BROKSTOCK SA (Pty) Ltd

RISK MANAGEMENT AND COMPLIANCE PROGRAMME (the"RMCP")

(in terms of section 42 of the Financial Intelligence Centre Act No 38 of 2001 (as amended))

Version 4.0
Effective from 8 December 2025

TABLE OF CONTENTS

1. ADOPTION AND OWNERSHIP

MEMBERS OF BOARD must acknowledge ownership and adopt this RMCP by signing this page.

Name	Signature
Alexey Annenkov	
Petrus Johannes Serfontein	PJ Serfontein

In accordance with the section 42A the Key Individual acting as Compliance Officer must also acknowledge the ownership and adoption of this RMCP by the Company, by signing this page. By adopting and signing this, he/she confirms that this RMCP will be reviewed annually and propose material changes to the Board for approval. The RMCP, together with all approved versions, will be made available to the Financial Intelligence Centre and any other relevant regulatory authorities upon request.

Name	Signature
Petrus Johannes Serfontein	PJ Serfontein

2. DEFINITIONS

2.1 "**Accountable Institution**" means all businesses or persons as listed in Schedule 1 of FICA and includes Financial Services Providers. All Accountable Institutions have certain obligations in terms of FICA.

2.2 "**AML**" means Anti-money Laundering.

2.3 "**Board**" means the Board of Directors of the Company.

2.4 "**Business Relationship**" means an arrangement between the Company and a Client that contemplates a series of Single Transactions on a regular basis.

2.5 "**Cash**" means paper money or coins as defined in section 1 of the FICA.

2.6 "**CDD**" means the Client due diligence referred to in section 21 of FICA.

2.7 "**Client**" means any individual or legal entity which has entered into a Business Relationship or a Single Transaction with the Company.

2.8 "**Client On-Boarding Checklist**" means the checklist a Prospective Client is required to complete and sign during the On-Boarding process, as set out in Schedule 2.

2.9 "**Company**" means BROKSTOCK SA (Pty) Limited ("BROKSTOCK"), registration number

2020/523823/07, an accountable institution in terms of Schedule 1 to the FICA.

2.10 "**Compliance Officer**" means the person assigned to the compliance function in terms of section 42A of FICA, having sufficient competence and seniority to ensure effectiveness of the compliance function.

2.11 "**CRM**" means system for managing all of company's interactions with current and potential clients.

2.12 "**DPEP**" means a domestic politically exposed person, being any person, or immediate family member or known close associate of a person as listed in Schedule 3A of FICA and Schedule 5 of this RMCP.

2.13 "**Employee**" means all of the Company's employees. This includes staff including directors, consultants, who are Client-facing and/or deal with Clients on a day-to-day basis.

2.14 "**Enhanced CDD**" means the process of conducting an enhanced investigation and obtaining more information about a Client. This may include applying closer scrutiny to the Client's transaction activities where ML/TF risks are assessed to be higher.

2.15 "**FIC**" means the Financial Intelligence Centre, a juristic person created under Chapter 2 of FICA. It is the regulatory body responsible for monitoring compliance by Accountable Institutions with FICA.

2.16 "**FICA**" means the Financial Intelligence Centre Act No.38 of 2001 (as amended).

2.17 "**FPEP**" means a foreign politically exposed person, being a person, or immediate family member or known close associate of a person, who occupies, or within the past 12 (twelve) months occupied, any of the positions listed in Schedule 3B of FICA and Schedule 9 of this RMCP.

2.18 **"Guidance Note 3A"** means Guidance for accountable institutions on client identification and verification and related matters of Financial Intelligence Centre

2.19 "**High-Risk Client**" means a Client/Prospective Client who poses high ML/TF risks to the Company.

2.20 "**High-Risk Transaction**" means a transaction that has been assessed by the Compliance Officer and found to pose high ML/TF risks to the Company.

2.21 "**ML/TF**" means Money Laundering and the Financing of Terrorism, where "money laundering" refers to any practice through which the proceeds of crime are dealt with so as to obscure their illegal origins, and where "the financing of terrorism" refers to the financing of Terrorist Activities.

2.22 "**POCA**" means the Prevention of Organised Crime Act No. 121 of 1998.

2.23 "**POCDATARA**" means the Protection of Constitutional Democracy against Terrorism and

Related Activities Act No. 33 of 2004 (as amended from time to time).

2.24 "**POPI**" means the Protection of Personal Information Act No. 4 of 2013.

2.25 "**Proceeds of Unlawful Activities**" means any property or any service, advantage, benefit or reward which was derived, received or retained, directly or indirectly, in the Republic or elsewhere at any time before or after the commencement of POCA, in connection with or as a result of any unlawful activity carried on by any person, and includes any property representing property so derived.

2.26 "**Prospective Client**" means a person who approaches the Company for financial services, whether for their own account or on another person's behalf.

2.27 **"Regulations"** means Money Laundering and Terrorist Financing Control Regulations of 20 December 2002 (as amended)

2.28 "**Republic**" means the Republic of South Africa.

2.29 "**RMCP**" means this risk management and compliance programme, which has been designed in response to the Company's obligations under section 42 of FICA.

2.30 "**Secondary Accountable Institution**" means another Accountable Institution (such as a bank) that the Company has a Client in common with in respect of the same Single Transaction, or Business Relationship.

2.31 "**Single Transaction**" means a transaction other than a transaction concluded in the course of a business relationship and where the value of the transaction is not less than R5,000.00 (five thousand rand).

2.32 "**Source of Funds**" means the origin of the funds financing a Business Relationship or Single Transaction. It includes the activity that generated the funds used in the Business Relationship (for example, the Client's salary, occupation, business activities, proceeds of sale, corporate dividends, etc).

2.33 "**Source of Wealth**" means, in respect of DPEPs and FPEPs, the activities that have generated the total net worth of the Client (for example, inheritance or savings).

2.34 "**Standard Risk Client**" means a Client who poses low to medium ML/TF risks to the Company.

2.35 "**Standard Risk Transaction**" means a transaction which has been assessed by the Compliance Officer and poses a low to medium ML/TF risk to the Company.

2.36 "**Terrorist Activities**" means any of the offences specified in POCDATARA, all of which relate to terrorism.

3. INTRODUCTION

3.1 FICA requires that an Accountable Institution must develop, document, maintain and implement a programme for AML and counterterrorist financing risk management and compliance. In this respect, an Accountable Institution is required to maintain internal rules providing for, amongst others:

3.1.1 the establishment and verification of client identities;

3.1.2 keeping of records; and

3.1.3 reporting of certain information.

3.2 The Company views its compliance with applicable AML laws and regulations to be of paramount importance.

3.3 The Company requires that every Director and other Employee maintain the highest standards of compliance in line with the benchmarks established globally in relation to combating ML/TF.

3.4 The methods employed by the Company must entail reasonable endeavors that ensure that it knows its Clients, that it is not used for ML/TF activities and that it is able to assist law enforcement agencies and other authorities, where such activities are investigated.

3.5 Some of the key measures include, amongst others, the implementation of an RMCP that provides for effective Client on-boarding measures, increased monitoring of measures by Fee Earners, increased review of Client information and increased sensitivity of risk sensitive CDD measures by the Compliance Officer.

3.6 It is the responsibility of the Company's directors and employees to thoroughly acquaint themselves with the Company's Risk Management and Compliance Programme (RMCP). Upon reviewing and understanding the RMCP, they must either sign the declaration in Schedule 1 or complete the necessary training and achieve a passing result to demonstrate their compliance and understanding of the requirements..

4. THE PURPOSE OF THIS POLICY

4.1 Section 42 of FICA requires an Accountable Institution to develop, document, maintain and implement a programme for AML and counterterrorist financing risk management and compliance.

4.2 The purpose of this policy is to document the Company's RMCP and to set out, amongst others, how the Company will:

4.2.1 collect information about its Clients/Prospective Clients and their representatives;

4.2.2 understand and obtain information on business relationship, including nature of business, its purpose and source of funds to be used in the course of business relationship;

4.2.3 monitor Clients' transactions

4.2.4 keep records of its Clients' transactions;

4.2.5 report to the FIC when required; and

4.2.6 train employees.

4.3 Records required by the FICA and Regulations will be retained for at least five (5) years from termination of the business relationship or completion of a single transaction.

5. RESPONSIBILITY AND COMPLIANCE

5.1 Every Employee is required to either sign a declaration confirming they have read and understood this RMCP, or complete the necessary training and achieve a passing result to demonstrate their understanding. .

5.2 The Board and the Compliance Officer are responsible for the implementation and enforcement of this RMCP.

5.3 The Compliance Officer shall be responsible for monitoring compliance with this RMCP and performing annual review. Any material changes must be submitted to the Board for approval.

5.4 Every Employee employed by the Company bears responsibility for compliance with the provisions of FICA (as amended), including (without limitation) compliance with the Company's RMCP.

5.5 Every Employee is required to comply with the Company's RMCP.

5.6 Failure by any Employee to comply with the provisions of FICA and/or the Company's RMCP (as the case may) will be formally disciplined in accordance with the Company's disciplinary policy and procedure.

6. APPOINTMENT AND RESPONSIBILITY OF COMPLIANCE OFFICER

6.1 In terms of FICA, the Company is required to appoint a person with the responsibility to ensure compliance by its employees with the provisions of FICA as well as the Company's RMCP.

6.2 The Company has appointed the Compliance Officer, with the necessary skills and knowledge to perform the duties required in terms of FICA and this RMCP. The Compliance

Officer is accountable to the Company's Board of Directors in carrying out the responsibility for the effective management of the Company's RMCP.

6.3 The Compliance Officer is responsible for:

6.3.1 ensuring that the RMCP is implemented and maintained in line with the FIC Act, Regulations and Guidance;

6.3.2 maintaining effective procedures for CDD, enhanced CDD, transaction monitoring, and reporting (Cash Threshold Report (CTR), Suspicious and Unusual Transaction Report (STR), Terrorist Financing Transaction Report (TFTR), Terrorist Financing Activity Report (TFAR), Suspicious Activity Report (SAR), Terrorist Property Report (TPR));

6.3.3 ensuring the submission of all cash threshold reports, terrorist financing transaction reports, as well as suspicious or unusual transaction reports to the FIC within prescribed timeframes and maintaining evidence of submission;

6.3.4 facilitating the training of all employees regarding their FICA duties in general, and to their duties under this RMCP, in particular;

6.3.5 conducting vendor due diligence for any third-party KYC/AML providers, ensuring contractual rights to underlying CDD records and compliance with POPIA on cross-border transfers;

6.3.6 reviewing and updating the Company's RMCP as necessary;

6.3.7 making the Company's RMCP available to all Employees in such a manner that they are alerted as to its existence, and can access it freely and with ease;

6.3.8 implementing appropriate client risk rating methodologies and source of fund verification;

6.3.9 liaising with representatives of the FIC as and when necessary and/or required;

6.3.10 ensuring that Employees sign the declaration at the end of this RMCP confirming their understanding of this RMCP; and

6.3.11 overseeing to the Company's effective implementation of this RMCP.

6.4 The Board shall ensure the Compliance Officer has adequate resources and authority to perform these duties.

7. DUTY TO ESTABLISH AND VERIFY CLIENTS' IDENTITY

7.1 FICA prevents the Company from establishing a Business Relationship or entering into a

Single Transaction with a Client, unless it has established and verified the identity of the Client concerned, or the person representing the Client, or another person on whose behalf the Client is acting.

7.2 In order to establish a Client's identity, the Company is obliged to obtain a range of information about the Client. Such information should be obtained during the on-boarding process. The detailed process is described in Client Onboarding and Identification Manual of BROKSTOCK.

7.3 Verification of the Client's identity obliges the Company to corroborate the information by comparing such information with information contained in documents or electronic data or created by reliable and independent third-party sources.

7.4 When the Client is a legal entity, the Company shall comply with the requirements of sections 21 and 21B of the Financial Intelligence Centre Act (FICA), read with Guidance Notes 3A and 4A, to establish and verify the identity of the Client and its Beneficial Owners.

7.5 The following documents must be obtained and verified prior to the establishment of a business relationship:

- Certificate of Incorporation or CIPC Company Extract, issued within the last three (3) months, confirming the entity's registration number and registered address.
- Proof of the physical business address of the entity, such as a utility bill, bank statement, or lease agreement, not older than three (3) months.
- Recent bank statement (last 3 months) from the entity's operational account, evidencing financial activity.
- Certificate of Incumbency or equivalent document, confirming the current directors, registered address, and shareholders.
- Identification documents (SA ID or passport) of all directors, authorised signatories, shareholders holding 5% or more, and any natural person identified as a Beneficial Owner (UBO).
- Proof of residence (utility bill not older than three (3) months) for each natural person referred to above.
- SARS Good Standing Certificate or other tax authority confirmation document for non SA legal entities
- Client Information Form, which must include:

  Legal form of the entity (company, trust, partnership, etc.);

  Nature of business activities;

  Shareholding and ownership structure (including intermediate entities).

7.6 To establish and verify the beneficial ownership structure of a legal person, the Company may request supporting documents necessary to evidence the full ownership chain up to natural persons.

Acceptable supporting documents include, but are not limited to:

- an ownership organogram reflecting the full chain of ownership;
- shareholder registers and CoR filings;
- CIPC UBO registers;
- foreign corporate registry extracts;
- constitutional documents (MOI, shareholder agreements);
- any other documentation required to establish ownership or effective control.

7.7 Or any other document that may be required to demonstrate compliance with customer due-diligence, enhanced due-diligence, and ongoing monitoring obligations.

7.8 Documents with an expiry date or periodic validity must be reviewed and updated in line with the client's assigned risk category. Where a client fails to provide the required updated documentation within the specified timeframes, the institution may impose a range of account restrictions to ensure continued compliance with FICA, internal governance standards, and the organisation's risk-based approach.

Possible account restrictions

- Limiting or suspending outward payments, withdrawals, or high-risk transactions.
- Restricting the opening of new trading positions or enabling only "close-only" functionality.
- Reducing transaction thresholds or imposing temporary caps on activity.
- Limiting access to online platforms to view-only mode.
- Suspending account upgrades, new product additions or changes to authorised persons.
- Freezing the account in whole or in part until documentation is received and validated.

7.9 Applying enhanced monitoring measures or escalating the matter to compliance.

7.10 The client will also be required to complete a Product Suitability Questionnaire. This assessment is designed to evaluate the client's financial objectives, risk tolerance, investment experience, and overall product understanding. The information gathered enables the company to determine whether the proposed products or services are appropriate for the client's profile and to ensure alignment with regulatory suitability and disclosure requirements.

7.11 All documents must be in English or accompanied by a certified English translation. Documents may not be older than three (3) months at the time of verification.

7.12 Where any inconsistencies, incomplete information, or doubts regarding the ownership or control structure are identified, the onboarding process shall be suspended pending clarification or application of Enhanced Due Diligence (EDD).

7.13 The Company recognises that legal entities may range from simple domestic structures to

complex cross-border arrangements. Accordingly, additional measures shall be applied where ownership or control cannot be readily established, where foreign entities are involved, or where other risk indicators are present.

7.14 Electronic verification may be used (e.g. through third-party providers such as SumSub or LexisNexis) provided vendor due diligence is performed, agreements are in place requiring access to underlying records, and periodic reviews are conducted. Where automated checks fail, manual verification is required, and the client is treated as high-risk until resolved. Responsibility for compliance remains with the Company.

7.15 The Company can request assistance from a third party accountable institution for:

- Identification of client and other required person's particulars.
- Verification of client and other required person's particulars.
- Information such as source of funds, source of wealth, geographic location.

7.16 The Company cannot request assistance from a third party accountable institution for:

- The ML/TF risk, and associated rating assigned to the Client by the third party accountable institution.
- The screening performed on the Client by the third party accountable institution.
- Ongoing due diligence.
- Any reporting obligations in terms of the FIC Act.

7.17 The Company shall identify Domestic and Foreign Politically Exposed Persons (PEPs). Enhanced CDD will be applied to all PEPs, including Board approval for DPEPs and Senior Management approval for FPEPs. Source of wealth and source of funds will be established.

7.18 Reliance on another Accountable Institution is permitted only where a written confirmation is obtained that it has conducted CDD and will provide documentation on request. The Company retains ultimate responsibility for compliance.

7.19 The Company may terminate a business relationship where it is unable to complete adequate Customer Due Diligence (CDD), where a client refuses or repeatedly fails to provide required information or updated documentation, where sanctions or Proliferation Financing concerns arise, or where suspicious activity persists. In addition, the Company may take action where a client does not respond to compliance requests or fails to follow formally established processes such as the complaints procedure, operational verification steps, or other regulatory requirements. Persistent non-engagement with mandatory compliance obligations may result in service limitations or account closure.

7.20 Termination must follow a structured and documented process, including escalation to Compliance, suspension of transactional activity where required, and the formal closure of the business relationship. Closure of an account or termination of the relationship may occur in any instance where the Company is unable to continue meeting its regulatory obligations, where client behaviour presents elevated financial crime or operational risk, or where the client fails to cooperate with mandatory processes.The Company reserves the

right to terminate the business relationship without prior notice where required to comply with legal or regulatory obligations, prevent financial crime, or protect the integrity of its operations. Immediate termination may occur where a client persistently fails or refuses to provide required CDD/EDD documentation, does not cooperate with compliance reviews or established internal processes, or where sanctions, Proliferation Financing concerns, or suspicious activity are identified. Termination may likewise be effected where the client's behaviour demonstrates a lack of good faith, including intentionally obstructing compliance processes, providing misleading information, engaging in abusive conduct towards staff, or publicly or privately bad-mouthing the Company in a manner that causes reputational harm. The Company may also act without notice where the client's actions compromise platform security, create unacceptable regulatory, operational, or reputational risk, or otherwise threaten the Company's ability to fulfil its statutory duties.

8. RISK-BASED APPROACH

8.1 In accordance with FICA's current risk-based approach, some intellectual input incorporating discretion and risk is required of the Accountable Institution.

8.2 A risk-based approach requires the Company to understand its exposure to ML/TF risks. By understanding and managing such risks, the Company not only protects and maintains its integrity but also contributes to the integrity of the South African financial system.

8.3 Sufficient information should be obtained from Clients in order to implement a risk rating methodology in terms of which the Prospective Client's level of risk will be measured. The BROKSTOCK Risk Rating Tool provides a structured, risk-based method for assessing both Company Risk and Client Risk across all onboarding and ongoing monitoring activities. The framework evaluates inherent exposure by considering jurisdictional factors, regulatory categorisation, business model complexity, ownership transparency, and the entity's status as an Accountable Institution, thereby determining the Company Risk profile. In parallel, the tool assesses behavioural, financial and compliance-related indicators to establish the Client Risk profile, including the client's willingness to cooperate with CDD/EDD requirements, transactional behaviour, source of funds, anticipated activity patterns, and any conduct that may pose reputational, operational, or financial-crime risk to BROKSTOCK. These two dimensions—Company Risk and Client Risk—are combined to generate an overall risk score that guides the level of due diligence, monitoring intensity and governance oversight required to maintain regulatory compliance and protect the integrity of the business relationship.

8.4 By applying a risk-based approach, the Company ensures that measures to prevent or mitigate ML/TF are commensurate with the risks identified.

8.5 The Company will apply CDD using a risk-based approach when it establishes a Business Relationship with a Client, carries out a Single Transaction, suspects ML/TF activities, or doubts the veracity of information previously provided by the Client.

8.6 There are two categories of risk which will be applied during the Company's CDD process. These are standard risk and high risk.

8.7 If a Client is categorised as a Standard Risk Client, the Company will apply a simplified CDD where less information will need to be obtained from that Client and less frequent scrutiny will be required, as ML/TF risks in respect of that Client are assessed to be lower.

8.8 If a Client is a High-Risk Client, the Company will apply an enhanced CDD where more information will need to be obtained from that Client and closer scrutiny to that Client's transaction activities will be required.

8.9 **Standard Risk Clients**

The following Clients are accepted as Standard Risk Clients:

8.9.1 Local Clients;

8.9.2 Clients with whom a Business Relationships has already been established; and/or

8.9.3 Clients who do not fall into the category of High-Risk Clients.

8.10 **High Risk Clients**

8.10.1 A High-Risk Client is any Client:

(a) who is a natural person, but not a citizen or permanent resident of South Africa;

(b) who is an FPEP. This includes family members and known close associates of FPEP's;

(c) who may be regarded as suspect by the Employee and/or the Compliance Officer for any reason relating to the Client's conduct in the context of a Single Transaction or Business Relationship, which conduct includes (without limitation):

(i) a reluctance or refusal to provide information;

(ii) a patent lack of concern or disregard for the costs involved;

(iii) an unusual or inexplicable preference for dealing with the Company via correspondence or via electronic media, as opposed to in person, particularly for the purposes of the CDD;

(iv) deliberate evasiveness or vagueness when providing information; or

(v) any other conduct or circumstances that, when viewed objectively,

and when considered in light of all of the relevant factors taken as a whole, should be regarded with suspicion.

8.10.2 If the Business Relationship or Single Transaction poses a high risk of facilitating ML/TF activities, the Company must obtain additional information from the client/prospective client to enable him/her to build a Client profile and to identify the possible proceeds of money laundering activities. In this respect, it should be noted that some services or areas of law could provide opportunities to facilitate money laundering or terrorist financing. By way of guidance, the following transactions may be considered higher risk:

(a) an "unusual" financial or property transaction(s);

(b) payments that are made to or received from unrelated third parties;

(c) providing assistance in setting up trusts or company structures, which could be used to obscure ownership of property;

(d) cash payments exceeding R49,999.99 must be reported in accordance with Guidance Note 5C on Cash Threshold Reporting under Section 28 of the Financial Intelligence Centre Act, 2001 (act 38 of 2001).

8.10.3 Employees must refer to the Company's Risk Matrix guidelines in addition to the the profiling a client and updating client information in the Company systems, including CRM..

8.11 **Verification in the absence of contact person (non-face to face clients)**

Reasonable steps must be taken to establish the existence and verify the identity of that natural person. The Company has identified the following additional measures to be taken when dealing with such Clients:

8.11.1 Client identification can be carried out via both web and mobile applications of BROKSTOCK. Before establishing relationship with the client BROKSTOCK will require the client to upload the photo (scan) of identification document. The documents will be submitted to BROKSTOCK.

8.11.2 The following automated checks will be performed using automatic KYC/AML system SumSub (detailed information on SumSub is available in Onboarding and identification manual) and LexisNexis:

(a) Integrity Check

(i) A solution for an automated verification and authentication of 3,500 various types of identity documents from nearly every country worldwide including all types of SA identification documents.. It allows to determine the authenticity and legitimacy as well as to ensure that the document is not forged or altered.

(b) Authenticity Check and Document Data check

(i) A solution that checks the image of the proof of identity document has not been subjected to any alteration, the document, an image of which the customer has provided, really exists and is a valid and proper proof of identity document, the document, an image of which the customer has provided, belongs to the individual with the name, surname, date of birth, personal identification number (where applicable), whom the customer claims to be. Before entering into business relations.

In case of successful integrity and authenticity checks the electronic verification of the client must be considered similar to face-to-face verification and such clients will be classified as Standard Risk Clients.

8.11.3 In the cases when the Company fails to check integrity and authenticity the Company must request documents to be certified as original documentation ; and

8.11.4 These clients will be classified as High-risk Clients and dealt with accordingly.

8.12 **Anonymous or Fictitious Clients**

8.12.1 The Company is strictly prohibited from dealing with anonymous persons, or persons who have fictitious names.

8.12.2 The Company must, by adhering to the provisions of this RMCP, ward against the risk of:

(a) dealing with an anonymous person by refusing to on-board as a Client anybody who appears to desire or expresses a desire to transact with the Company anonymously;

(b) dealing with a fictitiously named person by subjecting all Prospective Clients to the CDD procedures described in this RMCP, which procedures are aimed at ensuring, amongst other things, that the Company only deals with persons who exist.

8.13 **DPEP**

8.13.1 Automatic AML system SumSub will be used to identify whether a Client is a DPEP, the responsible Employee check results of the DPEP checklist check which correspond the checklist set out in Schedule 2 of this RMCP. A list of DPEP positions is also annexed as Schedule 5 of this RMCP. Additionally all clients must be asked whether they fall into this category.

8.13.2 Business Relationships or Single Transactions with DPEPs are not inherently high-risk. However, due to their position and influence, it is recognised that many DPEPs are in

positions that potentially can be abused for the purpose of committing ML/TF offences and related predicate offences, including corruption and bribery.

8.13.3 In addition to the standard CDD measures carried out, the Company will apply the following proactive measures in relation to Client's that are DPEPs:

(a) Board's approval for establishing the Business Relationship must be obtained;

(b) the Board will take reasonable steps to establish the source of wealth and funds of the Client; and

(c) the Board will conduct on-going monitoring on the Business Relationships with these Clients.

8.13.4 The measures listed in 9.13.3 will apply to family members and known close associates of a DPEP.

8.14 **FPEP**

8.14.1 Automatic AML system SumSub will be used to identify whether a Client is a FPEP. In terms of FICA, FPEPs are always considered high-risk. The decision to engage or maintain a Business Relationship with an FPEP Client should be taken by Senior Management.

8.14.2 If the Company decides to establish a Business Relationship or a Single Transaction with an FPEP Client, the Company will apply the following additional measures in addition to performing an enhanced CDD on the FPEP Client:

(a) the Company will take reasonable steps to establish the source of wealth and funds of the Client; and

(b) the Company will conduct on-going monitoring on the Business relationships with these Clients.

8.14.3 The measures listed in 9.14.2 will apply to family members and known close associates of an FPEP.

8.15 **Secondary Accountable Institutions**

8.15.1 If the Company:

(a) has a Client in common with a Secondary Accountable Institution (such as a bank or another financial institution); and

(b) that Client in common is in respect of the same Single Transaction or transactions under a Business Relationship between the Company and that Client; and

(c) the Secondary Accountable Institution agrees to subject, or has already subjected the Client to CDD procedures in accordance with that Secondary Accountable Institution's own RMCP; and

(d) the Secondary Accountable Institution agrees to furnish the Company with (i) a letter to the effect that it has satisfied itself as to the identity and otherprescribed particulars of the Client in compliance with FICA, and (ii) if requested by the Company, will provide copies of the documents and/or records of the information relied upon to carry out the Secondary Accountable Institution's customer due diligence procedures in respect of the Client,

8.15.2 Then the Company may rely on the letter referred to in clause 9.15.1(d), having complied with FICA and this RMCP. If the letter does not cover all the information that would have been required in terms of the Company's FICA checklist, the Company must supplement the information in the letter by means of the FICA checklist, which must be completed by the Client.

8.16 **Financial Action Task Force (FATF) Member States and Observers:**

A client who is a citizen of a country not listed as a member or observer of the Financial Action Task Force (FATF) will be classified as a high-risk client. The list of FATF member states is regularly updated to reflect current risks and global cooperation standards in combating money laundering and terrorist financing. To ensure compliance, the Country Risk Assessment Policy will include a detailed list of approved countries, taking into account the latest FATF updates. This assessment is essential for identifying higher-risk jurisdictions and implementing enhanced due diligence measures where required.

8.17 **Legal Entities Risk Assessment**

In assessing the risk level of legal entity, the Company shall evaluate both the entity itself and its ownership structure.
The following factors must be considered when determining whether a legal entity presents a higher risk:

- Complex or opaque ownership structures involving multiple layers of entities;
- Use of nominee shareholders or offshore holding companies;
- Incorporation or management in a jurisdiction classified by the FATF as high-risk or non-cooperative;
- Involvement in high-cash or high-value sectors (e.g., crypto trading, mining, real estate, money remittance);
- Absence of verifiable operational presence (e.g., shell or dormant entities);
- Frequent or large-value international transfers, particularly in USD or EUR;
- Association with Politically Exposed Persons (PEPs) or sanctioned entities;
- Mismatch between the stated nature of business and expected transactional pattern.

Legal entities are not automatically categorised as High Risk. Risk classification shall

follow a structured assessment of jurisdiction, ownership transparency, industry profile, UBOs, and adverse information.

The classification shall correspond with the procedures set out in the Onboarding Manual.

A legal entity may be classified as Standard Risk where its ownership and control structure is simple, transparent and readily verifiable.

A legal entity may fall into this category where:

- It is incorporated and registered with CIPC;
- A single natural person is both the director and shareholder;
- The UBO is a South African citizen or permanent resident;
- No nominee arrangements, trusts, offshore entities or layered structures are involved;
- No PEPs or sanctions indicators are identified;
- All documentation is internally consistent and can be reliably verified.

Standard CDD measures apply. EDD is not required unless new risk indicators emerge.

A legal entity shall be classified as High Risk where any high-risk indicators exist. High-risk indicators include, without limitation:

- Foreign incorporation or management;
- Multi-layered or opaque ownership structures;
- Involvement of foreign trusts, private foundations, partnerships or nominees;
- Jurisdictions with elevated ML/TF risk or insufficient transparency;
- Associations with PEPs or sanctioned individuals;
- Inconsistency or unverifiability of documents submitted;
- Mismatch between declared business activities and available data.

High-risk clients are subject to Enhanced Due Diligence in accordance with the procedure described in the Onboarding Manual.

The Company performs a formal Business Risk Assessment identifying inherent ML/TF/PF risks associated with its products, services, client segments, delivery channels, geographic exposure and counterparties.

Each inherent risk category is evaluated using a point-based methodology (1–5), taking into account the nature of the Company's activities and the vulnerabilities associated with them.

Risk mitigation controls are mapped to each inherent risk to determine residual risk exposure.

This Business Risk Assessment is reviewed at least annually or upon any material change in the Company's business model.

The Compliance Officer shall ensure that risk ratings are assigned to each legal entity based on the above criteria and that the rationale for the risk rating is documented in the client file.

A date stamp will be applied to certain documents and certificates, and the company will request updated versions upon their expiry. Should a legal entity fail to provide the required updated documents, a stepwise process for the temporary suspension of the account will be implemented. Suspension might include suspension of trading activity or in case of unwillingness of the legal entity to share the documents required termination of the account.

Proliferation Financing (PF) risk also forms part of the Company's risk assessment and control framework.

In accordance with PCC 54 and FATF Recommendation 7, the Company assesses PF risk indicators, including:

- jurisdictions or counterparties associated with proliferation concerns;
- transactions inconsistent with stated business purposes;
- opaque or multi-layered ownership structures;
- clients involved in high-risk goods or dual-use items.

PF screening is integrated into sanctions screening, transaction monitoring and client risk assessment processes.

9. OPERATIONAL RISKS

9.1 In the event of any disaster the Company will identify means to communicate with its clients, employees, the regulator, and institutions holding client funds. Key activities shall be retrieved by means of data backup. In the event that server has been destroyed the Company has to purchase a new server and ensure it's operational condition within a space period of 2 days. Monthly periodic reports are done for audit logs. Backup media stored in a secure place isolated from environmental hazards. Emergency contact details are always publicly available to all Company's employees.

9.2 Data backup procedures:

9.2.1 Proper electronic data backups will minimise the risk of loss of important information of the Company in the event of a disaster.

9.2.2 Permanent loss of data may have a significant impact on the Company's ability to perform core business functions. It is therefore imperative that backups are made and tested on a regular basis.

9.2.3 Data can be stored on any of the following devices:

- Flash-drives;
- External hard drives;
- Cloud storage;

- Network Storage or Servers; and
- Offsite backup systems (replication or synchronisation methods).

9.2.4 The frequency and the extent of backups will correspond proportionately with the importance of the data being stored. For example, where client information is of critical importance to the organisation's day-to-day functioning and/or regulatory compliance requirements, the information will be backed-up on a more frequent basis.

9.2.5 Back-up systems that are available at the Company are:

- One Drive;
- Office 365;

9.2.6 Storage systems for client data that are available at the Company are:

- SumSub;
- LexisNexis;
- Trading platform - MetaTrader5 and MetaTrader5 Manager.

9.2.7 The three main types of backup procedures are:

- Full Backups: A full backup captures all data files on disk. It is the simplest type of backup and provides a complete backup image, making restoring data and functionality easier and faster. The disadvantage of a full backup is that it takes time and uses more storage space than an incremental backup.
- Incremental Backups: Incremental backups only contain copies of data files that were changed subsequent to the previous backup. This allows for more device storage space and considerably reduces the time it takes to perform a backup.
- Custom Backups: Custom backups are usually made on an ad hoc basis.

9.2.8 Backups must be tested on a regular basis. Regular testing will minimise the risk of an unsuccessful data recovery exercise following a disaster.

9.2.9 Company's critical business information is kept electronically and is available on the following platforms / service providers:

- CRM
- Microsoft Office suite
- Banking Systems
- SumSub
- LexisNexis

9.2.10 The Responsible Person and the Key Individual have uninterrupted access to the Critical

Business Information.

9.3 The Company shall maintain a formal Business Continuity and Disaster Recovery Plan ("BCP") which defines critical business services and systems and responsibilities and contact lists for recovery actions. The BCP shall be tested at least annually (or after material change).

9.4 All third-party providers (including SumSub, LexisNexis, cloud providers and trading platforms) used to process or store personal or client-sensitive data must be subjected to vendor due diligence prior to onboarding. Due diligence must include information security standards (ISO 27001 / SOC2), POPIA compliance, access controls, right to audit, data location and a minimum SLA. Contracts must contain data protection clauses and a right to request underlying KYC evidence where applicable.

9.5 The Company shall maintain an incident response plan which sets out detection, containment, eradication and recovery steps for cyber incidents. Security incidents involving personal data must be reported to the Information Regulator in accordance with POPIA guidance.

10. FINANCIAL RISKS

10.1 The Company shall ensure ongoing financial soundness by maintaining minimum liquidity and capital buffers as approved by the Board and consistent with Board Notice 194 of 2017 (Fit and Proper and financial soundness requirements for FSPs). The Board will be notified by management upon any material deterioration.

10.2 Where financial thresholds are breached or there is a material risk to continuity of services, the Company shall notify the FSCA or other relevant regulator in accordance with applicable rules (and the Company's regulatory notification procedure).

10.3 In the event of a significant business disruption, the Company will determine its financial ability to continue to operate and service its clients.

10.4 The Company will contact product suppliers, clients and critical banks to apprise them of the financial status and notify the Regulator if required.

10.5 Please refer to our Business Continuity and Succession Plan Policy, which outlines procedures and strategies to ensure that the business can continue to operate effectively during unexpected disruptions, such as natural disasters, financial crises, or other significant events. The policy also addresses succession planning, which ensures that there is a clear plan for leadership transitions or replacements, protecting the company's operations and stability in the event of leadership changes due to retirement, resignation, or unforeseen circumstances.

11. RISKS TO KEY INDIVIDUAL

11.1 In the event of the Director of the South African Office and or Kl temporary absence (i.e. the expected absent period is to exceed 2 working days) due to illness, accident or vacation the Responsible Person will be elected to ensure the orderly implementation and execution of the day to day running of the organisation.

11.2 All parties affected by the KI's absence must be notified accordingly by the Responsible Person.

11.3 During the absence of the Kl, all support staff and authorised representatives will continue performing the necessary administrative tasks performed during the normal day-to-day operations of the Financial Services Provider (FSP).

11.4 The KI (prior to departure) to ensure an "out of office" reply has been set up on the KI's email account explaining the KI's absence, expected date of return as well as alternative contact numbers.

11.5 Where the Kl will be in an area without mobile phone coverage, the Kl is to ensure that they:

- check their voicemail boxes daily;
- provide an alternative method to enable key administrative staff to be able to contact him or her during a client or other emergency.

11.6 In the event of any of the FSP's Kl's death or permanent incapacity, the Responsible Person will be responsible to ensure the orderly implementation and execution of the day to day running of the organisation until the shareholders of the organisation identify a suitable replacement.

11.7 In a situation where no suitable replacement can be found and winding down the business remains the only option, then the normal cessation of business in terms of the FAIS Act and Code of Conduct processes will be followed.

11.8 Product suppliers shall also be contacted as well as External Compliance shall notify the registrar (FSCA) by email.

12. RISK AVERSIVE APPROACH IN CRYPTO INDUSTRY

12.1 The Company professes risk aversive approach providing financial services in crypto industry by implementing a diverse set of measures aimed at eliminating industry specific risks.

12.2 **Customers assets protection**

12.2.1 The Company is obligated to maintain client's assets safe and safeguard customer cash by segregating these assets from the Company's proprietary business activities, and promptly deliver to their owner upon request.

12.2.2 The Company provides security for customers by assessing external providers to ensure cryptocurrency liquidity and fulfil custodial function at the required level.

12.2.3 The Company obtains comprehensive professional services for digital assets under custody to protect against potential loss due to theft, hacking, or operational errors.

12.2.4 The Company applies a multi-factor authentication (MFA)including three channels as phone number, e-mail and Google Authenticator App

12.2.5 Changes in sensitive client's data (e.g. addition of authorised external crypto wallets, banking accounts or banking cards, changes of emails and phone numbers and etc.) are confirmed by client via MFA procedures;

12.2.6 Trading transactions are confirmed by a PIN assigned by a Client;

12.2.7 Withdrawal transactions are confirmed by Google Authenticator code;

12.2.8 Withdrawals of any assets are confirmed by BROKSTOCK Director and the Finance and Payment function;

12.2.9 Withdrawals may be additionally confirmed by direct phone conversation between Account Director and Client

12.2.10 Please refer to our Customer Assets Protection Policy. This policy outlines the measures implemented to prevent unathorised access, loss, theft, or misuse of client assets.

12.3 Cyber security for client assets

12.3.1 The Company develops solutions and constantly updates cybersecurity methods to protect customer assets, as well as conducts regular security audits and assessments to identify vulnerabilities and areas for improvement. This includes penetration testing and vulnerability assessments.

12.3.2 The Company establishes identity management and access control mechanisms to provide effective and consistent user administration, accountability and authentication.

12.3.3 The Company implements robust encryption mechanisms to protect sensitive customer data, both at rest and in transit. This includes encrypting data stored in databases as well as data transmitted over networks.

12.3.4 The Company ensures remote access to information assets is only allowed from devices or connections that have been secured according to the Company's security standards.

12.3.5 The Company ensures that IT systems managed by third-party service providers are accorded the same level of protection and subject to the same security standards or are subject to protections and security standards that are commensurate to the sensitivity and criticality of the information being managed by the third-party service provider.

12.3.6 The Company installs network security devices to secure the network between the financial institution and the internet, as well as connections with third-party service providers.

12.3.7 The Company reviews its network architecture, including the network security design; as well as systems and network interconnections on a periodic basis to identify potential vulnerabilities.

12.3.8 The Company systemically monitors and detects actual or attempted attacks on IT systems and business services as well as effectively responds to attacks.

12.3.9 The Company establishes security monitoring capabilities such as a security operations centre (or similar) or acquire managed security services in order to facilitate continuous monitoring and analysis of cyber events as well as prompt detection and response to cyber incidents.

12.3.10 The Company applies a set of anti-phishing procedures according to Cybersecurity policy to mitigate one of the common cybersecurity threats.

12.3.11 If there has been any security breach or hack attempt on the platform, users are notified immediately through all available channels such as email alerts, push notifications or social media messages so that they can take necessary actions to secure their assets.

12.3.12 Please refer to our Cyber Security Policy for detailed guidelines on safeguarding digital assets and protecting sensitive information from cyber threats. This policy outlines measures such as encryption, secure access protocols, threat detection, and employee training to prevent data breaches, hacking attempts, and unathorised access. It also covers incident response procedures to mitigate damage in the event of a cyber attack and ensures compliance with applicable data protection regulations.

12.4 **Reliability of technological infrastructure**

12.4.1 The Company evaluates internal and external technological infrastructure, including storage systems, monitoring, and other technical capabilities, and existence of technical audits.

12.4.2 The Company establishes robust disaster recovery and backup protocols to ensure asset safety in case of system failures, physical damage, or other catastrophic events.

12.4.3 The Company implements strict access controls and authentication measures, including biometric checks and MFA, to ensure that only authorised personnel can access different security levels.

12.4.4 The Company regularly updates and maintains the technological infrastructure to keep up with the latest security standards and mitigate risks associated with outdated systems.

12.5 **Key management and wallet safety**

12.5.1 The Company applies main principles of cryptographic key management that are crucial for ensuring the security, integrity, and confidentiality of cryptographic keys, which are fundamental to the protection of sensitive data and digital assets within the Company's crypto framework and processes.

12.5.2 The Company obliges all employees, contractors, and third parties involved in the generation, storage, usage, and management of cryptographic keys to keep them confidential and protected from unauthorised access. Access to keys should be restricted to authorised personnel, and strong encryption and access controls should be implemented to prevent exposure to unauthorised individuals or entities.

12.5.3 The Company maintains the integrity of cryptographic keys to ensure that they have not been altered, tampered with, or compromised in any way. Robust key generation, storage, and transmission mechanisms should be employed to prevent unauthorised modifications or unauthorised substitution of keys.

12.5.4 The Company obliges all the actors to ensure the authenticity of cryptographic keys to keep them genuine and not compromised. The Company employs mechanisms for verifying the authenticity of keys, such as digital signatures, digital certificates, and secure key distribution protocols to establish trust in the origin and validity of cryptographic keys.

12.5.5 Cryptographic keys are generated using industry-standard encryption algorithms and best practices to ensure their strength and randomness.

12.5.6 All cryptographic keys are securely stored using approved mechanisms, such as hardware security modules (HSMs), secure key vaults, or other industry-recognized secure storage solutions.

12.5.7 The Company applies regular key rotation practices to minimise the potential impact of key compromise and to align with industry best practices.

12.6 **Crypto assets deposit management**

12.6.1 All digital asset deposits are accompanied by detailed deposit records, including information about the depositor, the type and amount of digital assets, and the purpose of the deposit.

12.6.2 Digital asset deposits are securely stored in approved digital asset storage solutions, such as cold or hot wallets, with strong access controls, encryption, and segregation of duties in place to prevent unauthorised access and mitigate operational risk.

12.6.3 The Company conducts regular reconciliation and audit of digital asset deposits to ensure accuracy, completeness, and accountability.

12.6.4 Withdrawals or transfers of digital asset deposits are carried out in accordance with the Company's approved processes and controls, with proper authorisation and verification of the withdrawal requests to maintain the integrity and security of the Company's digital assets.

12.7 **Transaction monitoring and reporting**

12.7.1 Transaction monitoring involves keeping track of all transactions made within the system, including purchases and exchanges. All transaction reports contains all the necessary information such as the sender's details, recipient's details, amount transferred, timestamps, and transaction status.

12.7.2 The Company conducts regular inspections to detect any fraudulent or suspicious activities in real-time and reports them to prevent potential theft or loss of cryptocurrencies.

12.7.3 The Company must maintain transparency by making these reports available to their clients or shareholders upon request.

12.7.4 The Company maintains transparency by providing clear communication channels for users to report any suspicious activity or issues promptly. The reports are available to shareholders upon request.

12.8 **Personal and training**

12.8.1 The Company engages qualified personnel who understand the risks associated with cryptocurrency storage and usage.

12.8.2 The Company agrees to develop a training matrix, which determines the training needs for the continuous improvement cycle of safeguards.

12.8.3 The Key Individual oversees the training activities within the Company, and will, with the representative, review the Training Plan annually to ensure satisfactory progress.

13. COUNTERPARTY RISKS

13.1 The Company takes a highly selective approach when choosing liquidity providers. Within the Financial Group, there is a Risk Committee, which is tasked by BROKSTOCK to prepare reports on potential liquidity providers.

13.2 As part of these reports, a credit rating is assigned to each company. In this context, the

credit rating reflects the company's ability to meet its financial obligations in full and on time. The credit quality of the company is determined by a combination of internal and external factors. Each factor is described using both quantitative and qualitative indicators.

13.3 The rating model is structured in a three-level hierarchy:

13.3.1 At the first level, creditworthiness factors are grouped into three categories: the company's business profile, its financial profile, and the level of regulatory oversight in the country of registration.

13.3.2 At the second level, the business profile assessment is divided into three subgroups: company size, ownership, and time in the market. The financial profile is divided into four subgroups: operational efficiency, liquidity, debt load, and capital adequacy.

13.3.3 At the third level, final quantitative and qualitative indicators are used to calculate the rating based on their values.

13.4 A point-based system is used to calculate the rating, with expert evaluations of the significance of indicators and their weights. Each financial company is assigned a certain number of points based on the values of the indicators included in the model.

13.5 Points are allocated in such a way that the most important indicators carry the highest weight. The selection of indicators and their weights is determined through empirical analysis of creditworthiness factors and best practices in the rating of companies in the financial sector.

13.6 For the assignment of the rating, information is requested from the financial company (such as audited financial statements) as well as from public sources.

13.7 The Company interacts with several liquidity providers, including local providers licensed by the FSCA, to reduce reliance on any single provider. Additionally, the Company has the capability to utilise liquidity aggregators such as Finery Markets to mitigate liquidity risks.

13.8 The Company should regularly track the performance of all liquidity providers, keep up with regulatory changes, and identify any potential risks. This ongoing monitoring allows the Company to quickly address any issues and ensure the services remain stable and reliable.

13.9 Business Continuity plans have been developed to address outages or disruptions from any of liquidity providers to ensure business continuity.

13.10 The Company also conducts comprehensive due diligence for each liquidity provider. This process includes an in-depth analysis of their most recent audited financial statements. The main objective is to thoroughly assess the risk profile of each liquidity provider and

determine the appropriate exposure limits. The evaluation should be based on a wide array of metrics, including, but not limited to, assets, equity, income, credit ratings, regulatory status, country of incorporation, ultimate beneficial ownership (UBO), organisational structure, funding sources, etc.

13.11 Regarding cryptocurrency exchanges, the Company should also utilize real-time data services such as CoinMarketCap and Nansen Portfolio to monitor financial health. CoinMarketCap provides data on trading volume, liquidity, market capitalisation, and price changes, enabling to compare exchanges, track changes, and identify potential issues. Nansen Portfolio offers insights into exchange assets, liabilities, cryptocurrency flows, and user activity, allowing to assess the solvency of the exchange, monitor risks, and detect suspicious activities. In the event that the Company identifies unexplained anomalies, such as significant changes in assets at specific addresses or a decline in profit and loss (P&L), the Company should promptly take appropriate action in accordance with relevant internal policies and procedures.

14. SYSTEM RISKS

14.1 The Company, when carrying out its business activities, takes all essential measures to:

14.1.1 ensure that IT systems managed by third-party service providers are accorded the same level of protection and subject to the same security standards or are subject to protections and security standards that are commensurate to the sensitivity and criticality of the information being managed by the third-party service provider;

14.1.2 ensure that sensitive information stored in systems and endpoint devices is encrypted and protected by access control mechanisms commensurate to the risk exposure;

14.1.3 ensure that only authorised IT systems, endpoint devices and data storage mediums, are used to communicate, transfer, or store sensitive information;

14.1.4 ensure that security controls are implemented to prevent and detect the use of unauthorised internet services which allow users to communicate or store sensitive data;

14.1.5 ensure that the use of sensitive production information in non-production environments must be restricted. In exceptional situations where production data needs to be used in non-production environments, adequate processes and safeguards must be in place for the data request and approval must be obtained from senior management;

14.1.6 ensure appropriate controls are implemented in production and non-production environments to manage the access and removal of sensitive information to prevent data leakages;

14.1.7 ensure sensitive information is permanently deleted from storage media, IT systems and endpoint devices before it is disposed of or redeployed;

14.1.8 have an agreement in place for the secure return or transfer of data in instances where the contract, including a contract with a third-party service provider, is terminated and data must be returned. If return is impossible, there must also be processes in place for the permanent deletion of copies of the financial institution's information as well as the secure destruction of storage media containing the financial institution's information;

14.1.9 have appropriate non-disclosure or confidentiality provisions included in the relevant agreements in place with users;

14.1.10 install network security devices to secure the network between the financial institution and the internet, as well as connections with third-party service providers;

14.1.11 deploy network intrusion detection or prevention systems to detect and block malicious traffic;

14.1.12 review its network architecture, including the network security design; as well as systems and network interconnections on a periodic basis to identify potential vulnerabilities;

14.1.13 implement network access controls to detect and prevent unauthorised devices from connecting to its network. Network access mechanisms must be reviewed regularly, but at least annually, to ensure they are kept up-to-date;

14.1.14 review firewall rules on a periodic basis and test network perimeter controls and posture at least annually;

14.1.15 isolate internet web browsing activities from its sensitive IT systems through the use of physical or logical segregation, or implement equivalent controls, to reduce exposure of its IT systems to cyber-attacks;

14.1.16 encrypt remote connections to prevent data leakages through network sniffing and eavesdropping;

14.1.17 systemically monitor and detect actual or attempted attacks on IT systems and business services as well as effectively respond to attacks;

14.1.18 periodically evaluate the effectiveness of identified controls, including through network monitoring, testing and audits;

14.1.19 establish security monitoring capabilities such as a security operations centre (or similar) or acquire managed security services in order to facilitate continuous

monitoring and analysis of cyber events as well as prompt detection and response to cyber incidents.

15. DUTY TO MAINTAIN RECORDS

15.1 Sections 22 and 22A of FICA refers to records to be kept by Accountable Institutions in respect of the identification and verification process undertaken by them whenever it establishes a Business Relationship or concludes a transaction with a client, whether that transaction is a Single Transaction or one concluded in the course of a Business Relationship. Records are maintained in CRM.

15.2 **What records must be kept?**

The Company is required to keep the following records:

15.2.1 regarding the identity of the Client*:*

(a) The identity of the Client and, if applicable, the identity of the Client's agent or principal;

(b) The manner in which this identity was established;

(c) The name of the person who obtained this information or timestamp and source of data when the identity data was obtained through the Company system during automated onboarding and verification;

(d) Any document or copy obtained by the Company to verify the identity;

(e) Full documentation on the verification of legal entities, including all documents obtained to confirm the entity's existence, ownership, control, UBO and shareholder identification

15.2.2 regarding the transaction*:*

(a) The nature of the transaction;

(b) The amounts and parties involved in a transaction;

(c) The currency in which the transaction was denominated;

(d) The date and time on which the transaction was concluded;

(e) business correspondence;

(f) All accounts involved in the transactions concluded by the Company in the course of the Business Relationship or in the Single Transaction.

15.3 **Recordkeeping period**

15.3.1 Business Relationship*:* The records must be kept for at least 5 years from the date on which the Business Relationship is terminated.

15.3.2 Transaction*:* The records in respect of the Single Transaction or any other transaction must be kept for at least 5 years from the date on which the transaction is concluded.

15.3.3 Suspicious Transaction Reporting*:* If a transaction is reported to the FIC in terms of section 29 of FICA, then the records must be kept for at least a period of 5 years from the date on which the report is made.

15.3.4 The need to maintain adequate records for at least 5 years gives effect to the provisions of FICA and is essential to assist with the ultimate investigation and prosecution of crime if applicable.

15.4 **General Provisions, Processes and Responsibility**

15.4.1 FICA Recordkeeping Checklist*:* The required detail regarding the transactions will be completed on the FICA Recordkeeping Checklist (which is linked to CRM) (see Schedule 7). This Checklist must be completed on every transaction and must be stored in a central file. The person who obtained the information is responsible for completing the Recordkeeping Checklist.

15.4.2 FICA Compliance Officer: The Compliance Officer will be responsible for informing all Employees of the record keeping requirements as well as their responsibility to maintain these records as it pertains to the Company's Clients.

15.4.3 Electronic Recordkeeping: Records may be kept in electronic form. The necessary disaster recovery plan and backup procedures must be in place.

15.4.4 Admissibility of Records*:* A record kept, or a certified extract of such a record, or a certified printout of any extract from an electronic record, is on its mere production in a matter before a court admissible as evidence of any fact contained in it of which direct oral evidence would be admissible.

15.4.5 Recordkeeping Responsibility*:* Although it is the primary responsibility of the Company to maintain records, it is the responsibility of every Employee to obtain all the necessary information at the time of the transaction and keep these records safe. Although the basic information is completed on the CRM system, the supporting documentation must still be kept in the Client file. No record may be destroyed by a person before the expiry of the five-year period referred to.

15.5 **Outsourcing of Recordkeeping to third Parties**

Outsourcing of record keeping requirements is regulated by section 24 of FICA and Regulation 20 of the Regulations. Accountable Institutions must comply with these sections when records are being kept by third parties. The Company utilises the services of

CRM for these purposes.

15.6 **FIC's Access to Records**

15.6.1 An authorised representative of FIC has access during ordinary working hours to any records kept by the Company. This representative may examine, make extracts of or copies of any such records. If the records are not public documents, access may only be obtained by virtue of a duly issued warrant.

15.6.2 Any request for access of records must be forwarded to the Compliance Officer, and when he is satisfied that the representative is authorised and that the FIC is entitled to the records (either in accordance with the warrant or that the documents are public documents), then he/she must make the relevant documents available without delay.

16. ADVISE FINANCIAL INTELLIGENCE CENTRE OF CLIENTS

16.1 The Company is registered with the Financial Intelligence Centre (FIC) in terms of section 43B of the FICA. The Company shall ensure that its registration details are kept up to date and that any changes in particulars are notified to the FIC without delay.

16.2 If an authorised representative of the FIC requests the Company to advise whether a specific person is or has been a client of the Company, or if the specific person acted on behalf of a client of the Company, or if a client of the Company is acting or had acted for a specific person, the Company must inform the FIC accordingly.

16.3 Failure to inform the FIC is an offence, and on conviction one is liable to imprisonment not exceeding 15 years or to a fine not exceeding R100 Million.

16.4 All reports to the FIC, including Suspicious Transaction Reports (STRs), Terrorist Financing Transaction Reports (TFTRs) and Cash Threshold Reports (CTRs), shall be in accordance with the prescribed timeframes.

16.5 The Compliance Officer shall be responsible for ensuring that registration is current and that reporting obligations are met.

17. REPORTING OF SUSPICIOUS AND UNUSUAL TRANSACTIONS

FICA provides for the reporting of suspicious and unusual transactions. The reporting of suspicious and unusual transactions is regarded as an essential element of the AML programme of every country. Schedule 6 contains a list of indicators of suspicious transactions.

17.1 **Who must Report:**

The duty to report is imposed on all Employees of the Company whether or not they deal specifically with clients.

17.2 **When does the Reporting Obligation Arise?**

17.2.1 The obligation to report arises when a person knows or ought reasonably to have known or suspected that certain facts exist. These facts can relate to situations concerning the business itself or transactions to which the business is a party.

17.2.2 Situations relating to the business can be that the Company:

(a) has received, or is about to receive, the proceeds of unlawful activities or property which is connected to an offence relating to the financing of terrorist and related activities;

(b) has been used, or is about to be used, in some way for money laundering purposes; or to facilitate an offence relating to the financing of terrorist and related activities.

17.2.3 Situations relating to transactions to which the Company is a party and a person is aware or suspects that a transaction/series of transactions with the Company:

(a) Facilitated, or is likely to facilitate the transfer of proceeds of unlawful activities or property which is connected to an offence relating to the financing of terrorist and related activities;

(b) does not appear to have a business or lawful purpose;

(c) is conducted for the purpose of avoiding giving rise to a reporting duty under FICA;

(d) may be relevant to the investigation of the evasion of any tax administered by the South African Revenue Service; or

(e) somehow relates to an offence relating to the financing of terrorist activities.

17.3 **What constitutes a suspicion?**

17.3.1 This implies an absence of proof that a fact exists. One needs to consider all the circumstances as well as the normal business practices involved. A suspicious situation may involve several individual factors that on their own seem insignificant, but taken together, they may raise a suspicion. One must evaluate the transaction in relation to what seems appropriate as well as one's knowledge

about the Client. This can include his/her financial history, background and behaviour.

17.3.2 Any person who reasonably ought to have known or suspected that any of the facts referred to in 12.2 above exists, and who negligently fails to report the prescribed information in respect of a suspicious or unusual transaction or series of transactions or enquiry, is guilty of an offence and on conviction liable to imprisonment not exceeding 15 years or a fine not exceeding R100 Million.

17.3.3 There are indicators of suspicious behaviour at Schedule 6 but they should not be viewed in isolation and should always be considered in conjunction with other circumstances.

17.4 **Suspicious Transaction Threshold**

There is no monetary threshold that applies to this reporting. Once the conclusion is reached that a suspicious or unusual situation exists, the transaction must be reported.

17.5 **Can an institution continue with a transaction after a report has been made?**

The reporter may continue with and carry out a transaction unless the FIC directs him/her not to proceed with the transaction.

17.6 **Confidentiality and Privilege**

No duty of secrecy or confidentiality prevents any person or institution from complying with the obligation to file a report.

17.7 **Legal protection for the Reporter**

17.7.1 No legal action, whether criminal or civil, can be instituted against a person who complies in good faith with the reporting obligation.

17.7.2 The identity of the reporter is also protected. This person cannot be forced to give evidence in criminal proceedings concerning such a report. A person may choose to do so voluntarily, but if he/she elects not to testify, no evidence regarding his/her identity is admissible as evidence in criminal proceedings.

17.8 **Tipping-off**

17.8.1 The person involved may not inform anyone, including the Client or any other person associated with a reported transaction, of the contents of a suspicious transaction report or even the fact that such a report has been made.

17.8.2 FICA prohibits the reporter as well as any other person who knows or suspects that a report has been made, from disclosing information regarding that report, except where required by law.

17.8.3 Contravening these prohibitions constitutes offences that carry maximum penalties of imprisonment for a period up to 15 years or a fine up to R100 million.

17.9 **What is the time period for Reporting?**

A report must be sent ***as soon as possible*** but not longer than **15 days** (excluding Saturdays, Sundays and Public Holidays) after the person has become aware of the facts which give rise to a suspicion. Any person who fails to send a report under section 29 of FICA to the FIC within the period referred is guilty of an offence, and on conviction liable for imprisonment not exceeding 15 years or a fine not exceeding R100 million.

17.10 **Method of Reporting**

17.10.1 Any director or Employee who reasonably ought to have known or suspected that any of the facts referred to in 12.2 above exists must immediately report such knowledge or suspicion to the Compliance Officer.

17.10.2 Full particulars must be provided regarding the facts on which the knowledge or suspicion is based, including the date on which such knowledge was acquired or suspicion arose.

17.10.3 The director or Employee shall under no circumstances whatsoever discuss such knowledge or suspicion, or the making of a report with any other person whatsoever (including the Client).

17.10.4 No reference to any report being made must be placed in the Clients' files.

17.10.5 A director or other Employee who intentionally "tips-off" a Client or discusses the fact that a report has been made with any other person, commits an offence and may be liable to face disciplinary action and criminal prosecution.

17.10.6 The Compliance Officer will consult with Board for appropriate legal action.

17.10.7 If it is determined that a report is to be made to the FIC, then the Compliance Officer must make such report within 15 (fifteen) business days after the date on which the knowledge or suspicion first arose. This period may be extended with the consent of the FIC only.

17.10.8 A report must be made in accordance with the format specified by the FIC and sent to the FIC using reporting portal located at fic.gov.za or other method developed by the FIC for this purpose.

17.10.9 Employees are advised to proceed cautiously and should confirm with the Compliance Officer whether it is prudent to continue acting for such Client.

17.10.10 Should it be decided that the transaction will not be continued with, the Employee may not provide the reason for terminating the mandate with a Client in these circumstances or disclose the fact that a report has been made to the FIC in respect of such Client.

17.10.11 For each reporting obligation under the FIC Act (STR, SAR, TFTR, TFAR, TPR, CTR), the Company maintains a step-by-step internal process including:

- identification of unusual or suspicious activity;
- internal escalation to Compliance;
- analysis and determination of reporting obligation;
- preparation and submission of the report via the FIC's goAML platform;
- post-submission monitoring and record-keeping.

Reports must be filed within statutory timeframes.

18. DUTY TO TRAIN EMPLOYEES

The Company is required to provide training to all of its employees to enable them to comply with the provisions of FICA and this RMCP.

18.1 Who must receive Training?

18.1.1 Every new Employee must receive training within **30 days** after their appointment.

18.1.2 All other Employees must receive refresher FICA Training on a **yearly basis**.

18.1.3 The training register of the Employees must be updated with the training they receive from the Company.

18.2 Who must provide the Training?

The Compliance Officer is responsible for training Employees as well as updating the training register.

19. POPI COMPLIANCE

19.1 The Company shall comply with the Protection of Personal Information Act, 2013 (POPIA) and observe the rights granted to Clients under applicable privacy and data protection laws and will ensure that queries relating to privacy issues are promptly and transparently dealt with.

19.2 The Company shall ensure that all processing of personal information complies with POPIA's conditions, including lawfulness, minimality, purpose specification, security safeguards, participation and data subject rights. Personal data may not be transferred cross-border unless in compliance with section 72 of POPIA (adequate protection, consent, contractual clauses).

19.3 The Company will only collect and process Client personal information to comply with FICA and its RMCP. The Company will do so in a reasonable manner that does not infringe the Client's privacy unnecessarily.

19.4 The Company will implement and adhere to its information retention policies relating to Client personal and confidential information and ensure that Client information is securely disposed of at the end of the appropriate retention period.

19.5 The Company will not share Client information with any other parties, unless required to do so by law or with the Client's consent.

19.6 In the event of a personal data breach, the Company shall notify the Information Regulator and affected data subjects as soon as reasonably possible, in accordance with POPIA section 22.

19.7 The Company shall maintain POPIA Compliance Policy and training for all employees.

ANNEX 1 Employee Risk Rating Policy in Compliance with Directive 8 of the Financial Intelligence Centre (FIC)

1. Introduction

This policy outlines the Employee Risk Rating (ERR) process in compliance with Directive 8 issued by the Financial Intelligence Centre (FIC) in South Africa. The directive mandates that accountable institutions, including BROKSTOCK, report any suspicious or unusual transactions potentially linked to money laundering, terrorist financing, or other financial crimes. The Employee Risk Rating process is a critical component of the institution's compliance with Anti-Money Laundering (AML) and Counter-Terrorist Financing (CTF) regulations, ensuring all staff act in accordance with these requirements.

2. Purpose

The purpose of this policy is to:

- Establish a clear framework for assessing and mitigating the risk posed by employees in relation to AML and CTF compliance;
- Ensure that employees with greater exposure to high-risk transactions or access to sensitive financial information are subject to enhanced oversight and training;
- Minimise the risk of non-compliance with Directive 8 by continuously monitoring and managing the risk ratings of employees.

3. Scope

This policy applies to all employees, contractors, and third-party agents associated with the Company who have access to financial systems, client information, and transaction data. Employees whose roles involve handling high-value transactions, sensitive data, or relationships with clients deemed to be high-risk will be subject to more stringent risk assessment and monitoring protocols.

The Compliance Officer is responsible for implementing the ERR process as required under Directive 8 of the FIC.

All employees must be risk-rated on appointment, and reassessed at least annually or upon material change in role or responsibilities. ERR results must be recorded, retained for 5 years after termination of employment, and integrated into HR access control and disciplinary processes.

All employees must be screened at least annually against sanctions lists and adverse media databases. High-risk staff shall be subject to enhanced oversight, including dual sign-off for transactions and more frequent training. The ERR Questionnaire forms part of the employee's compliance record.

4. Employee Risk Rating (ERR) Framework

4.1 Key Factors in Risk Rating

The risk rating process will assess employees based on the following criteria:

- Role and Responsibilities: The employee's position and the nature of their responsibilities. Employees in roles such as transaction monitoring, client onboarding, and financial reporting are inherently higher risk.
- Access to Sensitive Information: The level of access the employee has to confidential financial or client data.
- Exposure to High-Risk Transactions: Whether the employee is directly involved in transactions or clients flagged as high risk.
- Transaction Volume and Value: Employees who handle a high volume of transactions, particularly large-value or cross-border transactions, are subject to more frequent assessments.
- Past Compliance Record: Previous history of non-compliance or failure to adhere to AML/CTF regulations.

4.2 Risk Categories

Employees will be classified into three main categories based on their risk level:

- Low Risk: Employees with minimal exposure to high-risk transactions and limited access to sensitive information.
- Medium Risk: Employees who have moderate exposure to financial systems or are involved in occasional high-risk activities.
- High Risk: Employees directly responsible for transaction monitoring, client onboarding, and handling high-risk transactions or clients.

5. Risk Mitigation Measures

5.1 Enhanced Monitoring

Employees rated as high risk will be subject to enhanced monitoring. This includes:

- Regular audits of their transactions and activities.
- Additional scrutiny on transactions they handle, especially if linked to high-risk clients or geographies.
- Reporting suspicious activities to senior management and the Compliance Department

for further investigation.

5.2 Targeted Compliance Training

High- and medium-risk employees will undergo targeted AML/CTF compliance training, focusing on:

- How to identify suspicious transactions and behaviors.
- Proper reporting procedures in line with Directive 8.
- Ongoing updates on changes in AML and CTF regulations.

5.3 Regular Assessments

The Employees undergo risk screening and assessment. Risk assessment results and screening records must be retained on file.The Employee Risk Rating will be reviewed at least annually or whenever there is a significant change in the employee's role or responsibilities. New employees will undergo a risk assessment during the onboarding process.

6. Reporting and Escalation Procedures

Any employee who identifies or suspects a suspicious or unusual transaction must immediately report it to the Compliance Department, who will then escalate the issue to the Financial Intelligence Centre if necessary. Failure to report suspicious activities may result in disciplinary actions, including termination of employment, and could expose the institution to penalties under Directive 8.

7. Confidentiality and Data Protection

All data collected during the Employee Risk Rating process, including personal and sensitive information, will be handled with strict confidentiality. Access to risk rating results will be limited to senior management and the Compliance Department. The institution will comply with the Protection of Personal Information Act (POPIA) to ensure the security of employee data.

8. Responsibilities

8.1 Compliance Department: Responsible for overseeing the ERR process, conducting regular assessments, and ensuring that employees receive proper training on AML/CTF regulations.

8.2 Senior Management: Ensures that the ERR policy is implemented and adhered to across all departments.

8.3 Employees: All employees are expected to follow AML/CTF protocols and report any

suspicious transactions. Employees must also complete the Employee Risk Rating Questionnaire when required.

9. Employee Risk Rating Questionnaire

All employees are required to complete the Employee Risk Rating Questionnaire as part of this process. The questionnaire will gather information on their role, access to sensitive information, and involvement in high-risk transactions.

In the event that an employee also acts as a representative, a representative questionnaire will be issued to assess any associated risks. Monthly representative meetings will be conducted, and the outcomes of these engagements will form part of the employee's overall risk-rating criteria.

SCHEDULE 1 EMPLOYEES DECLARATION

DECLARATION TO BE SIGNED BY ALL EMPLOYEES

I, _____(Full Name), hereby declare the following:

(a) I have read the contents of this RMCP and I have attended the FICA training provided by the Company;

(b) I acknowledge that to the extent that I do not understand any of my duties under FICA or this RMCP, I have contacted the Compliance Officer for clarification; and

(c) I undertake to observe strictly and diligently all of my duties imposed by FICA and this RMCP, fully understanding that my failure to do so:

(i) will potentially expose the Company to unacceptable ML/TF risk, as well as financial and reputational risk from the penalties that may be levied by the FIC against the Company for any instances of non-compliance with FICA and this RMCP; and

(ii) is a criminal offence in terms of FICA and constitutes serious misconduct in terms of the Company's disciplinary code.

(d) I undertake to report any suspicious activity to the Compliance Officer and to comply fully with the Company's policies and procedures.

_____

Employee Signature

_____

Date

_____

Employee name (please print)

SCHEDULE 2 Client On-Boarding Checklist

It is also recommended to read this section alongside the Client Onboarding and Identification Manual.

Section A
Section B

SECTION A	GENERAL CLIENT INFORMATION

CLIENT NAME	

SECTION B	SPECIFIC DETAILS OF CLIENT – Please tick the relevant box and complete the relevant sections

INDIVIDUAL:	☐ South African ☐ Foreign

ADDITIONAL CHECKS
Company may be required to carry out additional checks and confirm that the information provided, is correct. You hereby consent to Company carrying out a credit check, if necessary. For any additional information, please contact Company's Compliance Officer for assistance.

Section B1

SECTION B1:	**FOR INDIVIDUALS**	PLEASE PROVIDE THE FOLLOWING DOCUMENTATION	***For office use***
ID/Passport numbers:		ID/passport or driver's licence	☐
Employment Status: Please select relevant status	☐ Salaried ☐ Unemployed ☐ Self-employed ☐ Student ☐ Retired ☐ Minor	No verification required	☐
Residential address:		Utility bill or similar	☐
Country of birth:		No verification required	☐
Tax registration number:		Proof of tax number	☐

SCHEDULE 3 FICA Risk Matrix Guidelines

This checklist must be completed when on-boarding any client.

Client Name: _____

Representative: _____Date: _____

Questions to be answered	Answer: Yes/No
1. Are there any High-Risk Client indicators in relation to this Client?	
2. Are there any High-Risk Transaction indicators in relation to the work to be performed for this Client?	
3. Based on the assessment of the Client and/or the work to be performed for this Client, will this Client be classified as a Standard Risk Client?	
4. Based on the assessment of the Client and/or the work to be performed for this Client, will this Client be classified as a High-Risk Client?	

CLIENT RISK INDICATORS	
Standard Client Risk indicators	**High Risk Client indicators**
● All natural and juristic persons who make a deposit into the Company's trust account ● Professional individual or partnership	FPEP No face to face interaction with Client Client based in high risk country Client has provided false or stolen identification Client whose source of funds not consistent with known legitimate income A reluctance or refusal to provide information An unusual or inexplicable preference for dealing with the Company via correspondence or via electronic media, as opposed to in

	person, particularly for the purposes of the CDD • A patent lack of concern or disregard for the costs involved • Deliberate evasiveness or vagueness when providing information • Any other conduct or circumstances that when viewed objectively, and when considered in light of all of the relevant factors taken as a whole, should be regarded with suspicion
TRANSACTION RISK INDICATORS	
Standard Risk Transaction indicators	**High Risk Transaction indicators**
• Nothing that raises any suspicions.	• An "unusual" financial or property transaction • Payments that are made to, or received from unrelated third parties
RISK SCORING GRID	

The Company applies a structured, point-based client risk-scoring methodology as part of its risk-based approach. This approach aggregates defined risk factors according to the BROKSTOCK Risk Matrix.

Each factor carries an associated score (0–100) and the total client risk score is calculated by applying the factor to each risk type and summing the results as reflected in Risk Matrix.

Client risk is determined across the following risk categories: Identity Risk, Geographic Risk, Screening Risk, Financial Risk, Business Risk, Product & Service Risk, R50k EDD trigger, and T&Cs Acceptance. Each underlying risk indicator within these categories is scored in accordance with the Matrix (0, 20, 40, 60, 80 or 100, depending on the inherent risk), and multiplied by factor applicable to that category. These scores produce a consolidated numerical risk score for the client.

The client's final ML/TF/PF risk rating is mapped directly to the scoring thresholds adopted by the Company:

• Low Risk: 0–40
• Medium Risk: 41–60
• High Risk: 61 and above

A score above 60 reflects heightened exposure and automatically triggers Enhanced Due Diligence, senior-management Compliance Approval, and enhanced ongoing monitoring (as per the continuous Due Diligence schedule aligned to these bands).

The final risk score and resulting classification must be recorded in the client file and retained as part of the onboarding record, together with a documented rationale for the assigned score.

High-risk clients may not be activated until Compliance has completed Enhanced Due Diligence and a designated senior manager has granted formal Compliance Approval.

If any one of the above is identified as High Risk, then the Company needs to obtain additional information regarding the source of funds/income to profile the Client accordingly. Refer to the Suspicious Transaction Indicators for assistance as well. This transaction must be authorised by the Section 42 Compliance Officer.

Additional Information Obtained:

_____

_____

_____

Section 42A Compliance Officer Signature:

_____

SCHEDULE 4 DPEPS FICA Checklist

This checklist must be completed with every FICA Related Transaction concluded with a DPEP Client Name: _____

Representative: _____Date: _____

DPEP		
Is the client one of the following or a close family member or closely associated with one of the following:	YES	NO
Heads of state, heads of Government and cabinet ministers		
Influential functionaries in Government		
Senior Judges		
Senior Political party functionaries		
Senior and/or influential officials, functionaries and military leaders and people with similar functions		
Member of ruling families		
Senior and/or influential representatives of religious organisations		

If YES, obtain additional information regarding source of funds, the transaction and the client.

Source of Funds/Income:

_____

_____

Transaction Details:

_____

_____

If client is a DPEP, please obtain senior management authorisation.

Section 42 Compliance Officer Signature:

_____

This relationship will be monitored on an on-going basis.

SCHEDULE 5 List of DPEP Positions

A domestic prominent influential person is an individual who holds, including in an acting position for a period exceeding six months, or has held at any time in the preceding 12 months, in the Republic:

(a) a prominent public function including that of:

(i) the President or Deputy President;

(ii) a government minister or deputy minister;

(iii) the Premier of a province;

(iv) a member of the Executive Council of a province;

(v) an executive mayor of a municipality elected in terms of the Local Government: Municipal Structures Act, 1998 (Act No. 117 of 1998);

(vi) a leader of a political party registered in terms of the Electoral Commission Act, 1996 (Act No. 51 of 1996);

(vii) a member of a royal family or senior traditional leader as defined in the Traditional Leadership and Governance Framework Act, 2003 (Act No. 41 of 2003);

(viii) the head, accounting officer or chief financial officer of a national or provincial department or government component, as defined in section 1 of the Public Service Act, 1994 (Proclamation No. 103 of 1994);

(ix) the municipal manager of a municipality appointed in terms of section 54A of the Local Government: Municipal Systems Act, 2000 (Act No. 32 of 2000), or a chief financial officer designated in terms of section 80(2) of the Municipal Finance Management Act, 2003 (Act No. 56 of 2003);

(x) the chairperson of the controlling body, the chief executive officer, or a natural person who is the accounting authority, the chief financial officer or the chief investment officer of a public entity listed in Schedule 2 or 3 to the Public Finance Management Act, 1999 (Act No. 1 of 1999);

(xi) the chairperson of the controlling body, chief executive officer, chief financial officer or chief investment officer of a municipal entity as defined in section 1 of the Local Government: Municipal Systems Act, 2000 (Act No. 32 of 2000);

(xii) A constitutional court judge or any other judge as defined in section 1 of the Judges' Remuneration and Conditions of Employment Act, 2001 (Act No. 47 of 2001);

(xiii) an ambassador or high commissioner or other senior representative of a foreign government based in the Republic; or

(xiv) an officer of the South African National Defence Force above the rank of major- general;

(b) the position of:

(i) chairperson of the board of directors;

(ii) chairperson of the audit committee;

(iii) executive officer; or

(iv) Chief financial officer,

of a company, as defined in the Companies Act, 2008 (Act No. 71 of 2008), if the company provides goods or services to an organ of state and the annual transactional value of the goods or services or both exceeds an amount determined by the Minister by notice in the Gazette; or

(c) the position of head, or other executive directly accountable to that head, of an international organisation based in the Republic.

This list is based on the definitions in the FIC Act Regulations and must be updated annually or upon legislative change.

SCHEDULE 6 Indicators of Suspicious Transactions

Indicators of Suspicious and Unusual Business:

- The client makes deposits of funds with a request for their immediate transfer elsewhere;
- Unwarranted and unexplained international transfers;
- The payment of commission or fees that appear excessive in relation to those normally payable;
- Lack of concern about high commissions, fees, penalties etc. incurred as a result of a particular type or method of transaction;
- Transactions do not appear to be in keeping with normal industry practices;
- Purchase of commodities at prices significantly above or below market prices;
- Unnecessarily complex transactions;
- Unwarranted involvement of structures such as trusts and corporate vehicles in transactions;
- A transaction seems to be unusually large or otherwise inconsistent with the customer's financial standing or usual pattern of activities;
- Buying or selling securities with no apparent concern for making profit or avoiding loss;
- Unwarranted desire to involve entities in foreign jurisdictions in transactions;
- A client attempts to convince employee not to complete any documentation required for the transaction;
- A client makes inquiries that would indicate a desire to avoid reporting;
- A client has unusual knowledge of the law in relation to suspicious transaction reporting;
- A client seems very conversant with money laundering or terrorist activity financing issues;
- A client is quick to volunteer that funds are clean or not being laundered.

Indicators in terms of Client Identification:

- The use of seemingly false identity in connection with any transaction, including the use of aliases and a variety of similar but different addresses and, in particular, the opening or operating of a false name account;
- Opening accounts using false or fictitious documents;
- A client provides doubtful or vague identification information;
- A client refuses to produce personal identification documents;
- A client changes a transaction after learning that he must provide a form of identification;
- A client only submits copies of personal identification documents;
- A client wants to establish identity using something other than his or her personal identification documents;
- A client's supporting documentation lacks important details such as contact particulars;

- Client does not want correspondence sent to his/her home address.
- A client inordinately delays presenting corporate documents; or

General Indicators of Suspicious Behaviour:

- A client provides insufficient, vague or suspicious information concerning a transaction;
- Accounts that show unexpectedly large cash deposits and immediate withdrawals;
- Client appears to have accounts with several financial institutions without no apparent reason;
- Involvement of significant amounts of cash in circumstances that are difficult to explain.

SCHEDULE 7 FICA Recordkeeping Checklist

This checklist must be completed with every FICA Related Transaction. Records must be kept for a minimum period of 5 years. This checklist must be kept in a FIC Record File, together with the Risk Rating and DPEPs Checklist.

Client Name: _____

Representative: _____

Date: _____

Who established the client's identity	
How was the identity established (Attach duly completed and checked Client On-Boarding Checklist)	
Single transaction/Business Relationship	
What is the transaction amount	
What is the name of the parties involved	

SCHEDULE 8 Verification of Physical Address

Verification report if client does not have an acceptable account held in the client's name.

I, the undersigned, …….

Hereby confirm that:

1) I am currently employed by / am an agent for _____

2) On (DATE), I physically visited and inspected the residential address of our client; …….....

3) His/her physical residential address is

……which I confirmed by obtaining the following information:

……
……
……
……
……

…… SIGNED at …….. on this …….. DAY of

…….

……

….. (SIGNATURE)

SCHEDULE 9 List of FPEPS

A foreign prominent public official is an individual who holds, or has held at any time in the preceding 12 months, in any foreign country a prominent public function including that of a:

(b) Head of State or head of a country or government;

(c) member of a foreign royal family;

(d) government minister or equivalent senior politician or leader of a political party;

(e) senior judicial official;

(f) senior executive of a state-owned corporation; or

(g) high-ranking member of the military.

All foreign prominent public officials must be treated as high-risk clients. Senior management approval is required prior to establishing the relationship. Enhanced Due Diligence is mandatory, including establishing source of wealth and source of funds.

This list must be reviewed annually and updated in line with the Regulations.