VAULT MARKETS

FICA Risk Management & Compliance Programme

Version 1.0

Vault Markets (Pty) Ltd is a Juristic Representative of RocketX (Pty) Ltd, a company duly incorporated under the laws of South Africa, with company number 2020/824856/07, an authorised Financial Services Provider and Over-the-Counter Derivatives Provider , licensed and regulated by the Financial Sector Conduct Authority (FSCA) in South Africa, with FSP No: 52142.

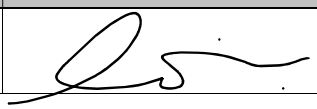
Document information

Document title	Vault Markets – FICA Risk Management & Compliance Program
Author(s)	Vault Markets Compliance
File name	Vault Markets – FICA RMCP
Version	Version 1.0
Approved by, on	Compliance and Legal – 17 January 2024

Document Review

Implemented	January 2024
Review	30 January 2024
Next Review	30 January 2024

Document approval

Approved		**date**
Nicky Eilers Compliance		17 January 2024

Contents

1 Risk Management & Compliance Program Statement

This programme forms part of the organisation's internal business policies, processes and procedures and must be read in context with all other policies and procedures.

The organisation's governing body and employees are required to familiarise themselves with the FICA RMCP and undertake to comply with the stated processes and procedures.

Risk owners and control owners are responsible for overseeing and maintaining control procedures and activities.

Purpose

The purpose of this FICA Risk Management and Compliance Programme is to:

- Enable the organisation to identify, assess, mitigate, manage and monitor the risk that the provision by the organisation of its products or services may involve or facilitate money laundering activities or the financing of terrorist and related activities.
- Provide for the manner in which the organisation determines if a person is:
  - A prospective client in the process of establishing a business relationship or entering into a single transaction with the organisation, or
  - A client who has established a business relationship or entered into a single transaction, is a client of the organisation.
- Provide for the manner in which the organisation complies with the compliance obligations of not establishing a business relationship or concluding a single transaction with an anonymous client or a client with an apparent false or fictitious name.
- Provide for the manner in which, and the processes by which, the organisation:
  - Establishes and verifies the identity of a client, and

- Establishes a client representative's authority to establish a business relationship or to conclude a single transaction on behalf of a client.

- Provide for the manner in which, and the processes by which, the organisation determines whether future transactions that will be performed in the course of the business relationship, are consistent with the organisation's knowledge of a prospective client.
- Provide for the manner in which, and the processes by which, ongoing due diligence and account monitoring in respect of business relationships are conducted by the organisation.
- Provide for the manner in which the examining of:
  - Complex or unusually large transactions, and
  - Unusual patterns of transactions which have no apparent business or lawful purpose takes place.
- Provide for the manner in which, and the processes by which, the organisation will confirm information relating to a client when the organisation has doubts about the veracity of previously obtained information.
- Provide for the manner in which, and the processes by which the organisation will perform the client due diligence requirements in accordance with the following compliance obligations:
  - The identification of clients and other relevant persons,
  - Understanding and obtaining information on business relationships,
  - Additional due diligence measures relating to legal persons, trusts and partnerships,
  - Ongoing due diligence when, during the course of a business relationship, the organisation suspects or knows that a transaction or activity is suspicious or unusual.

- Provide for the manner in which the organisation will terminate an existing business relationship where the organisation is unable to:
  - Establish and verify the identity of a client or other relevant person,
  - Obtain information describing the nature of the business relationship, the intended purpose of the business relationship concerned and the source of funds which a prospective client expects to use in concluding transactions in the course of the business relationship concerned,
  - Conduct ongoing due diligence.
- Provide for the manner in which, and the processes by which, the organisation will determine whether a prospective client is a foreign prominent public official or a domestic prominent influential person.
- Provide for the manner in which, and the processes by which, enhanced due diligence is conducted for higher-risk business relationships and when simplified client due diligence might be permitted in the organisation.
- Provide for the manner, place in which and the period for which client due diligence and transaction records are kept.
- Enable the organisation to determine when a transaction or activity is reportable to the FIC.
- Provide for the processes for reporting information to the FIC.
- Provide for the manner in which:
  - The FICA RMCP is implemented in branches, subsidiaries or other operations of the organisation in foreign countries so as to enable the organisation to comply with its compliance obligations under FICA
  - The organisation will determine if the host country of a foreign branch or subsidiary permits the implementation of measures required under FICA
  - The organisation will inform the FIC and supervisory body concerned, if the host country does not permit the implementation of measures required under FICA

- Provide for the processes for the organisation to implement its FICA RMCP.
- Indicate if any of the processes are not applicable to the organisation, and if so, the reasons why it is not applicable.

2 Control Owners

Establish a Regulatory Risk & Compliance Management Framework for the organisation.

Implement control measures (actions, activities, processes and/or procedures) that will provide reasonable assurance that the organisation's compliance obligations are met and that non-compliances are prevented, detected and corrected.

Control measures must be periodically evaluated and tested to ensure their continuing effectiveness.

Action / Activity / Process / Procedure	Control Owner
Annual review of the FICA RMCP	Legal and Compliance
Appointment of the AML / Compliance Officer	Compliance
Appointment of the Deputy AML / Compliance Officer	Compliance
Confirmation of FIC Registration	Compliance
Monitoring changes to organisation's registration particulars	FICA HOD
Periodic Product and Service ML/TF Risk Analysis	FICA HOD
Review of the Client ML/TF Risk Identification Criteria	Compliance
Periodic updating of UN Security Council Sanction List	FICA HOD
Submittal and Record Keeping of Cash Threshold Reports	FIC Officer
Submittal and Record Keeping of Suspicious or Unusual Transaction Reports	FIC Officer
Submittal and Record Keeping of Terrorist Property Reports	FIC Officer
Retention and Back-ups of FICA Transaction Records	IT
Retention and Back-ups of FICA Client Due Diligence Records	IT
Ensuring that employees undergo annual FICA Awareness Training	Compliance

Periodic review of Client Due Diligence Activity Sheet	Compliance
Periodic review of Client Due Diligence Forms	Compliance
Ongoing Due Diligence and Monitoring of Existing Business Relationships	FICA HOD
Client random spot checks: UN Security Council List	FICA HOD
Client random spot checks: False or Fictitious verification documents	FICA HOD
Client random spot checks: DPIP or FPPO	FICA HOD
Monitoring Compliance with Client Due Diligence procedure	Compliance
Monitoring Compliance with Additional Information on a New Business Relationship	Legal and Compliance
Annual review of the Compliance Monitoring Schedule	Compliance

3 RMCP Application

This FICA RMCP applies to:

- The organisation's governing body,
- Where applicable, all branches, business units and divisions of the organisation,
- All employees

The organisation's governing body requires all employees to fully comply with the processes and procedures outlined herein.

Any gross negligence or wilful noncompliance with the provisions of FICA and/or the processes and procedures outlined within the organisation's FICA RMCP, will be considered a serious form of misconduct which may result in a summary dismissal.

4 FICA Compliance Objectives

The organisation's FICA Compliance Objectives are:

- To protect the integrity of the organisation through the continued management of money laundering and terrorist financing risk.
- To apply a risk-based approach to client transactions and to understand the purpose of all business relationships entered into with clients.
- To educate employees how to identify business relationships and transactions that pose a higher risk to money laundering and terrorist financing.
- To implement robust Client Due Diligence procedures that will make it more difficult for criminals to hide the proceeds of unlawful activities.
- To submit to the FIC relevant reports concerning all transactions that are identified as being suspicious, unusual or above the prescribed cash threshold.
- To keep accurate records of all FICA related transactions and Client Due Diligence procedures.
- To prevent any reputational fallout or brand damage due to noncompliance with FICA and/or the organisation's AML & CTF RMCP.
- To prevent any civil or criminal fines or penalties due to noncompliance with FICA and/or the organisation's AML & CTF RMCP.
- To prevent loss of sales and client confidence due to noncompliance with FICA and/or the organisation's AML & CTF RMCP.

5 FICA Compliance Obligations

The organisation has identified the following twenty-one (21) FICA related compliance obligations:

Nr.	Domain	Compliance Obligation	Reference	Regulatory Designation
5.1.1	FICA GRC Standards	The Organisation must Develop, Document, Maintain and Implement a RMCP	FICA Sec 42	Accountable Institutions
5.1.2	FICA GRC Standards	The Organisation must Govern Compliance with its RMCP	FICA Sec 42A	Accountable Institutions
5.2.1	FICA Licensing and Maintenance	The Organisation must Register itself with the FIC	FICA Sec 43B(1)	Accountable & Reporting Institutions
5.2.2	FICA Licensing and Maintenance	The Organisation must inform the FIC of any changes to its Registration Particulars	FICA Sec 43B(4)	Accountable & Reporting Institutions
5.3.1	FICA CDD Procedure	The Organisation must perform Enhanced Client Due Diligence Procedures where a High-Risk Client is Identified	FICA Sec 42(2)	Accountable Institutions
5.3.2	FICA CDD Procedure	The Organisation must Understand and Obtain Information where a new Business Relationship is established to reasonably enable it to determine whether future transactions are consistent with the knowledge held of that prospective client (INCLUDES SOURCE OF FUNDS)	FICA Sec 21A	Accountable Institutions
5.3.3	FICA CDD Procedure	The Organisation must Establish and Verify the Identity of all prospective Clients	FICA Sec 21	Accountable Institutions
5.3.4	FICA CDD Procedure	The Organisation must Avoid Clients with apparent False or Fictitious Names and may not establish a business relationship or a single transaction with an anonymous client	FICA Sec 20A	Accountable Institutions
5.3.5	FICA CDD Procedure	The Organisation must Avoid and Terminate any Business Relationships or Single Transactions where it is unable to conduct a Client Due Diligence	FICA Sec 21E	Accountable Institutions

5.3.6	FICA CDD Procedure	The Organisation must Avoid Transactions and Business Relationships with Persons and Entities identified by the United Nations Security Council	FICA Sec 26B, 26C	Universal
5.3.7	FICA CDD Procedure	The Organisation must perform Additional Client Due Diligence Procedures where a client is a Domestic Prominent Influential Person	FICA Sec 21G	Accountable Institutions
5.3.8	FICA CDD Procedure	The Organisation must perform Additional Client Due Diligence Procedures where a client is a Foreign Prominent Public Official	FICA Sec 21F	Accountable Institutions
5.3.9	FICA CDD Procedure	The Organisation must perform Additional Client Due Diligence Procedures where a client is a Family Member or a Close Associate of a DPIP or a FPPO	FICA Sec 21H	Accountable Institutions
5.3.10	FICA CDD Procedure	The Organisation must when in Doubt, confirm the Veracity of previously obtained Client Information	FICA Sec 21D	Accountable Institutions
5.3.11	FICA CDD Procedure	The Organisation must perform Ongoing Client Due Diligence Procedures and the Monitoring of Transactions of existing Business Relationships	FICA Sec 21C	Accountable Institutions
5.4.1	FICA Reporting Duty	The Organisation must submit Suspicious or Unusual Transaction Reports within the prescribed time limit	FICA Sec 29	Universal
5.4.2	FICA Reporting Duty	The Organisation must submit Terrorist Property Reports within the prescribed time limit	FICA Sec 28A	Accountable Institutions
5.5.1	FICA Recordkeeping	The Organisation must keep and maintain Transaction Records for the required period	FICA Sec 22A & 23	Accountable Institutions
5.5.2	FICA Recordkeeping	The Organisation must keep and maintain Client Due Diligence Records for the required period	FICA Sec 22 & 23	Accountable Institutions
5.5.3	FICA Recordkeeping	The Organisation must ensure Compliance where Transaction Records or Client Due Diligence Records are kept and maintained by a Third Party	FICA Sec 24	Accountable Institutions

5.6	FICA Awareness Training	The Organisation must provide Training to ensure compliance with FICA and the Organisation's AML & CTF RMCP	FICA Sec 43	Accountable Institutions

5.1 FICA STANDARDS

5.1.1 Maintain FICA RMCP

For the purposes of risk management and crime prevention, the organisation has developed and implemented this FICA RMCP to detect and prevent instances of money laundering and terrorist financing from occurring or being associated with the organisation in any way.

The FICA RMCP has been approved by the organisation's governing body and will be reviewed on an annual basis to ensure that the FICA RMCP remains relevant to the organisation's operations and the achievement of the organisation's FICA compliance objectives.

The AML / Compliance Officer will conduct the annual review as indicated in the organisation's Compliance Monitoring Schedule under Annexure A.

5.1.2 Govern Compliance with the FICA RMCP

The organisation's governing body recognises its responsibility of ensuring that all employees comply with the provisions of FICA and the processes outlined in the RMCP.

The organisation has therefore established an AML Compliance function as part of its risk management framework. The compliance function will at all times be exercised with such due diligence, care and degree of competency as may reasonably be expected from the AML Compliance Officer.

In performing his or her duties, the AML Compliance Officer will provide written reports on the course of, and the progress achieved with, compliance monitoring duties and make recommendations to the organisation's governing body with regards to any AML & CTF compliance requirements.

The organisation's AML Compliance Officer is responsible for ensuring compliance with FICA and the organisation's FICA RMCP. Consideration will be given on an annual basis to the re-appointment or replacement of the AML Compliance Officer and the re-appointment or replacement of any Deputy AML Compliance Officers.

5.2 FICA LICENSING AND MAINTENANCE

5.2.1 FIC Registration

The AML Compliance Officer will ensure that the organisation is registered as an "accountable institution" with the FIC within 90 days from the date of commencing its business.

The AML / Compliance Officer will retain the following records pertaining to the registration process:

- The organisation's "Org ID"
- The organisation's particulars provided during the registration process
- The log-in particulars required to access the FIC's reporting portal ("goAML")
- The "Confirmation of Entity Registration" notification received from the FIC

The AML / Compliance Officer will ensure that the organisation remains registered whilst operating as one of the businesses listed under Schedule 1 and/or Schedule 3 of FICA.

5.2.2 Changes to Registration Particulars

The AML Compliance Officer will monitor any changes to the organisation's business particulars and/or contact details which must be communicated to the FIC.

Where any of the organisation's particulars are updated subsequent to the registration process, the AML Compliance Officer will communicate these changes to the FIC within 15 business days after such change, but no later than 90 days after such change.

The AML Compliance Officer will update the organisation's details via the FIC's website portal and will ensure that the updated information is validated within 5 business days of communicating any changes.

The AML Compliance Officer will keep a record of his or her instructions to the FIC as well as any confirmation notifications received from the FIC.

5.3 FICA CLIENT DUE DILIGENCE PROCEDURES

The organisation has adopted a risk-based approach with regards to performing Client Due Diligence procedures. The risk-based approach allows the organisation's

employees to conduct proportionate levels of identification and verification activities depending on the ML/TF risks that have been identified for each individual transaction.

All employees responsible for interacting with clients and/or maintaining client and transaction records will at all times observe the organisation's implemented control measures and conduct the appropriate Client Due Diligence procedures as outlined in:

- Vault Markets – AML Program
- Vault Markets – Customer Risk Assessment Methodology
- Vault Markets – Initial Screening Procedure
- Vault Markets – KYC and Ongoing Due Diligence Overview

The AML Compliance Officer will monitor employee's continued compliance with the Client Due Diligence procedures as outlined below.

5.3.1 EDD Procedures where a ML/TF High-Risk Client, Product or Service is Identified

As part of its client onboarding process, the organisation will determine whether a single transaction or business relationship to be concluded pursuant to a new or an existing business relationship, must be classified as ML/TF High-Risk.

ML/TF High-Risks are those that have been identified by the organisation as more likely to be exploited for money laundering or the financing of terrorism purposes.

The organisation will perform Enhanced Client Due Diligence procedures on all prospective and existing clients identified as ML/TF High-Risk.

For detailed information and review periods please refer to the following policies:

- Vault Markets – AML Program
- Vault Markets – Customer Risk Assessment Methodology

5.3.2 Understanding and Obtaining Information concerning a new Business Relationship

When engaging with a prospective client to establish a business relationship, the organisation will obtain information to reasonably enable the organisation to determine whether future transactions that will be performed in the course of the business relationship concerned, are consistent with the organisation's knowledge of the prospective client.

The process is recorded in detail within the "*Vault Markets – On-Boarding Procedure*".

The AML Compliance Officer will monitor the organisation's continued compliance with this requirement by performing regular spot checks.

5.3.3 Establishing and Verifying the Identity of Prospective Clients

When engaging with a prospective client to enter into a single transaction or to establish a new business relationship, the organisation will, in the course of concluding that business relationship establish and verify the identity of the client.

The process is recorded within:

- *Vault Markets – On-Boarding Procedure*
- *Vault Markets – AML Program*
- *Vault Markets – Process Flow Diagrams*

5.3.4 Avoiding Clients with apparent False or Fictitious Names

The organisation will not conclude a transaction or business relationship with an anonymous client, or a client with an apparent false or fictitious name.

If at any stage during the employee's interactions with a client or a client representative, the employee suspects that a false or fictitious name is being provided, the employee will:

- refrain from communicating his or her suspicion to the client or client representative,
- terminate the transaction, and
- report his or her suspicion to the AML Compliance Officer

The AML Compliance Officer will investigate all such reports and consider submitting a Suspicious or Unusual Transaction Report to the FIC.

Please refer to:

- Vault Markets – AML Program Policy

- Vault Markets - Process Flow Diagrams

5.3.5 Avoiding and Terminating a Business Relationship or Single Transaction where unable to conduct a Client Due Diligence

Where the organisation is unable to:

- establish or verify the identity of a client, and/or the identity of a client representative, or
- obtain information regarding the nature of and/or the intended purpose of the business relationship, or
- obtain information regarding the source of funds the client expects to use in concluding transactions in the course of the business relationship concerned, or
- perform ongoing due diligence procedures

The organisation will (as it applies):

- Not establish a business relationship with that client
- Terminate an existing business relationship with a client.

Where employees responsible for interacting with clients and/or maintaining client and transaction records are unable to conduct a Client Due Diligence procedure for any reason, the employee will cancel the transaction and inform the AML Compliance Officer.

The AML Compliance Officer will investigate the reason why the Due Diligence procedure cannot be performed and will take the necessary appropriate action.

5.3.6 Avoiding Transactions and Business Relationships with Persons and Entities identified by the United Nations Security Council

The organisation will avoid transactions where it is suspected that the transaction will or may facilitate the acquisition, collection, use or provision of property or any other economic support, for the benefit of, or at the direction of, or under the control of a person or an entity identified pursuant to a resolution of the Security Council of the United Nations.

The organisation will take reasonable measures to establish whether a prospective client, or an existing client or client representative is indicated on the UN Security Council Sanction List.

The organisation has detailed its Sanction Policy and detailed information can be found within:

- Vault Markets - Sanctions Policy
- Vault Markets - Initial Screening Procedure
- Vault Markets - Process Flow Diagram.

If at any stage during the employee's interactions with a client or a client representative, the employee suspects that a client is listed on the UN Sanction list, the employee will report this suspicion to the AML Compliance Officer.

The AML Compliance Officer will investigate all such reports and consider submitting a Suspicious or Unusual Transaction Report, a Terrorist Financing Activity Report or a Terrorist Financing Transaction Report to the FIC.

5.3.7 Additional Due Diligence Procedures where a client is a Domestic Prominent Influential Person

The organisation will determine whether a prospective client with whom it engages, or the beneficial owner of that prospective client, is a domestic prominent influential person.

Where it is established that the prospective client, or the beneficial owner of the prospective client, is a domestic prominent influential person, the organisation will, as per its AML Policy (*Vault Markets - AML Program*) determine whether it does not want to enter into a relationship with the customer or apply enhanced due diligence.

5.3.8 Additional Due Diligence Procedures where a client is a Foreign Prominent Public Official

The organisation will determine whether a prospective client with whom it engages, or the beneficial owner of that prospective client, is a foreign prominent public official.

Where it is established that the prospective client, or the beneficial owner of the prospective client, is a foreign prominent influential person, the organisation will, as per its AML Policy (*Vault Markets - AML Program*) determine whether it does not want to enter into a relationship with the customer or apply enhanced due diligence.

5.3.9 Additional Due Diligence Procedures where a client is a Family Member or a Close Associate of a DPIP or a FPPO

The organisation will determine whether a prospective client with whom it engages, or the beneficial owner of that prospective client, is an immediate family member or a known close associate of a domestic prominent influential person or a foreign prominent public official.

Where it is established that the prospective client, or the beneficial owner of the prospective client, is an immediate family member or a known close associate of a domestic prominent influential person or a foreign prominent public official, the organisation will, as per its AML Policy (*Vault Markets - AML Program*) determine whether it does not want to enter into a relationship with the customer or apply enhanced due diligence.

5.3.10 When in Doubt, confirming the Veracity of previously obtained Client Information

Where the organisation, subsequent to entering into a business relationship, doubts the veracity or adequacy of previously obtained information, the organisation will repeat the steps required to establish and verify the client's or client representative's identity, to the extent that is necessary to confirm the information in question.

In order to confirm the veracity of previously obtained client information, the AML Compliance Officer will compare the information established and verified during the previous and latest Client Due Diligence process and where there is a discrepancy, the AML Compliance Officer will update the customer file/information.

The organisation will conduct periodic client information reassessments in order to confirm whether the information that the organisation has on record is still accurate and up-to-date. The frequency of these reassessments is depended on the client's ML/TF Risk-Rating and is further detailed in "*Vault Markets - Customer Risk Assessment Methodology".*

The Frequencies are:

Customer Risk Rating	Review Schedule
Low	Every 3 years
Medium	Every 2 Years
High	Annually

5.3.11 Ongoing Due Diligence and the Monitoring of Transactions of Existing Business Relationships

The organisation will conduct ongoing due diligence in respect of all existing business relationships. The ongoing due diligence process will include the monitoring of transactions undertaken throughout the course of the business relationship, including, where necessary:

- the source of funds, to ensure that the transactions are consistent with the organisation's knowledge of the client and the client's business and risk profile, and
- the background and purpose of all complex, unusually large transactions, and all unusual patterns of transactions, which have no apparent business or lawful purpose.

The ongoing due diligence process will also ensure that client information that was obtained during the Client Due Diligence procedure remains accurate and up-to-date.

The AML Compliance Officer will monitor client activities during the business relationship which are not consistent with the organisation's knowledge of the client.

Where the AML Compliance Officer has identified unusual patterns of transactions, he or she will investigate whether or not there is a valid reason or purpose for the client to conclude these unusual transactions.

Where it is established that these transactions have no valid or lawful purpose, the AML Compliance Officer will submit a Suspicious and Unusual Transaction Report to the FIC.

Further information can be found in:

- Vault Markets - Suspicious Matters Reporting Policy
- Vault Markets - Transaction Monitoring Procedure
- Vault Markets - KYC and Ongoing Due Diligence Overview
- Vault Markets - AML Program

5.4 FICA REPORTING DUTY

5.4.1 Submitting Suspicious or Unusual Transaction Reports within the Prescribed Time Limit

Any person who knows or ought reasonably to have known or suspected that:

- the organisation has received, or is about to receive, or if a transaction was concluded, may have received, the proceeds of unlawful activities or property which is connected to an offence relating to the financing of terrorist and related activities, or
- a transaction or series of transactions to which the organisation is a party:
    - facilitated or is likely to facilitate, or if the transaction was concluded, may have facilitated, the transfer of the proceeds of unlawful activities or property which is connected to an offence relating to the financing of terrorist and related activities, or
    - has no apparent business or lawful purpose, or
    - is conducted for the purpose of avoiding giving rise to a reporting duty under FICA, or
    - may be relevant to the investigation of an evasion or attempted evasion of a duty to pay any tax, duty or levy imposed by legislations administered by the South African Revenue Services, or
    - relates to an offence relating to the financing of terrorist and related activities, or

- will or may facilitate the acquisition, collection, use or provision of property or any other economic support, for the benefit of, or at the direction of, or under the control of a person or an entity identified pursuant to a resolution of the Security Council of the United Nations, or

- the organisation has been used or is about to be used, or if the transaction was concluded, may have been used, in any way for money laundering purposes or to facilitate the commission of an offence relating to the financing of terrorist and related activities,

must within the prescribed period after the knowledge was acquired or the suspicion arose, report to the FIC the grounds for the knowledge or suspicion.

Where an employee suspects that the organisation has been used or is about to be used, for money laundering or terrorist financing purposes, he or she will notify the AML Compliance Officer of this transaction in writing within one business day of such a transaction.

The employee may not disclose his or her suspicion, or any information regarding the contents of any such notification to any other person, including the person in respect of whom the report is or must be made.

The AML Compliance Officer will submit a Suspicious or Unusual Transaction Report to the FIC as soon as possible but not later than fifteen days after the employee became aware of a fact concerning a transaction on the basis of which knowledge or a suspicion concerning the transaction must be reported.

The AML Compliance Officer will keep a record of all reports submitted to the FIC.

The AML Compliance Officer will also keep a record of all transactions and activities which gave rise to the submittal of a suspicious and unusual transaction report, for at least five years from the date on which the report was submitted to the FIC.

5.4.2 Submitting Terrorist Property Reports within the Prescribed Time Limit

Where the organisation has in its possession or under its control:

- property associated with terrorist and related activities, or
- property owned or controlled by or on behalf of, or at the direction of a specific person or entity identified:

- by a notice issued by the President under Section 25 of POCDATARA, or
- pursuant to a resolution of the Security Council of the United Nations, the organisation will within the prescribed period report that fact to the FIC.

Where an employee has knowledge that the organisation has in its possession or under its control property associated with terrorist or related activities, he or she will notify the AML Compliance Officer within one business day after he or she has established this fact.

The AML Compliance Officer will submit a Terrorist Property Report to the FIC as soon as possible but not later than five (5) days after the employee established that the organisation has property associated with terrorist and related activities in its possession or under its control.

The AML Compliance Officer will keep a record of all reports submitted to the FIC.

5.5 FICA RECORDKEEPING

5.5.1 Maintaining Transaction Records for the Required Period

The organisation will keep a record of every transaction (whether the transaction is a single transaction or concluded in the course of a business relationship), which the organisation has with all its clients.

The organisation will ensure that the transaction records:

- contain sufficient information, to enable the organisation to readily reconstruct the transaction, and
- that all transaction records reflect at least:
  - the amount involved and the currency in which it was denominated
  - the date on which the transaction was concluded
  - the parties to the transaction
  - the nature of the transaction
  - any business correspondence, and

- where the organisation provides account facilities to its clients, the identifying particulars of all accounts and the account files at the organisation that are related to the transaction.

The transaction records may be kept in electronic form. Where the organisation maintains transaction records in electronic form, the AML Compliance Officer will ensure that these records are capable of being reproduced in a legible format and that they are backed-up on a periodic basis.

The AML Compliance Officer will keep all transaction records for at least five years from the date on which the transaction was concluded.

5.5.2 Maintaining Client Due Diligence Records for the Required Period

The organisation will keep an accurate record of:

- all information pertaining to a client, or a prospective client, pursuant to the Customer Due Diligence requirements
- copies of, or references to, information provided to or obtained by the organisation to verify a person's identity, and
- in the case of a business relationship, reflect the information obtained by the organisation concerning:
  - the nature of the business relationship
  - the intended purpose of the business relationship, and
  - the source of funds which the prospective client is expected to use in concluding transaction in the course of the business relationship.

The due diligence records may be kept in electronic form. Where the organisation maintains due diligence records in electronic form, the AML Compliance Officer will ensure that these records are capable of being reproduced in a legible format and that they are backed-up on a periodic basis.

The AML Compliance Officer will keep all Customer Due Diligence records, for at least seven years from the date on which the business relationship is terminated. The legal requirement is to retain records for 5 years – JP Markets therefore employs a stricter approach to record retention than that which is required.

5.5.3 Ensuring Compliance where Transaction or Due Diligence Records are maintained by a Third Party

Where the organisation has outsourced the recordkeeping requirements to a third party, the organisation will ensure that:

- the organisation has free and easy access to the records,
- the records are readily available to the FIC or any other relevant supervisory body, and
- it provides the FIC with the prescribed particulars concerning the third party.
- The AML Compliance Officer will without delay provide the FIC with the third party's:
    - full name, if the third party is a natural person, or registered name, if the third party is a close corporation or a company
    - The full name and contact particulars of the individual who exercises control over access to the records
    - The address where the records are kept
    - The address where the third-party exercises control over the records
    - The full names and contact particulars of the individual who liaises with the third party on behalf of the organisation.

5.6 FICA AWARENESS TRAINING

The organisation will provide ongoing training to its employees to enable them to comply with the provisions of FICA and the FICA Risk Management and Compliance Programme.

An example of a FICA Awareness Training Register can be found under Annexure B.

6. COMPLIANCE RISK AND IMPLEMENTED CONTROLS

The organisation has identified compliance risks considering its compliance objectives and obligations.

The compliance risks have been assessed and evaluated based on the likelihood of the risk occurring, as well as the potential impact should the risk event occur and is contained within the 'Vault Markets - AML-CTF Risk Register'.

7. DISCIPLINARY ACTION

Where a FICA related complaint or an investigation related to an infringement of FICA or the organisation's FICA RMCP has been finalised, the organisation may recommend any appropriate administrative, legal and/or disciplinary action to be taken against any employee reasonably suspected of being implicated in noncompliance.

In the case of ignorance or minor negligence, the organisation will undertake to provide further FICA Awareness training to the employee.

Any gross negligence or the wilful noncompliance, will be considered a serious form of misconduct for which the organisation may summarily dismiss the employee. Disciplinary procedures will commence where there is sufficient evidence to support an employee's gross negligence.

Examples of immediate actions that may be taken subsequent to an investigation include:

- A recommendation to commence with disciplinary action.
- A referral to appropriate law enforcement agencies for criminal investigation.
- Recovery of funds and assets in order to limit any prejudice or damages caused.

8. COMPLIANCE MONITORING

The AML Compliance Officer will use well-established methods for the reviewing, sampling and testing of internal controls. The purpose of compliance monitoring is to reasonably ensure that the organisation complies with FICA and the FICA RMCP. An example of a Compliance Monitoring Schedule can be found under Annexure A.

ANNEXURES

ANNEXURE A

(INSERT YEAR) COMPLIANCE MONITORING SCHEDULE													
Activity to be Monitored	**Random Checks**	**Annual**	**Jan**	**Feb**	**Mar**	**Apr**	**Jun**	**Jul**	**Aug**	**Sept**	**Oct**	**Nov**	**Dec**
Annual review of the AML & CTF RMCP		•											
Appointment of the AML / Compliance Officer		•											

Appointment of the Deputy AML / Compliance Officer		•											
Confirmation of FIC Registration		•											
Monitoring changes to organisation's registration particulars			•			•			•			•	
Periodic Product and Service ML/TF Risk Analysis	•	•											
Review of the Client ML/TF Risk Identification Criteria				•						•			
Periodic updating of UN Security Council Sanction List			•						•				
Submittal and Record Keeping of Cash	•												

Threshold Reports													
Submittal and Record Keeping of Suspicious or Unusual Transaction Reports	•												
Submittal and Record Keeping of Terrorist Property Reports	•												
Retention and Back-ups of FICA Transaction Records	•			•			•			•			•
Retention and Back-ups of FICA Client Due Diligence Records	•			•			•			•			•
Ensuring that employees undergo annual FICA Awareness Training		•											
Periodic review of Senior Management					•						•		

Approval Procedure													
Periodic review of Client Due Diligence Activity Sheet			•			•			•			•	
Periodic review of Client Due Diligence Forms			•			•			•			•	
Ongoing Due Diligence and Monitoring of Existing Business Relationships	•		•	•	•	•	•	•	•	•	•	•	•
Client random spot checks: UN Security Council List	•												
Client random spot checks: False or Fictitious verification documents	•												
Client random spot checks:	•												

DPIP or FPPO													
Client random spot checks: Family or Associate of DPIP or FPPO	•												
Monitoring Compliance with Client Due Diligence procedure	•												
Monitoring Compliance with Additional Information on a New Business Relationship	•												
Annual review of Compliance Monitoring Programme		•											

ANNEXURE B

Learner Name	Date of Training	Type of Training / Link to training material	Training Provider	Date Successfully Completed	Next Training Date	Comments

Version 1.0 January 2024

Version 1.0 January 2024