FICA AND AML POLICY

Type of policy:	FICA and AML Policy
Executive summary:	The scope of this policy is applicable to Constantia Risk and Insurance Holdings (Pty) Limited (CRIH) and its insurance subsidiaries including Constantia Life Limited (CLL). Ensuring the policy is aligned to the relevant regulations in terms of FICA Amendment Act. Scope of policy applicable to Constantia Risk and Insurance Holdings (Pty) Limited and its subsidiaries. The FICA Amendment Act requires that every accountable institution has a board approved FICA and AML Policy.
Area of governance:	Compliance
Approving authority:	The Board of Constantia Risk and Insurance Holdings (Pty) Limited
Group Exco sponsor:	Chief Executive Officer
Responsible department:	Enterprise Risk Management
Date of approval:	10 September 2021
Review frequency:	Biennial (every two years)
Date of next review:	September 2024
Version:	V3.0
Draft resolution:	The Insurance companies within the Constantia Risk and Insurance Holdings (Pty) Ltd group of companies recognise the value as well as the risks associated with the Regulatory requirements pertaining to their activities. This policy statement and framework has been approved by the Board of Directors of each of the above listed insurers who have duly authorised the signatories to this document. The Board is required to approve the policy in line with regulations as specified in the FICA amendment Act.

SIGNED AT Kyalami ON THE DAY 09 OF April 2024

Themba Baloyi
Themba Baloyi (Apr 9, 2024 09:11 GMT+2)

TP BALOYI
CHAIR OF THE BOARD
INDEPENDENT NON-EXECUTIVE

SIGNED AT Table View ON THE DAY 9 OF April 2024

Lusani Mulaudzi (Apr 9, 2024 13:25 GMT+2)

LK MULAUDZI
CHAIR OF THE JOINT RGA COMMITTEE
INDEPENDENT NON-EXECUTIVE

Table of Contents

1. DEFINITIONS

TERM	DESCRIPTION
Accountable Institution (AI)	An Accountable Institution is any person or entity as described in Schedule 1 of the FICA who must ensure adherence to the legal requirements and responsibilities as set out therein.
Anti-Money Laundering/Combating the Financing of Terrorism (AML/CFT)	In relation to AIs, money laundering (ML)/terrorism financing (TF) risks are threats and vulnerabilities which put AIs at risk of being abused to facilitate ML/TF activities.
Business Entity	All entities within Constantia insurance businesses. Business Entities may be statutory entities or business divisions, but with the governance oversight requirements provided on a group level.
Business Partner	The term "business partner" includes, but is not limited to, the following: • any party, other than an intermediary or client or employee, with whom Constantia has entered into a business arrangement; • any joint venture partners; • any party that performs services on behalf of Constantia; • any party to whom Constantia refers any business or outsources any part of its business to; and any party that performs any services to a client of Constantia in terms of an agreement or arrangement between the client and Constantia.
Business Relationship	An arrangement between a client and an AI for the purpose of concluding transactions on a regular basis (i.e., entering into a relationship which gives rise to the issuing of an insurance policy, including an undertaking to pay premiums under a policy).
Business Day	Any day other than a Saturday, Sunday or public holiday in the Republic of South Africa.

TERM	DESCRIPTION
Constantia	Constantia Risk and Insurance Holdings Proprietary Limited; and Constantia Life Limited.
Compliance Risk (Constantia definition – Source Group Compliance Policy)	The current and prospective risk of damage to Constantia's business model or objectives, reputation and financial soundness arising from non-adherence with regulatory requirements and failure to uphold the core values and code of Ethical Conduct of Constantia.
Confirmed Positive	An instance of a party whose appearance on a sanction list or reputation source has been confirmed as relevant to this particular party.
Country Risk	Denotes the risks associated with the AI or one of its branches or subsidiaries being located in a specific geographical location. Several factors should be considered when assessing this risk, viz, whether: • any of the AI's foreign operations are conducted via third parties; • Management has adequate and effective oversight over the foreign operations of the AI; • the AI requires any regulatory or statutory approvals or registrations to operate its business in its home-country or foreign jurisdiction; The local or foreign jurisdiction: • is subject to a United Nations Security Council (UNSC) resolution; • is on the Financial Action Task Force's non-co-operative countries and territories (NCCT) list; • is subject to sanctions or similar measures from regional bodies or groupings; • is designated as having insufficient AML/CFT policies and procedures by FATF; • has been assigned an amber or a red rating in terms of Transparency International's Corruption Perception Index (TICPI);

TERM	DESCRIPTION
Country Risk	• is known to be a high-risk jurisdiction for money laundering, financing of terrorism, tax evasions, bribery and corruption; and • is currently experiencing political or civil unrest or has experienced any such unrest in the last 6 months.
Customer (Client)	Any person who: • purchases or owns a product distributed or sold by Constantia, or is a beneficiary of such product; • receives a product or service from Constantia; • enters a business relationship or a single transaction with Constantia; • enters into any agreement in respect of the first or third item above, or a person who on behalf of someone else enters into such an agreement.
Customer Due Diligence (CDD)	A term used for customer identification process. It involves making reasonable efforts to determine: • the true identity and beneficial ownership of accounts; • source of funds; • the nature of customer's business; • Reasonableness of operations in the account in relation to the customer's business, etc. This in terms helps institutions to manage their risks. The objective of the KYC guidelines is to prevent institutions being used, intentionally or unintentionally by criminal elements for money laundering. For the purpose of KYC, a "customer" may be defined as: • a person or entity that maintains an account and/or has a business relationship with Constantia; • one on whose behalf the account is maintained (i.e., the beneficial owner); • beneficiaries of transactions conducted by professional intermediaries; • any person or entity connected with a financial transaction which can pose significant reputational or other risks to Constantia.

TERM	DESCRIPTION
Dual Citizenship	A person who has a dual citizenship is a citizen of two countries. Like a regular citizen, the person must abide by each country's laws, but also gains access to special government programs only allowed to citizens.
Due Diligence	"Due diligence" generally refers to the care a reasonable person should take before entering into a relationship, an agreement or a transaction with another person. See also: Enhanced Due Diligence, Customer Due Diligence (CDD) and Ongoing Due Diligence.
Enhanced Due Diligence	A next level of due diligence on parties that have been identified as high-risk during the Party Due Diligence process. This requires additional information about the party as well as identifying specific controls to put in place to manage the risk identified. *Note: in context of Relationship Management for Party Due Diligence, the term "High-Risk Party Maintenance" is used rather than "Enhanced Due Diligence" (Enhanced Due Diligence being part of, rather than additional to, Party Due Diligence). The PDD Capability Model's definition for High-Risk Party Maintenance is given in section 5, par. "Relationship Management Overview".* See also: Due Diligence and Customer Due Diligence (CDD).
False Negative	An instance of a party that fails to be matched to a sanction list or reputation source during screening, when in actual fact the party does appear on a sanction list or reputation source.
False Positive	An instance of a party that has been matched to a sanction list or reputation source during screening, but the match has subsequently been proven as incorrect.

TERM	DESCRIPTION
FATF	The Financial Action Task Force, an inter-governmental policy making body that has a Ministerial mandate to establish international standards for combating money laundering and financing of terrorism.
FIC	The Financial Intelligence Centre is a unit established in terms of the FICA to ensure compliance with the FATF standards.
FICA	The Financial Intelligence Centre Act, 38 of 2001.
Terrorism Financing	Terrorism Financing includes the financing of terrorist acts and of terrorists and terrorist organisations. Consequently, terrorist financing offences relate to any person who wilfully provides or collects funds with the unlawful intention (or in the knowledge) that they are to be used by terrorist organisations to carry out an attack.
GoAML	The software solution implemented by the FIC as its preferred IT platform for registration, reporting, data collection, analysis, case management and secure communications required for the FIC's daily operational functions and requirements.
Intermediary	The term "intermediary" includes, but is not limited to, the following: • any financial advisor employed by or contracted to a business in Constantia; • any broker contracted to a business in Constantia; • any natural person or entity performing an intermediary service as foreseen in the Financial Advisory and Intermediary Services (FAIS) Act in respect of a Constantia business, including any natural person or entity performing similar services outside of South Africa; and • any other person or entity, regardless of location, that refers business to an entity in Constantia (including investment product consultants).

TERM	DESCRIPTION
Money Laundering (Source: Prevention of Organised Crime Act 121 of 1998)	An activity which has or is likely to have the effect of concealing or disguising the nature, source, location, disposition or movement of the proceeds of unlawful activities or any interest which anyone has in such proceeds and includes any activity which constitutes an offence in terms of section 64 of the FICA or section 4, 5 or 6 of the Prevention of Organised Crime Act 121 of 1998.
Party	A natural person or entity with whom Constantia has or intends to have a relationship, the nature of which includes the following: • Customer; • Third party – either Business Partner or Intermediary; • Employee.
Party Due Diligence (PDD)	The knowledge that an AI has about its client and the institution's understanding of the business that the client is conducting with it.
Prospective Client	Means a person/s seeking to conclude a business relationship or a single transaction with the AI.
PEP	Refers to Politically Exposed Persons: • Foreign PEPs are individuals who are or have been entrusted with prominent public functions by a foreign country. • Domestic PEPs are individuals who are or have been entrusted domestically with prominent public functions. • PEPs refer to members with senior ranking and is not intended to cover middle ranking or more junior individuals in the foregoing categories.
PIP	Refers to a Domestic Prominent Influential Person as per the definition in the FICA, as amended.

TERM	DESCRIPTION
PPO	Refers to a Foreign Prominent Public Official as per the definition in the FICA, as amended.
RMCP	The Risk Management and Compliance Programme, as provided in section 42 of the FIC Amendment Act 1 of 2017.
Sector Risk	Certain industry sectors present potentially higher AML/CFT related risks than others. Doing business with customers in these sectors may therefore expose Constantia to higher risks. Several factors should be considered when assessing this risk, viz, whether the AI conducts transactions with businesses in: • Extractive industries; • Defence and armaments manufacturers; • Construction, infrastructure and development industries; • Sectors where government approval/authority to operate is required (e.g., property industry); • Sectors which conduct most of their business with governmental or quasi-governmental or parastatals entities; • Sectors with a large percentage of PIPs or entities controlled by PIPs; and • State/government-controlled entities or entities managed by PIPs.
Special Interest Person	SIPs are people who are accused of, convicted, arrested or undergoing trial for financial or serious crime such as including financial crime, organised crime, terrorism, drug trafficking, crime, war crimes and other crimes.
Transaction	A transaction concluded between a client and an AI in accordance with the type of business carried on by that institution.
Single Transaction *(Not relevant to CRIH business)*	A transaction other than a transaction concluded during a business relationship and where the value of the transaction is not less than R5 000.

2. POLICY STATEMENT AND PREAMBLE

2.1 Constantia is committed to establishing and maintaining an internal culture of awareness and vigilance with respect to anti-money laundering and counter terrorism financing, and to this end strives to comply with the letter and the spirit of all statutes, regulations and supervisory requirements that apply to its businesses, and is committed to ensuring compliance with provisions of the FICA.

2.2 Constantia Life Limited as a life insurance company, is an accountable institution that must comply with anti-money laundering and counter terrorist financing laws.

Constantia has also adopted the following policies which reinforces Constantia's commitment to AML/CFT:
1. Constantia Group Governance Policy
2. Constantia Group Compliance Policy
3. Constantia Group Code of Ethical Conduct

3. PURPOSE

3.1 The purpose of this document is to describe the minimum standards that will ensure that Constantia can meet their obligations in terms of the RMCP as described in the FICA. The RMCP sets out how a risk-based approach will be adopted by Constantia to comply with the FIC Amendment Act 1 of 2017.

4. RISK BASED APPROACH

4.1 The FIC Amendment Act 1 of 2017 requires AIs to apply a risk-based approach when carrying out Customer Due Diligence (CDD) measures. In terms of the risk-based approach AI's must have systems and controls that are commensurate with the specific risk of ML/TF that applies to them. The important steps in creating the RMCP is to identify, assess, monitor, mitigate and manage those risks.

4.2 In relation to AI's, ML/TF risks are threats and vulnerabilities which put the AIs at risk of being abused in order to facilitate ML/TF activities. These relate to the potential that clients, by using the AI's products and services, can exploit the AIs to promote money laundering or terrorist financing activities. The nature of these risks relates to several aspects, including the features of the intended target market of clients who are likely to use an AI's range of products and services, the geographic locations of an AI's operations and of its clients, the delivery channels through which persons become clients of an AI or through which clients access its products and services, the features of a particular product or service, etc.

5. CONSTANTIA RISK MANAGEMENT – IDENTIFICATION OF RISKS AND FACTORS TO BE CONSIDERED WHEN IDENTIFYING RISKS

5.1 Products and services:

5.1.1 **Attributes associated with <u>low-risk products & services:</u>**

5.1.1.1 No accumulation for cash values during the lifetime of the product.

5.1.1.2 Product provides a structured flow of transactions.

5.1.1.3 Access to funds restricted to specific contractual events.

5.1.1.4 Specified termination dates or events.

5.1.1.5 Uncertain insured event.

5.1.1.6 No access to funds at early termination.

5.1.1.7 Benefits only payable at stage of claim for specified insured event.

5.1.1.8 Contributions are limited by legislation or regulation.

5.1.1.9 Benefits governed by specific regulatory- and tax regimes.

5.1.1.10 Not available to retail investors.

5.1.1.11 Cannot be offered as security or ceded.

5.1.1.12 Funds linked to a specific source:

(a) Estate

(b) Order of court

(c) Retirement fund benefits

(d) Employer Administrative service only.

Product	Assessed risk
Risk Products, including Group Life Insurance, Spouses Insurance, Severe Illness, Funeral Insurance, Lump Sum Disability Insurance, Income Continuation Insurance	Low
Retirement Annuities	Low
Retirement Funds	Low
Funeral Products including Group Scheme Funeral Plans	Low
Life, Disability, Health, Assistance Business	Low

5.1.1.13 The assessment has determined that Constantia's insurance products are low-risk products in terms of the attributes above.

5.1.2 **Attributes associated with <u>medium risk products or services:</u>**

5.1.2.1 Accumulation of cash values.

5.1.2.2 Lump sum payments, including ad-hoc lump sum payments.

5.1.2.3 Can be offered as security and be transferred to another person (ceded).

5.1.2.4 Can be accessed without any restrictions.

5.1.2.5 Online transactions and automated access.

5.1.2.6 Access to the values may be limited by legislation.
5.1.2.7 Allows for restricted number of withdrawals.
5.1.2.8 Access to primary benefits only at claim stage but have access to cash during the lifetime of the product.

5.1.3 **Attributes associated with high-risk products and services:**
5.1.3.1 Transparency is limited in respect of source of funds.
5.1.3.2 Funds can be accumulated and easily accessed.
5.1.3.3 Unlimited contributions and withdrawals.
5.1.3.4 Product allows for investment in or via a foreign jurisdiction(s).
5.1.3.5 Investments are made with discretionary money.
5.1.3.6 Significant fund flows are involved.

5.1.3.7 None of Constantia's insurance product fall within the ambit of high-risk and medium-risk products and services.

5.1.4 **Attributes associated with low-risk clients:**
5.1.4.1 Client information, including source of funds, easily verifiable.
5.1.4.2 High levels of transparency and publicly available information.
5.1.4.3 Regulated persons, natural as well as juristic.

Client Type	Assessed risk
Natural Person: Salaried, employed individuals	Low
Natural Person: Pensioners	Low
List Companies	Low
Retirement Funds	Low

5.1.4.4 Constantia's clients fall within the low-risk clients portfolio.

5.1.5 **Attributes associated with medium risk clients:**
5.1.5.1 Information of client, including income or source of funds, only verifiable with some effort.

5.2 Clients linked to high-risk industries:
5.2.1 Extractive industries.
5.2.2 Defence and armaments manufacturing.
5.2.3 Construction, infrastructure and development industry.
5.2.4 Governmental / Quasi-governmental & State-owned entities.

5.3 Limited levels of transparency and publicly available information

Client Type	Assessed risk
Natural Person: High Net-worth Individual. An individual with investable assets of R10 million or more.	Medium
Natural Person: Self-employed individuals	Medium
Natural Person PIP	Medium
Retirement Funds in specified industries	Medium
Private Companies	Medium
Family Trusts & Schools	Medium
Religious Organisations	Medium
Non-Profit Organisations (NPOs) and Non-Governmental Organisations	Medium

5.4 Attributes associated with high-risk clients

5.4.1 Foreign PPOs.
5.4.2 Associated with government or high-risk parties.
5.4.3 Acting as agents or representatives for other high-risk parties.
5.4.4 Complex ownership structures.
5.4.5 Clients in high-risk business sectors.

Client Type	Assessed risk
Natural Person: PPO	High
State Owned Entities	High
Trusts	High
Political Parties	High
Trust Companies	High
Sectors which conduct most of their business with governmental or quasi-governmental or parastatals entities	High
Defence and armaments manufacturing	High
Construction, infrastructure, and development industry	High
Attorneys	High

5.5 Transactions

Transaction Types	Risk Factor Considerations
Business Relationships: Agreement or mandate between the client and product/service provider for the provision of products or services	Consider the risk associated with the transaction when: • entering into a new agreement or accepting a new mandate; • amending an existing agreement or mandate; • terminating the agreement or mandate.
Contributions (Money In)	For each contribution type, consider the risk associated with each of the following payment methods:

Transaction Types	Risk Factor Considerations
	• cash or cash equivalents such as cash into the institution's bank account; • direct deposits other than cash;
Initial contribution	Recurring
Initial contribution – Once-off	Once-off
Ad-hoc contributions	Not contractually provided for
Recurring contributions	Contractually provided for
Payments and Exits (Money Out)	Consider the risk associated with the transaction when: • money is transferred to the client's bank account in the same jurisdiction; • money is transferred from one institution to another for the benefit of the client; • payment is made to a third party or third-party bank account in the same jurisdiction.
Transfer of ownership to a third party	Commence due diligence process on the new owner of the account.
Termination of Business Relationships:	
Lapses – no flow of money	
Cooling-off	Consider the reasons advanced for termination.

5.6 Delivery Channel

Delivery Channel	Assessed risk
Constantia Advisers (including those managed in terms out outsourced arrangements) – conform to Constantia standards and requirements.	Low
Brokerages within Constantia – managed according to the same standards required of all legal entities within Constantia.	Low
Direct face to face engagement with clients – Constantia employees are managed in a structured environment that conforms to Constantia standards.	Low
Independent brokers (other than Bank or Corporate Brokerages) – although there is a contractual relationship and brokerages are subject to the same regulatory requirements and oversight, compliance oversight may be limited.	Medium
Front Offices – although these functions are governed by an outsourcing or binder agreement, this type of arrangement poses a higher risk due to potentially inadequate processes.	Medium

5.7 Geographical Location

5.7.1 The Country Risk Management Model (the model) was prepared as a generic model which can be used by any business situate in any jurisdiction. It is a tool which assists a business in understanding the potential risk associated with:

5.7.1.1 doing business in a country from a due diligence perspective; or

5.7.1.2 a potential client resident in or born in any of the countries listed in the model; and

5.7.1.3 The transfer of funds to or from a bank account situate in any of the countries listed in the model.

5.7.2 Each country has been allocated a risk rating based on a number of considerations and an assessment of various international resources relating to anti-money laundering and the countering of the financing of terrorism (AML/CFT), sanctions and anti-bribery and corruption (ABC).

5.7.3 The model also lists the "Constantia footprint" – in other words, whether Constantia does business in a specific country where the business is regarded as a group company, group associate or a managed fund.

5.7.4 Rationale for the risk ratings associated with the Country Risk Management Model

5.7.4.1 Sanctions: If any sanctions regime imposed by one or more of the United Nations (UN), Office of Foreign Assets Control (OFAC), European Union (EU) or the Treasury of the United Kingdom (UK HMT) in respect of a country, that country is automatically categorised as extremely high-risk. The overall PDD risk indicator for that county will refer to "sanctioned". Any business relationship or transaction in respect of which a "sanctioned country" indicator applies must be flagged for review regardless of the level of risk indicated by the other risk factors. The business relationship or transaction may only continue after a review in terms of the business' internal PDD review process, including senior management approval where appropriate.

5.7.4.2 AML/CFT: If a country is regarded as a *"High-Risk & Non-Cooperative Jurisdiction"* or *"Improving Global AML/CFT compliance: On-going process",* that country is categorised as high-risk even if it is a Financial Action Task Force (FATF) member. The overall PDD risk associated with this country will always be high. If a country is not a FATF member, that country will be categorised as medium risk if it is not marked as "High-Risk & Non-Cooperative Jurisdiction" or "Improving *Global AML/CFT compliance: On-going process" that country is marked as low risk.*

6. PARTY DUE DILIGENCE (PDD) REQUIREMENTS

6.1 Introduction

6.1.1 PDD measures, if properly implemented, enables an AI to better manage its relationships with clients and to better identify possible attempts by clients to exploit the institution's products and services for illicit purposes. Requiring AIs to apply PDD is a key component of a framework to combat money laundering and terrorism financing effectively.

6.1.2 Previously AIs were required to establish and verify the identity of a client in accordance with the AML/CFT Laws. The principle of client identification and verification is now expanded significantly with the introduction of the obligation to conduct PDD. As a result, the regulations and exemptions relating to client identification and verification have been amended significantly to align with the amendments to the FICA, with most of the regulations having been repealed and exemptions having been withdrawn.

6.1.3 This, combined with the obligation to apply a risk-based approach, gives AIs greater discretion to determine the appropriate compliance steps to be taken in given instances. This means that AIs now have the flexibility to choose the type of information by means of which it will establish clients' identities and the means of verification of clients' identities, instead of following the rigid steps provided for in the AML/CFT laws.

6.1.4 AIs should use the findings from their risk assessment to decide on the appropriate level and type of PDD that they will apply to a client (or business relationship and single transactions). AIs should also determine when they consider persons to be prospective clients to whom their PDD measures apply. An AI's RMCP must describe the PDD measures which the institution applies and how these measures are attenuated or intensified based on ML/TF risks.

6.2 Identification of Compliance Obligations

6.2.1 The FICA, FATF Recommendations as well as other legislative requirements, locally and internationally, requires an identification, analysis and understanding of the compliance obligations imposed on Constantia. The below obligations have been identified as being the key components which should facilitate the effective implementation of a RMCP:

6.2.1.1 Overall Risk Context: The overall risk context is based on an assessment of the Constantia overall risk exposure to money laundering and terrorist financing. The overall risk context comprises:

(a) Conducting a static risk assessment which comprises an analysis of several generic risk factors as well as internal factors unique to Constantia.

(b) Consideration of the dynamic risk factors which are related to the specific product, customer, transaction, and delivery channel, source of funds and area of jurisdiction.

(c) Constantia has been classified as Low-risk business.

6.3 **Establishment and verification of the identity of clients**

6.3.1 PDD begins with AI knowing the identity of its clients.

6.3.2 Establishing the client's identity requires obtaining a range of information about the client.

6.3.3 Verification of the information obtained by comparing it against the original source or reliable third party. Such verification must be completed before the transaction is concluded.

6.3.4 Constantia has, based on the findings from the risk assessment conducted, decided on the requirements for its customers (natural persons and legal entities) please see the generic PDD requirements table.

6.3.5 Verification methods vary and are mostly dictated by the type of information used to establish a person's identity in a given scenario. Regardless of the method applied, it is important that verification be done using information obtained from a reliable and independent third-party source and as far as possible, the original source of the information.

6.3.6 This table illustrates Constantia Key Information required for PDD purposes for each client (both natural and juristic persons):

Natural Person	Juristic Person
First Name	Registered Name
Last Name	Country of Registration
Date of Birth	Nature of Business
Country of Birth	Details of the Juristic Person's Directors
Country of Residence	
ID Number	
Nationality	

6.4 Constantia levels of due diligence

6.4.1 Simplified due diligence

6.4.1.1 Understand the static risk assessment.

6.4.1.2 Process the client information.

6.4.1.3 Screen the client against the Sanctions and PEP/PIP lists.

6.4.1.4 Any confirmed match on a Sanctions list follows the escalation process for intolerable risk.

6.4.1.5 Parties on the PEP/PIP lists as well as their family members and close associates must be subjected to enhanced due diligence.

6.4.1.6 Proceed with the simplified customer due diligence process in terms of record keeping and reporting.

6.4.1.7 If, while following the simplified due diligence process, there are indications of suspicious activity or Transactions, the enhanced due diligence process must be followed.

6.4.2 Enhanced due diligence

6.4.2.1 Constantia's systems and controls should provide for more information to be obtained about their clients, more secure confirmation of clients' information to be applied and closer scrutiny to be conducted to their clients' transaction activities where they assess the risk of abuse to be higher, and in particular:

(a) increased intensity of measures aimed at identifying the nature of the client`s business and the source of his income, funds & wealth;
(b) increased monitoring of the client's transactions;
(c) increased review periods of customer information that has already been obtained;
(d) using more or higher quality sources to confirm the information provided by clients;
(e) senior management involvement in the onboarding of clients.

6.4.3 From the abovementioned, what is required to be answered is the manner in which EDD will be conducted and by whom (the specification is completed per category of client, i.e., natural persons, legal persons, trusts and partnerships).

6.5 PDD on the client and premium payer if the premium payer is different from the client

6.5.1 Constantia may not establish a business relationship unless it has taken the prescribed steps to establish and identify the identity of the client or the person representing the client.

6.5.2 Constantia must ensure that it identifies and verifies both the client and the premium payer in accordance with the provisions of FICA because the transaction poses a greater risk for money laundering activities.

6.5.3 Constantia must obtain from the person acting on behalf of another person information that provides proof of that person's authority to act on behalf of that other natural person, legal person or trust.

6.5.4 The following are examples of documents that may be accepted to confirm the authority of a person to act on behalf of another person and to confirm the particulars of the person authorising the third party to establish the relationship:

6.5.4.1 power of attorney;
6.5.4.2 written mandate;
6.5.4.3 resolution duly executed by authorised signatories; or
6.5.4.4 a court order authorising the third party to conduct business on behalf of another person;
6.5.4.5 any other document deemed relevant and acceptable by the Legal Advisor and/or Compliance Officer.

6.5.5 Constantia is required to establish and verify the identity of each natural person who purports to be authorised to establish a business relationship or to enter into a transaction with the AI on behalf of a legal person.

6.5.6 This authorisation is because a natural person may be authorised or mandated to transact on behalf of the legal entity and bind the legal entity in a contractual relationship.

6.5.7 Constantia must then verify the identities of each of those particular persons as well as their authority to establish a business relationship or conduct transactions with Constantia.

6.6 Prohibited Client Relationships

6.6.1 Constantia is prohibited from keeping anonymous accounts or accounts in fictitious names.

6.6.2 Enter into or maintain a business relationship with a minor or a legally incapacitated person without also performing the required PDD on a person with legal standing who represents the minor or a legally incapacitated person. For example, a parent or legal guardian.

6.6.3 Enter into or maintain business relationships or conclude single transactions if it cannot perform the required PDD as prescribed.

6.6.4 Enter into or maintain business relationships with persons or entities who appears on any sanctions lists.

6.6.5 Transacting with a client with whom a business relationship has been entered into or concluding a single transaction where the PDD of the client has not been completed.

6.7 PDD Verification Processes

6.7.1 Verification of the client's identity entails that the AI corroborates the person's identity information by comparing this information with information contained in documents or electronic data issued or created by reliable and independent third-party sources. * [(Dow Jones/Companies and Intellectual Property Commission (CIPC)].

6.7.2 Verification methods are dictated by the type of information used to establish a person's identity in a given scenario. Verification must be done using information obtained from a reliable and independent third-party source and the original source of the information. AI should evaluate the adequacy of corroboration of a person's identity characteristics. This implies that institutions must determine the level of confidence they have that any particular method of corroboration provides certainty as to the relevant identity characteristics. Information sources created or generated by the client him/herself are not considered to be reliable and independent third-party sources.

6.7.3 Government issued or Government controlled sources of information such as various forms of identity documents (e.g. South African identity documents including smart card identity documents, driver's licenses, foreign identity documents, passports, asylum seeker or refugee permits, work permits, visitors' visas) and the underlying electronic databases where information evidenced in identity documents are kept, provide a high level of confidence as a means to corroborate a natural person's basic identity characteristics. AIs in Constantia shall therefore use government issued or Government controlled sources as the means of verification when verifying basic identity characteristics.

6.7.4 Verification of a person's identity in relation to both basic and other identity characteristics should be done in documentary and electronic form. In addition to documentary verification AI shall make use of information in electronic form to verify a prospective client's information against multiple third-party data sources. The same test as in the case of documentary sources, i.e., that the sources must be reliable and independent third-party sources and as far as possible, the original source of the relevant information, applies in respect of electronic verification. Electronic solutions that allow prospective customers to manipulate source information in any manner shall not be considered credible information sources to enable verification of customer particulars.

6.7.5 Electronic verification of a client's identity by any AI in Constantia shall, at the very minimum, include a cross referencing/ screening of the client's identity against the financial sanction list of persons and entities from time to time identified upon resolution by the Security Council of the United Nations. Where such cross referencing/ screening renders a result indicating that the client's name is listed in the financial sanction list of the Security Council of the United Nations, the institution shall be prohibited from entering into a business relationship or concluding a transaction, directly or indirectly, with such client.

6.8 Timing of PDD

6.8.1 A party's identity and, where applicable, the identities of beneficial owners and other persons associated with a party, must be established and verified in the course of conducting a single transaction or entering into a business relationship. *Constantia must complete the verification before a transaction concluded in the course of the resultant business relationship or performs any act to give effect to the resultant single transaction.*

6.8.2 AIs within Constantia may, for example, accept a mandate from a prospective client to establish a business relationship or to conclude a single transaction or take any similar preparatory steps with a view of establishing a business relationship or concluding a single transaction before completing verification of the identities of the prospective client and other relevant persons. However, in doing so, those AIs shall take care not to incur unmitigated ML/TF risks by, for example, receiving funds from a client which may have to be returned to the client before completing the verification or making funds available to a client before completing the verification.

6.9 Who conducts Enhanced Due Diligence (EDD) investigation for Constantia (escalation process)?

6.9.1 The initial investigation shall be conducted by the AML Analyst.

6.9.2 Depending on expertise required, any employee or contractor may be delegated or appointed to assist with the investigation.

6.9.3 All postponed cases are escalated to the relevant segment head to acquire more information.

6.9.4 All positive/true matches on PEP/PIP list are escalated to Head of Department (HOD) of the relevant segment channel.

6.9.5 All positive/true matches on the Sanction list are escalated to the Compliance Officer.

6.10 When are EDD investigations applied and what do they entail?

6.10.1 Enhanced investigative and control measures are applied linked to an increased ML/TF risk that has been identified.

6.10.1 The following are examples of when EDD is required but is not limited to these:

6.10.1.1 When the client is regarded as a **Politically Influential Person (PIP)**.

6.10.1.2 When a client is **Prominent Public Official (PPO)**.

6.11 Customers identified as Prominent Influential Persons (PIPS)

6.11.1 PIPS are persons who hold prominent positions of influence in the public and/or private sectors. Such individuals are identified by verifying their identity against a list of PIPS that are published and regularly updated.

6.11.1 When it is identified that Constantia is about to enter into a business relationship or enter into a single transaction with (or has an existing relationship) a natural person who is listed as a PIP, an enhanced due diligence process must be conducted that would include the following:

6.11.1.1 the ML/TF risk that Constantia would be exposed to would need to be assessed;

6.11.1.2 in the process of assessing such business relationship, reasonable measures should be taken to establish the source of the wealth and the source of funds that will form part of the business relationship with such client. It is not necessary to verify the information relating to the source of wealth and source of funds, but will have to be considered when conducting on-going monitoring in relation to the business relationship;

6.11.1.3 in the process of investigating the source of funds, Constantia needs to consider the origins of such funds and the ability to transfer such funds as part of the business relationship;

6.11.1.4 before any business relationship is entered into (or a single transaction concluded), HOD of the relevant Distribution Channel needs to approve such business transaction based on the ML/TF risk that such a business relationship with such a PIP would hold for Constantia;

6.11.1.5 similar EDD investigative steps are required to be taken in relation to persons who are identified as immediate family members or known associates of PIPS.

6.12 Customers identified as foreign prominent public officials (PPOs)

6.12.1 PPOs are persons who hold or have held at any time during the preceding 12 months public prominent positions of influence in the public sector.

6.12.2 When it is identified that Constantia is about to enter into a business relationship or enter into a single transaction or has an existing relationship with a natural person who is identified as a PPO, such a relationship must always be regarded as exposing Constantia to a high level of ML/TF risk. An enhanced due diligence process needs to be conducted that would include the following:

6.12.2.1 an investigation needs to be conducted into understanding what the intended or existing business relationship would entail;

6.12.2.2 the ML/TF risk that Constantia would be exposed to would need to be assessed;

6.12.2.3 in the process of assessing such business relationship, reasonable measures should be taken to establish the source of the wealth and the source of funds that will form part of the business relationship with such client. It is not necessary to verify the information relating to the source of wealth and source of funds, but will have to be considered when conducting on-going monitoring in relation to the business relationship;

6.12.2.4 in the process of investigating the source of funds, Constantia needs to consider the origins of such funds and the ability to transfer such funds as part of the business relationship;

6.12.2.5 before any business relationship is entered into (or a single transaction concluded), Senior Management needs to approve such business transaction based on the ML/TF risk that such a business relationship with such a PIP would hold for Constantia;

6.12.2.6 similar enhanced due diligence investigative steps are required to be taken in relation to persons who are identified as immediate family members or known associates of PPOs. Immediate family members of foreign prominent public officials include the following:

(a) spouse, civil partner or life partner;
(b) a previous spouse, civil partner or life partner if applicable;
(c) children and stepchildren of their spouse, civil partner or life partner;
(d) siblings and stepsiblings and their spouse, civil partner or life partner.

6.12.3 Reliance on third parties

6.12.3.1 In the process of conducting PDD, Constantia sales personnel and intermediaries are regarded as the "eyes and ears" of Constantia in assisting to identify possible ML/TF risks that Constantia may be exposed to when entering into (or maintaining) a business relationship or concluding a single transaction with a client;

6.12.3.2 It is required of Constantia personnel and intermediaries to alert management of the potential ML/TF risks that are identified;

6.12.3.3 When there is a need identified to conduct an EDD investigation, it is expected of Constantia employees and intermediaries to source (or facilitate the sourcing of) relevant and sufficient information from clients to enable Constantia to make an informed decision of the ML/TF risk that such a client relationship would expose Constantia to.

6.12.4 On-going Due Diligence

6.12.4.1 On-going due diligence refers to the on-going monitoring and scrutiny of transactions undertaken throughout the course of the business relationship to ensure that same is consistent with the Constantia knowledge and information on the customer.

6.12.4.2 This will include monitoring of transactions undertaken throughout the course of the relationship, including, where necessary:

(a) the source of funds, to ensure that the transactions are consistent with the AI's knowledge of the client and the client's business and risk profile;

(b) the background and purpose of all complex, unusually large transactions, and all unusual patterns of transactions, which have no apparent business or lawful purpose; and

(c) keeping information obtained for the purpose of establishing and verifying the identities of clients up to date.

6.12.5 Doubts about veracity of previously obtained information

6.12.5.1 Where Constantia doubts the veracity or adequacy of the previously obtained information, it must re-establish and re-verify the identity of the client.

6.12.5.2 If a client is a legal person, Constantia must re-establish the identity of the beneficial owner of the client.

6.13 Inability to conduct due diligence

6.13.1 If Constantia is unable to conduct on-going due diligence, it may not:

6.13.1.1 establish a business relationship or conclude a single transaction with a client.

6.13.1.2 conclude a transaction in the course of a business relationship, or perform any act to give effect to a single transaction; or

6.13.1.3 must terminate an existing relationship with a client, as the case may be.

7. TERMINATION OF BUSINESS RELATIONSHIPS

7.1 The FICA and FATF Recommendation 5 include specific references to the termination of business relationships because a financial institution is unable to comply with obtaining relevant information in order to mitigate any risks related to local or international standards on, inter alia, money laundering or terrorist financing.

7.2 This means that the AI should not open the account, commence a business relationship or perform the transaction. If a business relationship is already in existence, the business relationship should be terminated, and the AI should consider making a suspicious transactions report in relation to the customer.

7.3 Termination process:

7.3.1 The proposed transaction should be escalated to senior management;

7.3.2 The client or prospective client should be informed (subject to tipping-off considerations);

7.3.3 There should be notification to the Head of Compliance;

7.3.4 There should be escalation to the Executive Compliance Officer; and

7.3.5 A report should be made to the FIC, where appropriate.

8. REPORTABLE TRANSACTIONS

8.1 Cash Transactions above the Prescribed Limit – Section 28

8.1.1 These are cash transactions made by or to an AI in excess of the prescribed limits set by the authorities. This limit is **R49 999.99 (and as may be amended from time to time by the Act)**. These transactions must be reported to the Money Laundering Compliance Officer/ Money Laundering Risk Officer (MLCO / MLRO).

8.1.2 Below find Constantia guidelines regarding cash transactions:

8.1.2.1 **Can the R49 999.99 be a single transaction or multiple transactions adding up to R49 999.99?** You must report aggregates of smaller amounts which, when combined, add up to the prescribed amount in cases where it appears to you that the transactions involving those small amounts are linked in such a way that they should be considered as fractions of one transaction. Therefore, the threshold amount can be a single cash transaction to the value of R49 999.99 or more, or an aggregation of smaller amounts with a combined value of R R49 999.99 or more. While the aggregation period is not specified, the FIC requests that a period of at least 24 hours be applied when considering aggregation.

8.1.2.2 **What is the time period for reporting a transaction that has exceeded the prescribed threshold?** A report must be sent to the FIC by the MLCO/ MLRO *as soon as possible but no later than 2 days* after Constantia has become aware of a cash transaction or series of cash transactions that has exceeded the prescribed threshold. However, reports to the MLCO/ MLRO by employees must be made immediately after becoming aware of them, but not later than 1 day.

8.2 Property associated with terrorist and related activities - Section 28A

8.2.1 AI is required to report to the FIC in respect of any property that it has in its possession or over which it has control, and which is owned by an entity that has committed or has facilitated the committing of a terrorist or related activity; where "property" means money, movable and immovable property, rights, privileges, claims and securities and interests therein and proceeds thereof.

8.2.2 A report must be sent to the FIC by Constantia *as soon as possible but no later than 5 days* after the AI had established that it has property associated with terrorist and related activities in its possession or under its control.

8.2.3 However, reports to the MLCO/ MLRO by employees must be made immediately after becoming aware of them, but not later than 2 days.

8.3 Suspicious and Unusual transactions - Section 29

8.3.1 **There are four main types of suspicious and unusual transactions:**

8.3.1.1 those that assist with or may assist with, the transfer of the proceeds of unlawful activities;

8.3.1.2 those that have no apparent business or lawful purpose (i.e., they make no business sense);

8.3.1.3 those that are conducted for the purpose of avoiding giving rise to a reporting duty in terms of the provisions of the Act; or

8.3.1.4 those that may be relevant to the investigation of an evasion of any tax, duty or levy.

8.4 Reporting procedure when a suspicious transaction has been identified:

8.4.1 Continue with the transaction and do not "TIP" the client off;

8.4.2 Report the transaction to the Compliance Officer or the MLRO or complete and submit the "FICA suspicious reporting notification form" within 5 days of the transaction occurring;

8.4.3 The Compliance Officer and/or MLRO will contact a senior manager or official of the originating area for details;

8.4.4 The Compliance Officer and MLRO, will assess the transaction and determine whether the transaction warrants reporting to the FIC or not;

8.4.5 If so, the Compliance Officer or MLRO will report the transaction to the FIC within 15 days of receiving details of the case and ensure that the decision is recorded.

8.4.6 However, reports to the MLCO/ MLRO by employees must be made immediately after becoming aware of them, but not later than 5 days.

8.5 Conveyance of cash above the prescribed limit to/ from the Republic - Section 30

8.5.1 Any person intending to convey an amount of cash in excess of the prescribed amount to or from the Republic must be reported to Compliance Officer / MLRO before the transaction occurs.

8.5.2 **Reporting process**

8.5.2.1 FICA requires that all suspicious transactions and cash transactions above the prescribed limit of R49 999.99 must be reported.

8.5.2.2 In view of the protective measures put in place by Constantia's employees may possibly not be at risk of being exposed to cash transactions above the prescribed limit, property associated with terrorist and related activities and suspicious and unusual transactions.

8.5.2.3 However, any employee of an AI may commit a money-laundering offence by intentionally or negligently assisting a criminal to launder the proceeds of a crime. This can be done by deliberately ignoring any suspicious transaction or behavior of a client (called "willful blindness"), by being negligent and not checking whether the transaction could be suspicious (called "negligent ignorance") or by letting a suspect know that a suspicious report will be filed on the transaction (called "tipping-off").

8.5.2.4 FICA also prescribes that an AI must appoint a compliance officer who is responsible to ensure compliance by employees of the institution with provisions of FICA as well as compliance by the institution itself with its obligations under FICA.

8.5.2.5 If any employee reasonably suspects any unlawful suspicious activity as discussed above, the employee must continue with the transaction and complete it but report it as follows: Emailing their suspicion of the transaction to the Centre MLRO mailbox: AMLCompliance@constantiagroup.co.za or to the Compliance Officer.

8.5.2.6 If any employee becomes aware of a cash transaction in excess of R49 999.99, they must report this immediately to the MLRO/ MLCO.

8.5.2.7 The MLCO/ MLRO will contact a senior manager or official of the originating area for full details after which a decision will be made whether to report the matter or not. The employee initiating the report must not investigate the matter further and the matter should not be discussed with colleagues or managers.

9. FAILURE TO REPORT

9.1 Where a person/institution becomes aware of a reporting failure to the FIC, such person/institution must mitigate the loss of intelligence data to the FIC in the following manner:

9.1.1 Inform the FIC in writing of the reporting failure immediately after becoming aware of such failure. The notification must be sent to the Executive Manager, Compliance, FIC; and

9.1.2 Request an engagement with the FIC to discuss relevant mitigation factors.

9.1.3 The subsequent arrangements for the mitigation of lost intelligence data due to the FIC does not imply condonation of the failure to report information to the FIC, nor does it absolve the reporter from its continuing reporting obligations under FICA or prevent enforcement action being taken by the relevant supervisory body.

10. COMMUNICATION, TRAINING AND MONITORING

10.1 RMCP Communication Plan

10.1.1 RMCP Communication Plan has been approved at Constantia group level for all AIs within the group.

10.1.2 The approved RMCP shall be kept on the Intranet to allow easy access to all employees.

10.1.3 Compliance will ensure that there is awareness on the existence and importance of RMCP.

10.1.4 Such awareness may be through various platforms. For example, Intranet.

10.2 Training and Awareness

10.2.1 Constantia's PDD Training applies to all Constantia Business Segments. The document will set out the Training Strategy's Guiding Principles.

10.3 All new staff must attend FICA training

10.3.1 It remains the primary responsibility of the manager of the respective division or department to ensure that training is arranged for new staff within **35 working days** of joining the company.

10.3.2 Training can be offered through face-to-face interaction and via online platforms (i.e., MS Teams).

10.3.3 Compliance will keep copies of the workbook and test for completion.

10.3.4 People and Strategy will send a copy of the report listing all new staff to Learning and Development Department every month for training monitoring purposes.

10.3.5 Business/Management will monitor completion and may require confirmation of course attendance.

10.3.6 A Course Attendance Register must be included for each training session, with the delegates' details and signature on it, as well as details of the training session and accreditation test.

11. COMPLIANCE RISK MONITORING

11.1 Routine monitoring by the compliance function as per the Compliance Monitoring Plan

11.1.1 Routine monitoring should be conducted by the compliance function, as part of the Compliance Monitoring Plan, to assess, *inter alia*, whether the processes and controls relating to the implementation of a risk-based approach is adequate and effective.

11.2 Compliance Risk Reporting

11.2.1 Timeous and efficient notification and escalation of any compliance incidents or risk associated with ML/TF is imperative for the effective implementation of the RMCP.

11.2.2 Compliance incidents and risks relating to ML/TF should be notified to the EXCO as and when they are identified and not only at predetermined intervals.

12. ESCALATION PROCEDURE

12.1 Transactions classified as high-risk should be escalated to Senior Management; the compliance function and the EXCO.

12.2 The EXCO will provide a recommendation on whether to proceed with the transaction. If there is any difference in opinion/approach between Senior Management and the EXCO, the decision on whether to proceed with the transaction will be escalated to the CEO for resolution.

13. RECORD KEEPING

13.1 The following components of record-keeping are set out below:

13.1.1 **Due Diligence Records:**

13.1.1.1 Constantia must ensure that due diligence records of the client or prospective client are kept. Such records must include copies of, or references to, information provided to or obtained to verify the person's identity, viz:

(a) documents used to establish and verify identity of the client;

(b) if the client is acting on behalf of another person, record of documents used to identify that other person and client's authority to establish the business relationship or conclude a single transaction on behalf of that other person;

(c) documents/information used to understand the nature of the business relationship; intended purpose of the business relationship; source of funds the prospective client is expected to use in concluding transactions during the business relationship;

(d) documents/information for additional due diligence measures relating to legal persons, trusts and partnerships;

(e) documents/information relating to on-going due diligence in respect of a business relationship and keeping information obtained for the purpose of establishing and verifying identities of clients up to date;

(f) documents/information obtained when there are doubts about the veracity of previously obtained information;

(g) documents/information when there is an inability to conduct customer due diligence;

(h) documents/information relating to foreign public officials; domestic influential persons and family members and close associates of the aforementioned persons.

13.1.2 **Transaction records:**

13.1.2.1 Constantia must ensure that transaction records are kept of single transactions and transactions concluded in the course of the business relationship.

13.1.2.2 Records must reflect the information as contained in Section 22A of the AI, viz. that transaction records must be sufficient to enable the transaction to be reconstructed and include the:

(a) amount;

(b) currency;

(c) date of transaction;

(d) parties to the transaction;

(e) nature of the transaction;

(f) business correspondence; and

(g) identifying particulars of all account files related to the transaction if account facilities are provided.

13.1.3 **Period for which records must be kept:**

13.1.3.1 Records in relation to establishment of a business relationship referred to in the section related to due diligence records must be kept for at least 5 years from the date on which the business relationship is terminated;

13.1.3.2 Records of all transactions relating to transaction records must be kept for at least 5 years from the date on which that transaction is concluded; and

13.1.3.3 Records of a transaction or activity which gave rise to a report contemplated in terms of a suspicious and unusual transaction must be kept for at least 5 years from the date on which the report was submitted to the FIC.

13.1.3.4 Records relating to pending investigations by either the FIC or any Supervisory Body must be kept for a period longer than 5 years for as long as such investigation continues.

13.1.4 **Manner in which records must be kept:**

13.1.4.1 Constantia must ensure that records are kept in the following manner:

(a) in electronic format or hard copies by Third parties (i.e., Metro File);

(b) must have free and easy (i.e., unencumbered) access to the relevant records;

(c) the records must be readily available to the FIC and the relevant supervisory body, when required;

(d) the records must be capable of being reproduced in a legible format;

(e) if the records are stored off-site, the FIC and the relevant supervisory body must be provided with the details of the third party storing the records;

(f) it must be ensured that records are tamper proof and that there are safeguards in place to prevent the unauthorised access to information stored electronically;

(g) Constantia makes use of commercial third parties' services therefore regular assessments of service providers need to be conducted to provide assurance to the relevant supervisory body that the AI can access and retrieve data and/or documents envisaged in the FICA.

14. IMPLEMENTATION

14.1 This RMCP encapsulates Constantia policy and procedures aimed at complying with its obligations under the FICA, as amended on a risk sensitive basis.

14.2 Constantia's approach and commitment to ML/ TF risk management and AML/ CTF compliance is documented in this RMCP.

14.3 This RMCP will therefore apply to all life insurance businesses within Constantia.

15. REVISION HISTORY

Version	Date	Author	Organisation	Revision
1.0	September 2019	Compliance	CRIH	Policy created
2.0	September 2021	Compliance	CRIH	Policy reviewed and updated
3.0	September 2023	PG Todd	CRIH	Policy reviewed and updated

CRIH FICA and AML Policy-Sept 2023

Final Audit Report 2024-04-09

Created:	2024-04-02
By:	Rene Kok (renek@conduitcapital.co.za)
Status:	Signed
Transaction ID:	CBJCHBCAABAAclG-PJagEsQftTG_1RUlfkbXxCgapGFq

"CRIH FICA and AML Policy-Sept 2023" History

Document created by Rene Kok (renek@conduitcapital.co.za)
2024-04-02 - 12:22:15 PM GMT- IP address: 102.220.209.226

Document emailed to Themba Baloyi (thembab@gmail.com) for signature
2024-04-02 - 12:22:20 PM GMT

Document emailed to Lusani Mulaudzi (lusani.mulaudzi@gmail.com) for signature
2024-04-02 - 12:22:20 PM GMT

Email viewed by Lusani Mulaudzi (lusani.mulaudzi@gmail.com)
2024-04-02 - 7:03:57 PM GMT- IP address: 66.249.93.101

Email viewed by Themba Baloyi (thembab@gmail.com)
2024-04-08 - 2:36:04 PM GMT- IP address: 104.28.82.93

Document e-signed by Themba Baloyi (thembab@gmail.com)
Signature Date: 2024-04-09 - 7:11:57 AM GMT - Time Source: server- IP address: 196.192.169.198

Document e-signed by Lusani Mulaudzi (lusani.mulaudzi@gmail.com)
Signature Date: 2024-04-09 - 11:25:40 AM GMT - Time Source: server- IP address: 197.215.164.186

Agreement completed.
2024-04-09 - 11:25:40 AM GMT