment Business Relationships), the Group does not set out a definite timeframe in which to collect CDD documentation. The Group instead evaluates each situation according to its individual merits and makes decisions as to timing (specifically the time allowed to collect supporting documents) according to the circumstances of each case.

CDD Documentation Requirements

The prospective client risk rating will determine the required CDD, as stipulated below.

- **LOW RISK CLIENTS: INVESTMENT PRODUCT & NON-INVESTMENT RELATED BUSINESS**

Natural Persons & their Representatives:

This category is used for natural persons who do not reside in or originate from high-risk jurisdictions and who invest in low-risk products, who invest small amounts per annum or who do not pose any significant risks with regards to Non-investment Related Business.

IDENTIFY	VERIFICATION DOCUMENT	VERIFICATION PROCESS
Full Name, Surname and ID of the Client and (if applicable) their Representatives	<ul style="list-style-type: none"> - ID Document - Passport - Driver's License - Birth Certificate (ico minors) - Proof of Address - Source of Funds 	Certified copy / signed verification certificate by third party confirming that documents were verified or digital biometric verification
Proof of Representation (if applicable)	<ul style="list-style-type: none"> - Letter of Authority - Court Order - Proof of Guardianship (ico minors) - Other authorising Documents 	

Legal Persons & their Representatives

Registered retirement funds listed companies and regulated financial services business and other low risk juristic entities which do not originate from the high-risk jurisdictions are deemed to be low risk due to the nature of these juristic entities and the regulatory oversight they are subject to and compliance requirements imposed on them. Should the Group and its Associates have any doubts with regards to the CDD documents provided by these entities they will immediately be regarded as high risk and enhanced CDD documents will be required (Reference table on next page).

LEGAL ENTITY	IDENTIFY	VERIFICATION DOCUMENT	VERIFICATION PROCESS
Registered Retirement Fund	Name & Reg. No. of Fund	<ul style="list-style-type: none"> - Registration Certificate - Fund Rules 	Certified copy of document or signed verification certificate by third party confirming that

	Proof of Representation	<ul style="list-style-type: none"> - Letter of Authority - Letter of Appointment - Resolution of Authority 	documents were verified or digital biometric verification.
	Names & Surname of Representatives	<ul style="list-style-type: none"> - ID Document - Passport - Driver's License 	Additionally, fund registration/ listing/authority to act can be confirmed on the applicable regulatory authority and/or exchange website.
LEGAL ENTITY	IDENTIFY	VERIFICATION DOCUMENT	VERIFICATION PROCESS
Listed Company (LTD)	Name and Reg No. of Listed Company	<ul style="list-style-type: none"> - Confirmation of Listing - Annual Report/Accounts - Incorporation Documents - Director/Member Register - Confirmation of Trade Name - Confirmation of Reg. Address 	<p>Certified copy of document or signed verification certificate by third party confirming that documents were verified or digital biometric verification</p> <p>Additionally, registration/ listing / authority to act can be confirmed on the applicable regulatory authority/ exchange website</p>
	Proof of Representation	<ul style="list-style-type: none"> - Letter of Authority - Letter of Appointment - Resolution of Authority 	
	Name & Surname of Representatives	<ul style="list-style-type: none"> - ID Document - Passport - Driver's License 	
LEGAL ENTITY	IDENTIFY	VERIFICATION DOCUMENT	VERIFICATION PROCESS
Regulated Financial Services Business	Name and Reg. No. of the Financial Services Business:	<ul style="list-style-type: none"> - Incorporation Documents - Director/Member Register - Confirmation of Trade Name - Confirmation of Reg. Address - Confirmation of FSP status - Shareholder Register and/or Organogram (Identity of UBOs) 	<p>Certified copy of document or signed verification certificate by third party confirming that documents were verified or digital biometric verification</p> <p>Additionally, registration/ listing / authority to act can be confirmed on the applicable regulatory authority/ exchange website</p>

	Proof of Representation	- Letter of Authority - Letter of Appointment - Resolution of Authority	
	Name & Surname of Representatives	- ID Document - Passport - Driver's License	
LEGAL ENTITY	IDENTIFY	VERIFICATION DOCUMENT	VERIFICATION PROCESS
Low Risk Juristic Entities (Unregulated financial services and non-investment entities)	Name and Reg. No. of Juristic Entity	- Incorporation Documents - Director/Member Register - Confirmation of Trade Name - Confirmation of Reg. Address - Shareholder Register and/or Organogram (Identity of UBOs)	Certified copy of document or signed verification certificate by third party confirming that documents were verified or digital biometric verification Additionally, registration/ listing / authority to act can be confirmed on the applicable regulatory authority/ exchange website
	Proof of Representation	- Letter of Authority - Letter of Appointment - Resolution of Authority	
	Name & Surname of Representatives	- ID Document - Passport - Driver's License	

The Group and its Associates acknowledge that the decision to apply the simplified CDD measures with regards to all low risk clients does not remove its responsibility to adopt CDD measures, it only allows for application of reduced measures.

• **MEDIUM RISK CLIENTS: INVESTMENT PRODUCTS**

The NBTD which are requested as part of the application process shall be sufficient to cover the CDD requirements of medium risk clients.

Natural Persons & their Representatives:

Natural persons who do not reside in or originate from the high-risk jurisdictions.

IDENTIFY	VERIFICATION DOCUMENT	VERIFICATION PROCESS
Full Name, Surname and ID of Client and (if applicable) their Representative	- ID Document - Passport - Driver's License - Birth Certificate (ico minors)	Certified copy of document or signed verification certificate by third party confirming that documents were verified or digital biometric verification
Residential Address of Client:	- Proof of Address (not older than 3 months) <ul style="list-style-type: none"> Recent utility bill issued to the Client by name; 	

	<ul style="list-style-type: none"> • Recent bank or credit card Statement; • Recent reference or letter of introduction from a regulated financial services business which is operating in an equivalent jurisdiction (or a jurisdiction that complies with the FATF standards); • Co-habitant affidavit 	
Proof of Representation (if applicable)	<ul style="list-style-type: none"> - Letter of Authority - Letter of Appointment - Resolution of Authority 	
Source of Funds:	- As per confirmation in Application Form	Confirmation in application is sufficient
Income Tax Number of Client:	- As per confirmation in Application Form	

Legal Persons & their Representatives¹⁰

Any local and foreign legal persons which does not originate from the high-risk jurisdictions.

LEGAL ENTITY	IDENTIFY	VERIFICATION DOCUMENT	VERIFICATION PROCESS
Trusts	Name and Reg. No. of Trust and address of Master's Office/ Government Dept (if applicable):	<ul style="list-style-type: none"> - The Trust Deed - The will & letter of Executorship (only for Testamentary Trusts) - Letter of Authority for Trustees - Confirmation of all Beneficiaries (Identity of UBOs) 	Certified copy of document or signed verification certificate by third party confirming that documents were verified
	The Trust Founder, Trustees and Beneficiaries		
	Proof of Banking Details	- Bank Statement (not older than 3 months)	
	Proof of Representation (if applicable)	- Trustee Resolution authorising designated signatories for the Trust.	
	Full Name & Surname of: <ul style="list-style-type: none"> - Trust Founder - Trustees - Beneficiaries 	<ul style="list-style-type: none"> - ID Document - Passport - Driver's License 	

¹⁰ While not specifically addressed within South African legislation, the Group and its Associates shall have no dealings with "shell banks". Defined as a local or foreign banking institution with no physical address, the Group does not deal directly with such institutions and such institutions will not be able to pass the Group's CDD requirements.

	- Representative(s) (if applicable)		
	Proof of Address for: - Trust Founder - Trustees - Beneficiaries - Representative(s) (if applicable)	- Proof of Address for: • Trust Founder • Trustees • Beneficiaries • Representatives • (if applicable)	
	Source of Funds	- Bank Statement - Bank Reference Letter - Other Confirmation Document	
	Income Tax No.	Confirmation in Application	Confirmation is sufficient
LEGAL ENTITY	IDENTIFY	VERIFICATION DOCUMENT	VERIFICATION PROCESS
Unlisted/Private Companies (Pty Ltd) Closed Corporations (CC)	Name and Registration No. Directors/ Members Shareholders / UBO	- Incorporation Documents - Director/Member Register - Confirmation of Trade Name - Confirmation of Reg. Address - Shareholder Register and/or Organogram (Identity of UBOs)	Certified copy of document or signed verification certificate by third party confirming that documents were verified. Additionally, registration be confirmed on the applicable regulatory entity's website.
	Proof of Banking Details	- Bank Statement (not older than 3 months)	
	Proof of Representation (if applicable)	- Director Resolution authorising designated signatories for the Company / CC..	
	Full Name(s) & Surname of: - Each company director - All authorised signatories - Shareholders holding more than a 25% ownership.	- ID Document - Passport - Driver's License	

	Proof of Address for: - Each company director - All authorised signatories - Shareholders holding more than a 25% ownership.	- Proof of residential address for each authorised representative	
	Source of Funds	- Bank Statement - Bank Reference Letter - Other Confirmation Document	
	Income Tax No	Confirmation in Application	Confirmation is sufficient
LEGAL ENTITY	IDENTIFY	VERIFICATION DOCUMENT	VERIFICATION PROCESS
Partnerships Societes Foundations Other Legal Entities	Name and Reg No. of Entity Members / Partners UBOs	- Incorporation or Founding Documents - Confirmation of Trade Name - Confirmation of Reg. Address - Shareholder Register and/or Organogram (Identity of UBOs)	Certified copy of document or signed verification certificate by third party confirming that documents were verified. Additionally, registration be confirmed on the applicable regulatory entity's website if possible
	Proof of Banking Details	- Bank Statement (not older than 3 months)	
	Proof of Representation (if applicable)	- Letter of Authority - Letter of Appointment - Resolution of Authority	
	Full Name & Surname of: - Each company director - All authorised signatories - Shareholders holding more than a 25% ownership.	- ID Document - Passport - Driver's License	

	<p>Proof of Address for:</p> <ul style="list-style-type: none"> - Each company director - All authorised signatories - Shareholders holding more than a 25% ownership. 	<ul style="list-style-type: none"> - Proof of residential address for each authorised representative 	
	<p>Source of Funds</p>	<ul style="list-style-type: none"> - Bank Statement - Bank Reference Letter - Other Confirmation Document 	
	<p>Income Tax No.</p>	<p>Confirmation in Application</p>	<p>Confirmation is sufficient</p>
LEGAL ENTITY	IDENTIFY	VERIFICATION DOCUMENT	VERIFICATION PROCESS
Registered CIS Funds	<p>Name and Confirmation of Fund Registration or Regulation</p>	<ul style="list-style-type: none"> - Copy of the Prospectus/PPM/ Main Deed of the Scheme - Copy of the supplemental deed of the specific fund - Confirmation of registration with Regulatory Authority if not clear from the aforementioned documents 	<p>Certified copy of document or signed verification certificate by third party confirming that documents were verified.</p> <p>Additionally registration be confirmed on the applicable regulatory entity's website</p>
	<p>Proof of Banking Details</p>	<ul style="list-style-type: none"> - Bank Statement (not older than 3 months) 	
	<p>Proof of Representation (if applicable)</p>	<ul style="list-style-type: none"> - Director Resolution authorising designated signatories for the Fund. 	
	<p>Full Name & Surname of:</p> <ul style="list-style-type: none"> - Each company director - All authorised signatories - Shareholders holding more than a 25% ownership. 	<ul style="list-style-type: none"> - ID Document - Passport - Driver's License 	
	<p>Proof of Address for:</p> <ul style="list-style-type: none"> - Each company director 	<ul style="list-style-type: none"> - Proof of residential address for each authorised representative 	

	<ul style="list-style-type: none"> - All authorised signatories - Shareholders holding more than a 25% ownership. 		
	Source of Funds	<ul style="list-style-type: none"> - Bank Statement - Bank Reference Letter - Other Confirmation Document 	
	Income Tax No.	Confirmation in Application	Confirmation is sufficient

• **MEDIUM RISK CLIENTS: NONINVESTMENT RELATED BUSINESS**

Natural Persons & their Representatives:

Natural persons who do not reside in or originate from the high-risk jurisdictions.

IDENTIFY	VERIFICATION DOCUMENT	VERIFICATION PROCESS
Full Name, Surname and ID of Client and (if applicable) their Representative	<ul style="list-style-type: none"> - ID Document - Passport - Driver’s License - Birth Certificate (ico minors) 	Certified copy of document or signed verification certificate by third party confirming that documents were verified or digital biometric verification
Residential Address of Client:	<ul style="list-style-type: none"> - Proof of Address (not older than 3 months) <ul style="list-style-type: none"> • Recent utility bill issued to the Client by name; • Recent bank or credit card Statement; • Recent reference or letter of introduction from a regulated financial services business which is operating in an equivalent jurisdiction (or a jurisdiction that complies with the FATF standards); • Co-habitant affidavit 	
FProof of Representation (if applicable)	<ul style="list-style-type: none"> - Letter of Authority - Letter of Appointment - Resolution of Authority 	
FSource of Funds:	Documents will depending on the relationship (majority will be payments made by Group entity to Service Provider)	Confirmation via risk rating sufficient

Legal Persons & their Representatives¹¹

Any local and foreign legal persons which does not originate from the high-risk jurisdictions.

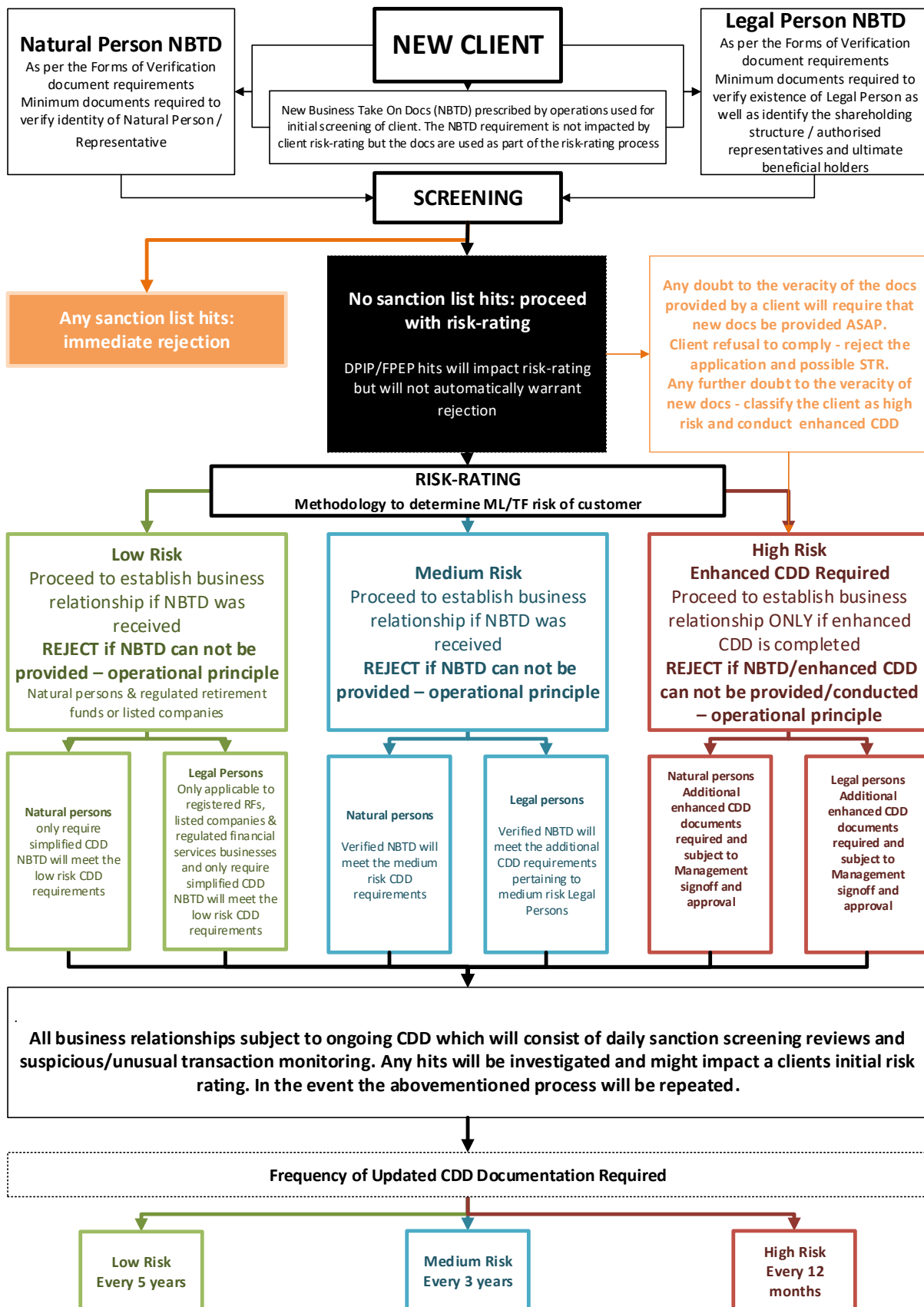
¹¹ While not specifically addressed within South African legislation, the Group and its Associates shall have no dealings with “shell banks”. Defined as a local or foreign banking institution with no physical address, the Group does not deal directly with such institutions and such institutions will not be able to pass the Group’s CDD requirements.

LEGAL ENTITY	IDENTIFY	VERIFICATION DOCUMENT	VERIFICATION PROCESS
Trusts	Name and Reg. No. of Trust and address of Master's Office/ Government Dept (if applicable):	<ul style="list-style-type: none"> - The Trust Deed - The will & letter of Executorship (only for Testamentary Trusts) - Letter of Authority for Trustees 	Certified copy of document or signed verification certificate by third party confirming that documents were verified
	The Trust Founder, Trustees and Beneficiaries	<ul style="list-style-type: none"> - Trust AFS / Annual Report - Confirmation of all Beneficiaries (Identity of UBOs) 	
	Proof of Banking Details	<ul style="list-style-type: none"> - Bank Statement (not older than 3 months) 	
	Proof of Representation (if applicable)	<ul style="list-style-type: none"> - Trustee Resolution authorising designated signatories for the Trust. 	
	Full Name & Surname of: <ul style="list-style-type: none"> - Trust Founder - Trustees - Beneficiaries - Representative(s) (if applicable) 	<ul style="list-style-type: none"> - ID Document - Passport - Driver's License 	
	Proof of Address for: <ul style="list-style-type: none"> - Trust Founder - Trustees - Beneficiaries - Representative(s) (if applicable) 	<ul style="list-style-type: none"> - Proof of Address for: <ul style="list-style-type: none"> • Trust Founder • Trustees • Beneficiaries • Representatives (if applicable) 	
	Source of Funds	<ul style="list-style-type: none"> - Bank Statement - Bank Reference Letter - Other Confirmation Document 	
LEGAL ENTITY	IDENTIFY	VERIFICATION DOCUMENT	VERIFICATION PROCESS
Unlisted / Private Companies	Name and Reg. No of Company / CC. Directors / Members	<ul style="list-style-type: none"> - Incorporation Documents - Director/Member Register 	Certified copy of document or signed verification certificate by third party confirming
Closed Corporations	Shareholders / UBO	<ul style="list-style-type: none"> - Confirmation of Trade Name 	

		<ul style="list-style-type: none"> - Confirmation of Reg. Address - Shareholder Register and/or Organogram (Identity of UBOs) - Entity AFS / Annual Report 	<p>that documents were verified</p> <p>Additionally, registration be confirmed on the applicable regulatory entity's website</p>
	Proof of Banking Details	<ul style="list-style-type: none"> - Bank Statement - Bank Reference Letter - Other Confirmation Document 	
	Proof of Representation (if applicable)	<ul style="list-style-type: none"> - Director Resolution authorising designated signatories for the Company / CC. 	
	Full Name & Surname of: <ul style="list-style-type: none"> - Each company director - All authorised signatories - Shareholders holding more than a 25% ownership. 	<ul style="list-style-type: none"> - ID Document - Passport - Driver's License 	
	Proof of Address for: <ul style="list-style-type: none"> - Each company director - All authorised signatories - Shareholders holding more than a 25% ownership. 	<ul style="list-style-type: none"> - Proof of residential address for each authorised representative 	
	Source of Funds	<ul style="list-style-type: none"> - Bank Statement - Bank Reference Letter - Other Confirmation Document 	
LEGAL ENTITY	IDENTIFY	VERIFICATION DOCUMENT	VERIFICATION PROCESS
Partnerships	Name & Form of Entity	<ul style="list-style-type: none"> - Incorporation Documents - Partner/Member Register 	Certified copy of document or signed verification certificate by third party confirming
Societes	Members / Partners	<ul style="list-style-type: none"> - Confirmation of Trade Name 	
Foundations	UBO		

Other Legal Entities		<ul style="list-style-type: none"> - Confirmation of Reg. Address - Beneficial Interest Register (Identify UBOs) - Entity AFS / Annual Report 	<p>that documents were verified</p> <p>Additionally, registration be confirmed on the applicable regulatory entity's website if possible</p>
	Proof of Banking Details	<ul style="list-style-type: none"> - Bank Statement - Bank Reference Letter - Other Confirmation Document 	
	Proof of Representation (if applicable)	<ul style="list-style-type: none"> - Partner / Member Resolution authorising persons as designated signatories for the Entity. 	
	Full Name & Surname of: <ul style="list-style-type: none"> - Each company director - All authorised signatories - Shareholders holding more than a 25% ownership. 	<ul style="list-style-type: none"> - ID Document - Passport - Driver's License 	
	Proof of Address for: <ul style="list-style-type: none"> - Each company director - All authorised signatories - Shareholders holding more than a 25% ownership. 	Proof of residential address for each authorised representative	
	Source of Funds	<ul style="list-style-type: none"> - Bank Statement - Bank Reference Letter - Other Confirmation Document 	

ANNEXURE 3: RISK ASSESSMENT & ONBOARDING PROCESS OVERVIEW



ANNEXURE 4: SAMPLE INTERNAL DISCLOSURE FORM FOR SUBMISSION TO THE MLRO

A copy of the completed report must be retained by the person reporting the suspicious activities elaborated on therein. This retained copy should be signed by the MLRO.

DETAILS OF CLIENT BEING REPORTED

Full name:

Address (registered if required):

Postal: _____

Physical: _____

Telephone numbers (as appropriate):

Home: _____

Work: _____

Cell: _____

Email: _____

Identity /Passport / Company Registration No:

Income Tax Number:

Bank account details (as appropriate):

Name of Organization the client represents or works for:

Capacity / Position:

NATURE OF SUSPICION:

ANNEXURE 5: SECTION 42 BREAKDOWN

SECTION 42 REQUIREMENTS	POLICY SECTIONS
Subsection 2	
<p>a. The RMCP must enable the company to:</p> <ul style="list-style-type: none"> - Identify; - Assess; - Monitor; - Mitigate; and - Manage <p>the risk that the provision of products or services may involve or facilitate money laundering activities or the financing of terrorist activities.</p>	Paragraph 4.1
<p>b. Provide for the manner in which the company determines if a person is:</p> <ul style="list-style-type: none"> - A prospective client in the process of establishing a business relationship or entering into a single transaction with the business. - A client who has established a business relationship or entered into a single transaction. 	Paragraph 4.2 to 4.5
<p>c. Provide for the manner in which the institution complies with Section 20A.</p>	Paragraph 4.6 to 4.7
<p>d. Provide for the manner in which and the processes by which the establishment and verification of the identity of persons whom the accountable institution must identify in Part 1 of the Act is performed by the company.</p>	Paragraph 4.8 to 4.21
<p>e. Provide for the manner in which the institution determines whether future transactions that will be performed in the course of the business relationship are consistent with the company's knowledge of its prospective client.</p>	Paragraph 4.22
<p>f. Provide for the manner in which and the processes by which the company conducts additional due diligence measures in respect of legal persons, trusts and partnerships.</p>	Paragraph 4.23 to 4.24
<p>g. Provide for the manner in which and the processes by which ongoing due diligence and account monitoring in respect of business relationships is conducted by the institution.</p>	Paragraph 4.25 to 4.26
<p>h. Provide the manner in which the examining of:</p> <ul style="list-style-type: none"> - Complex or unusually large transactions; and - Unusual patterns of transactions which have no apparent business or lawful purpose, <p>and keeping of written findings relating thereto, is done by the company.</p>	Paragraph 4.27 to 4.28
<p>i. Provide for the manner in which and the processes by which the company will confirm information relating to a client when the company has doubts about the veracity of previously obtained information.</p>	Paragraph 4.29 to 4.31
<p>j. Provide for the manner in which and the processes by which the institution will perform the customer due diligence requirements in accordance with Sections 21, 21A, 21B and 21C when, during the course of a business relationship, the institution suspects that a transaction or activity is suspicious or unusual as contemplated in Section 29.</p>	Paragraph 4.32 to 4.39
<p>k. Provide for the manner in which the company will terminate an existing business relationship as contemplated in Section 21E.</p>	Paragraph 4.40
<p>l. Provide for the manner in which and the processes by which the company determines whether a prospective client is a foreign prominent public official or a domestic prominent influential person.</p>	Paragraph 4.41
<p>m. Provide for the manner in which and the processes by which enhanced due diligence is conducted for higher-risk business relationships and when simplified customer due diligence might be permitted in the company.</p>	Paragraph 4.42 to 4.43
<p>n. Provide for the manner in which and place at which the records are kept in terms of Part 2 of the Act.</p>	Paragraph 4.44 to 4.50
<p>o. Enable the company to determine when a transaction or activity is reportable to the FIC under Part 3 of the Act.</p>	Paragraph 4.51

p. Provide for the processes for reporting the information to the FIC under Part 3 of the Act.	Paragraph 4.52 to 4.57
q. Provide for the manner in which – <ul style="list-style-type: none"> - the RMCP is implemented in branches, subsidiaries and other operations of the company in foreign countries so as to enable the company to comply with its obligations under this Act; - the company will determine if the host country of a foreign branch or subsidiary permits the implementation of measures required under this Act; and - the company will inform the FIC and supervisory body concerned if the host country contemplated in point 2 above does not permit the measures required under this Act. 	Paragraph 1.1
r. Provide for the processes for the company to implement its Risk Management and Compliance Programme; and provide for any prescribed matter.	Paragraph 4.58
Subsection 2A	
The company must indicate in its Risk Management and Compliance Programme, if any paragraph under Subsection 2 is not applicable to that company and the reasons for the same.	Nothing to note.
Subsection 2B	
The Board of Directors, senior management or other person or Group of Persons exercising the highest level of authority in the company must approve the Risk Management and Compliance Programme.	Paragraph 4.58
Subsection 2C	
A company must review its Risk Management and Compliance Programme at regular intervals to ensure that it remains relevant to the company’s operations and the achievement of requirements contemplated in Subsection 2.	Paragraph 4.58
Subsection 3	
The company must make documentation describing its Risk Management and Compliance Programme available to each of its employees involved in the transactions to which this Act applies.	Paragraph 4.58
Subsection 4	
The company must, on request, make a copy of the documentation describing its Risk Management and Compliance Programme available to:- <ul style="list-style-type: none"> - The FIC; or - A supervisory body (FSCA) which performs regulatory and supervisory functions in respect of that company. 	Paragraph 4.58
Section 42A.	
Governance of anti-money laundering and counter terrorist financing compliance	
(1) The board of directors of an accountable institution which is a legal person with a board of directors, or the senior management of an accountable institution without a board of directors, must ensure compliance by the accountable institution and its employees with the provisions of this Act and its Risk Management and Compliance Programme.	Paragraph 4.58
(2) An accountable institution which is a legal person must—	
(a) have a compliance function to assist the board of directors or the senior management, as the case may be, of the institution in discharging their obligation under subsection (1); and	Paragraph 4.58
(b) assign a person with sufficient competence and seniority to ensure the effectiveness of the compliance function contemplated in paragraph (a).	Paragraph 4.58

<p>(3) The person or persons exercising the highest level of authority in an accountable institution which is not a legal person must ensure compliance by the employees of the institution with the provisions of this Act and its Risk Management and Compliance Programme, in so far as the functions of those employees relate to the obligations of the institution.</p>	<p>Not Applicable (Legal Personage)</p>
<p>(4) An accountable institution which is not a legal person, except for an accountable institution which is a sole practitioner, must appoint a person or persons with sufficient competence to assist the person or persons exercising the highest level of authority in the accountable institution in discharging their obligation under subsection (3).</p>	<p>Not Applicable (Legal Personage)</p>

ANNEXURE 6: GUIDANCE NOTES INCLUDED IN RMCP

For ease of reference and drafting / revision purposes, this Annexure details the guidance notes (as issued by the FIC and not including draft versions of the same) considered and/or incorporated (to the extent applicable and possible) into the policy document. As of this version, the following guidance notes have been considered and/or applied to the RMCP:

- Guidance Note 1
- Guidance Note 2
- Guidance Note 3 & 3A
- Guidance Note 4, 4A, and 4B
- Guidance Note 5, 5A, 5B, and 5C
- Guidance Note 6, and 6A
- Guidance Note 7

ANNEXURE 7: OWNERSHIP, APPROVAL & REVISION HISTORY

POLICY OWNER

The FICA Risk Management & Compliance Programme is owned by the Corporate Governance Department who maintains the document through consultation with and the assistance of the Compliance Department.

POLICY APPROVAL

The policy document has yet to be approved by the Board of Directors.

POLICY REVISION

Detailed below is a list of policy versions and the changes/amendments/additions made to the policy with each new version:

DATE	VERSION	CHANGES
Apr 2014	1.0	"FICA" policy established.
Sep 2014	1.1	<ul style="list-style-type: none"> - Complete format overhaul - Inclusion of Retirement Funds in Group structure - Information on PEP's included - Information on Non-Disclosures under Section 29(3) of the Act included - Reference made to the "United Nations Security Council Sanctions List Compliance Document" with regard to Terrorist fund
Feb 2015	1.2	- Include On-site Review information under Section 4: Clients & FICA
Jun 2015	1.3	<ul style="list-style-type: none"> - Inclusion of Prime Alternative Investments (Pty) Ltd in Group structure - Removal of Retirement Funds from Group structure
Aug 2015	1.4	<ul style="list-style-type: none"> - Inclusion of PAI Holdings in Group structure. - GAA's name is changed to Ascent Capital (Pty) Ltd.
Sep 2015	1.5	<ul style="list-style-type: none"> - Inclusion of Prime Asset Management (Pty) Ltd in Group structure. - GAA's name is changed to Ascent Capital (Pty) Ltd.
Nov 2015	1.6	<ul style="list-style-type: none"> - Amendments made to Annexure 1 - Inclusion of Annexure 4: Revision History - Inclusion of "Third Party Accounts".
Apr 2016	1.7	- Amendment to Annexure 1 stating that no FICA documentation is required for Listed companies except a Proof of Listing.
Aug 2016	1.8	<ul style="list-style-type: none"> - Global Employee Benefits (Pty) Ltd included in Group structure. - Inclusion of "Associates" in Group Structure. Policy reworded to make reference to both the Group and Associates where applicable. - Group structure amended to refer to "Prime Collective Investment Schemes Management Company (RF) (Pty) Ltd" and "Prime Alternative Investments (RF) (Pty) Ltd". - Header formatting. - "PIP" changed to "PEP". - Points 4.15 and 4.16 merged with Point 4.14. - Point 4.14 amended as follows: "The audit report will be filed for record keeping purposes with the Compliance department." - Section 6 amended to refer to "Politically Exposed Persons". - Point 6.3 amended as follows: "Conducting ongoing monitoring of identified PEPs. The client base of the Group and its Associates is regularly verified against an internal database of PEPs. Records of such verifications are kept by the Compliance department for record keeping purposes." - Point 8.4 merged with Point 8.3. - Section 10's point numbering corrected. - Annexure 2 updated to make reference to (RF) provisions.
Nov 2017	1.9	<ul style="list-style-type: none"> - Global Financial Administrators (Pty) Ltd included in Group structure. - Global Investment Administrators (Pty) Ltd. included in Group structure.

		<ul style="list-style-type: none"> - Global Payroll Services (Pty) Ltd included in Group structure. - Global Nominees (Pty) Ltd - Ascent Capital (Pty) Ltd reclassified as an Associate company. - References to FICA now include reference to the Financial Intelligence Centre Amendment Act of 2017 throughout the policy. - Policy entirely revised in accordance with the Act Amendments, including: <ul style="list-style-type: none"> ➤ The definition of a PIP ➤ Section 3: A Brief Look at Anti-Money Laundering & FICA ➤ Section 4: Risk Management & Compliance Programme ➤ Section 7: Staff Training (specifically “Disciplinary Proceedings” ➤ Annexure 1: Client Risk Rating ➤ Annexure 2: “Customer Due Diligence” Documentation ➤ Annexure 3: Screening & Watchlists ➤ Annexure 4: Politically Influential Persons ➤ Annexure 5: CDD Confirmation Certificate ➤ Annexure 6: Anti-Money Laundering Report
Jan 2018	1.10	- Ascent Capital (Pty) Ltd reclassified as a Group company.
Feb 2018	1.11	- Annexure 2 amended to include investments from retirement funds.
Apr 2018	1.12	<ul style="list-style-type: none"> - Group name amended to “Prime Financial Services Group” - Prime Trade Finance (RF) (Pty) Ltd removed from the Group structure. - Mashamba Asset Management (Pty) Ltd removed as an Associate company. - Orca Global Advisory (Pty) Ltd removed as an Associate company. - Section 2: Definitions updated. - New Annexure (Annexure 6: Screening for Suspicious Transactions included.)
May 2018	1.13	<ul style="list-style-type: none"> - New Annexure (Annexure 8: FIC Act Enforcement). - Dormant companies removed from Group structure.
Jul 2018	1.14	- Annexure 2 amended to include a footnote detailing the definition of shell banks and the Group’s treatment of such institutions within the South African Regulatory environment.
Oct 2018	1.15	<ul style="list-style-type: none"> - PIP Definition expanded. Client Risk Rating (Section 4.7 – 4.9) was amended in line with the FSCA comments arising from the onsite visit of Sep 2018. - Sections 4.15, 4.20, 4.21 and 4.22 were moved to 4.3 – 4.6. - Footnotes 2 and 3 were amended to include reference to prospective clients. - Section 5 amended to include some examples of suspicious transactions. - Section 8 amended to refer to reporting processes outlined in Section 5. - Annexures renumbered. - Annexure 3 amended with a risk scoring and rating system. - Annexure 4 amended to include client source of funds and processes to be followed when doubting the veracity of provided documentation. - Footnote 7 included.
Nov 2018	1.16	<ul style="list-style-type: none"> - Annexure 5 amended to include specific confirmations related to prospective client screening, PIP validation and risk assessments. - Annexure 6 amended to broaden the triggers for suspicious transaction reporting.
Jan 2019	1.17	- Annexure 3 amended to state that high risk clients are referred to Board level for final approval.
Jul 2019	2.0	<ul style="list-style-type: none"> - Section 5: “Reporting Suspicious Activities” amended to refer more comprehensively to the FIC Guidance Notes and reporting timelines. - Section 8: “Other Reportable Activities” has been incorporated into Section 5. - Annexure 3 has been amended to expand the risk-rating model, specifically incorporating the nature of an investor. - Annexure 7 amended. - Address updated. - Format changes.

		<ul style="list-style-type: none"> - Global Financial Administrators (Pty) Ltd removed from Group structure. - Umbrella Funds removed from Group structure. - Retirement CDD requirements amended in Annexure 4. - Policy Simplification
Dec 2019	2.1	<ul style="list-style-type: none"> - New heading “Application of Policy” updated. - High Risk Jurisdictions detailed in Annexure 1 updated according to latest FATF information (December 2019). - Ongoing CDD Measure timeframes in Annexure 1 revised.
Sep 2020	3.0	<ul style="list-style-type: none"> - FICA: Risk Management & Compliance Programme finalised and implemented in terms of the FICA Amendment Act of 2017.
Jul 2021	4.0	<ul style="list-style-type: none"> - Appendix 5 and 6 updated with revised supporting documents.
Jan 2023	5.0	<ul style="list-style-type: none"> - FICA Policy revised to simplify document and follow the flow of Section 42 as set out in the Act.