DATE: 20 AUGUST 2020

RISK MANAGEMENT AND COMPLIANCE PROGRAMME

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

FOR

[BCS MARKETS SA (PTY) LIMITED]

TABLE OF CONTENTS

1. ADOPTION OF THIS POLICY

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

Name		**Signature**

The section 43 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.

Name		**Signature**
[ ]		

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.

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 0.

2.9 "**Company**" means BCS Markets SA (Pty) Limited.

2.10 "**Compliance Officer**" means the Compliance Officer of the Firm appointed in terms of section 43 of FICA.

2.11 "**CRM**" means [Please complete]

2.12 "**DPIP**" means a domestic prominent public influential person, being any person, or immediate family member or known close associate of a person as listed in Schedule 3A of FICA and 0 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 "**FPPO**" means a foreign prominent public official, 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 0 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 Firm for legal 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 DPIPs and FPPOs, 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 Firm.

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 endeavours 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 incumbent upon the Company's directors and other Employees to familiarise themselves with the Company's RMCP and sign the declaration (Schedule 1) once the RMCP has been read and understood.

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.

5. RESPONSIBILITY AND COMPLIANCE

5.1 Every Employee is required to sign a declaration that they have read and understand this RMCP.

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

5.3 The Compliance Officer will review (and if necessary, update) this Policy annually.

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 Firm's RMCP (as the case may) will be formally disciplined in accordance with the Firm's disciplinary policy and procedure.

6. APPOINTMENT AND RESPONSIBILITY OF COMPLIANCE OFFICER

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

6.2 The Firm 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 Firm's Board of Directors in carrying out the responsibility for the effective management of the Firm's RMCP.

6.3 The Compliance Officer is responsible for:

6.3.1 ensuring the submission of all cash threshold reports as well as suspicious or unusual transaction reports to the FIC;

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

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

6.3.4 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;

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

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

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

6.3.8 seeing to the Company's effective implementation of this RMCP.

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 Onboarding and Identification manual of BCS Markets SA.

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.

8. VERIFICATION PROCEDURE

8.1 There are different types of clients, and each of them requires their own identification and verification:

8.1.1 South African citizens or residents;

8.1.2 foreign nationals;

8.2 Verification Documents

8.2.1 The Company has adopted the BCS CRM system to assist with gathering verification documents. BCS CRM is a web-based application that assists in collating and submitting FICA documentation. Whilst CRM is a very useful system in this regard it remains the responsibility of Employees to ensure that verification documentation is submitted by their respective Clients.

8.2.2 At all times CRM will work together with the automatic KYC system. The detailed description of automatic KYC system can be found in Onboarding and Identification manual of BCS Markets SA.

8.2.3 0 of this RMCP contains the on-boarding checklist which will be completed by the Prospective Clients and/or Clients (as the case may be) online to ensure compliance with FICA and this RMCP.

8.2.4 All the required information must be obtained, the information must be verified against the original documentation or by electronic verification software and the necessary copies of the original documents must be kept as part of the record keeping duty.

8.2.5 As part of the customer acceptance process, the relevant Employee is required to ensure that the:

(a) Client On-Boarding Checklist (i.e. 0) is completed by the Prospective Client / Client, completed and the necessary documents provided by the Client. The Compliance Officer is required to ensure that all required documentation is received and verified by the Company for each Client;

(b) Risk Matrix Checklist (i.e. 0) is completed; and

(c) DPIP Checklist (i.e. 0) is completed.

8.3 Maintaining the correctness of Client's Particulars (Current Clients)

8.3.1 The Company is required to take reasonable steps, in respect of a Business Relationship, to maintain the correctness of particulars which are susceptible to change. The company will perform ongoing checks of Client's identity and his/her status on applicable witch and sanctions lists.

8.3.2 The "Know your Client" procedure must be performed every time the Company enters into a transaction with the Client. Should any Employee become aware of

changes in a Client's particulars, the new information should immediately be obtained.

8.4 **Additional Measures when representing another**

8.4.1 An Accountable Institution must, in addition to the normal identification and verification requirements, obtain from an individual information which provides proof of his authority to act on behalf of a Client.

8.4.2 This includes a Mandate or Power of Attorney.

9. RISK-BASED APPROACH

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

9.2 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.

9.3 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.

9.4 By applying a risk-based approach, Accountable Institutions are able to ensure that measures to prevent or mitigate ML/TF are commensurate with the risks identified.

9.5 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.

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

9.7 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.

9.8 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.

9.9 **Standard Risk Clients**

The following Clients are accepted as Standard Risk Clients:

9.9.1 Local Clients;

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

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

9.10 **High Risk Clients**

9.10.1 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 FPPO. This includes family members and known close associates of FPPO'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.

9.10.2 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) cross-border transactions; or

(e) payments made by cash which exceed R100,000.00 (one hundred thousand Rand).

9.10.3 Employees must refer to the Company's Risk Matrix guidelines in addition to the On-boarding Checklist to profile a client.

9.10.4 0 of this RMCP sets out the Company's Risk matrix guidelines.

9.11 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 or legal person. The Company has identified the following additional measures to be taken when dealing with such Clients:

9.11.1 Customer identification can be carried out via both web and mobile applications of BCS. Before establishing relationship with the customer the BCS will require the customer to upload the photo (scan) of at least two identification documents. The documents will be submitted to BCS.

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

(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. 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.

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

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

9.12 **Anonymous or Fictitious Clients**

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

9.12.2 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.

9.13 **DPIP**

9.13.1 Automatic AML system SumSub will be used to identify whether a Client is a DPIP, the responsible Employee check results of the DPIP checklist check which correspond the checklist set out in 0 of this RMCP. A list of DPIP positions is also annexed as 0 of this RMCP. Additionally all clients must be asked whether they fall into this category.

9.13.2 Business Relationships or Single Transactions with DPIPs are not inherently high-risk. However, due to their position and influence, it is recognised that many DPIPs are in positions that potentially can be abused for the purpose of committing ML/TF offences and related predicate offences, including corruption and bribery.

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

(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.

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

9.14 **FPPO**

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

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

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

9.15 **Secondary Accountable Institutions**

9.15.1 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 other

prescribed 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,

9.15.2 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.

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

A client who is also citizen of a country that is **not** indicated on the financial actions task force member states and observers list would be considered a high-risk client. The list of member states is frequently updated and may be viewed by navigating to the following internet website link:

(https://www.fatf-gafi.org/about/membersandobservers/#d.en.3147)

10. DUTY TO MAINTAIN RECORDS

10.1 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.

10.2 **What records must be kept?**

The Company is required to keep the following records:

10.2.1 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;

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

10.2.2 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 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.

10.3 **Recordkeeping period**

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

10.3.2 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.

10.3.3 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.

10.3.4 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.

10.4 **General Provisions, Processes and Responsibility**

10.4.1 FICA Recordkeeping Checklist*:* The required detail regarding the transactions will be completed on the FICA Recordkeeping Checklist (which is linked to CRM) (see 0). 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.

10.4.2 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.

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

10.4.4 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.

10.4.5 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.

10.5 **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.

10.6 **FIC's Access to Records**

10.6.1 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.

10.6.2 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.

11. ADVISE FINANCIAL INTELLIGENCE CENTRE OF CLIENTS

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

11.2 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.

12. 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. 0 contains a list of indicators of suspicious transactions.

12.1 **Who must Report:**

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

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

12.2.1 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.

12.2.2 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.

12.2.3 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.

12.3 **What constitutes a suspicion?**

12.3.1 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.

12.3.2 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.

12.3.3 There are indicators of suspicious behaviour at 0 but they should not be viewed in isolation and should always be considered in conjunction with other circumstances.

12.4 **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.

12.5 **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.

12.6 **Confidentiality and Privilege**

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

12.7 **Legal protection for the Reporter**

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

12.7.2 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.

12.8 **Tipping-off**

12.8.1 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.

12.8.2 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.

12.8.3 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.

12.9 **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.

12.10 **Method of Reporting**

12.10.1 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.

12.10.2 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.

12.10.3 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).

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

12.10.5 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.

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

12.10.7 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.

12.10.8 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.

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

12.10.10 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.

13. 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.

13.1 Who must receive Training?

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

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

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

13.2 Who must provide the Training?

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

14. POPI COMPLIANCE

14.1 The Company will 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.

14.2 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.

14.3 The Company will not ask for more personal information than what is needed for FICA purposes.

14.4 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.

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

SCHEDULE 1

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.

_____
Employee Signature

_____
Date

_____
Employee name (please print)

SCHEDULE 2 - Client On-Boarding Checklist

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		No verification required	☐
	☐ Self-employed	☐ Student			
	☐ Retired	☐ Minor			
Residential address:				Utility bill or similar	☐
Country of birth:				No verification required	☐
Tax registration number:				Proof of tax number	☐

Section D
Section E
Additional checks

SECTION D: PARTICULARS OF PERSON RESPONSIBLE FOR PAYMENT OF ACCOUNT		PLEASE PROVIDE THE FOLLOWING DOCUMENTATION	*For office use*
Full name:		ID/passport or driver's licence	☐
Email address:			☐
Telephone number (business):			☐
Cellphone number:			☐
VAT number:		Proof of VAT number	☐

SECTION E: ADDITIONAL INFORMATION					
Source of Funds: *(Please select)*					
(Activity that generates the funds for a particular business relationship /occasional transaction)	☐	Allowance	☐	Bursary	No verification required, unless specifically requested ☐
	☐	Company profits	☐	Company sale or sale of interest in company	
	☐	Court order	☐	Director/member of company/CC	
	☐	Director/owner of own business	☐	Dividends from investments	
	☐	Divorce settlement	☐	Encashment claim	
	☐	Gift/donation	☐	Income from employment	
	☐	Income from previous employment	☐	Inheritance	

	Loan		Lottery/gambling winnings		
	Maintenance		Maturing investments		
	New investment		Other		
	Pension		Private capital raise		
	Sale of asset/property		Sale of shares		
	Savings		Cryptocurrency		
	Deceased estate				

Source of Wealth:
(Please select)

(Activities that have generated the total net worth of client)

	Allowance		Bursary	No verification required, unless specifically requested	
	Company profits		Company sale or sale of interest in company		
	Court order		Director/member of company/CC		
	Director/owner of own business		Dividends from investments		
	Divorce settlement		Encashment claim		
	Gift / donation		Income from employment		
	Income from previous employment		Inheritance		
	Loan		Lottery/gambling winnings		
	Maintenance		Maturing investments		
	New investment / capital		Other		
	Pension		Private capital raise		
	Public capital raise		Sale of asset/property		
	Sale of shares		Savings		
	Cryptocurrency		Deceased estates		

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 Firm's trust account • Professional individual or partnership	• FPPO • 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 Firm 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

If any one of the above is identified as High Risk, then you need 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 authorized by the Section 43 Compliance Officer.

Additional Information Obtained:

_____

_____

_____

Section 43 Compliance Officer Signature:

_____

SCHEDULE 4 - DPIPS FICA Checklist

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

Representative: _____Date: _____

DPIP		
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 DPIP, please obtain senior management authorization.

Section 43 Compliance Officer Signature:

_____

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

SCHEDULE 5 - List of DPIP 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.

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 DPIPs 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 FPPOS

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.