FICA POLICYAND PROCEDURE

Policy Number	**RD-P-TR-03**
Last Approved	**January 2021**
Version Number	**03**
Policy Type	**Strategic**
Compiled by:	**Risk Division**
Approved by:	**TCTA Board**
Signed on behalf of the Board by:	**Board Chairperson** **Name: Gerald Dumas**
	Signature: Digitally signed by Gerald Dumas Date: 2021.05.13 11:33:32 +02'00'
	Effective Date: 29 April 2021

TABLE OF CONTENTS

1. PURPOSE OF THE POLICY

1.1 This Policy documents TCTA's commitment to the Financial Intelligence Centre Act No 38 of 2001 as amended by the Financial Intelligence Centre Amendment Act of 2017. It further aims to foster compliance with the Act's associated regulations and guidance notes and the Prevention of Organised Crime Act No 24 of 1999.

1.2 The procedures outlined in this Policy re-enforce TCTA's commitment to preventing money-laundering activities from occurring within the organization. This Policy is developed to meet its regulatory and statutory obligations, covering several business-related activities including *inter alia* due diligence, record-keeping requirements, internal controls, internal training and internal communication and reporting procedures.

1.3 For the purpose of this policy, the provisions of section 42 (2)(q) of the Fica Amendment Act shall not be applicable to the policy because TCTA does not have any branches or subsidiaries, the policy will be implemented at head office where all TCTA operations are managed.

2. DEFINITIONS, ABBREVIATIONS, ACRONYMS

Accountable Institution	An accountable institution is any person or entity, as described in Schedule 1 of the Financial Intelligence Centre Act No. 38 of 2001, that must ensure adherence to the legal requirements and responsibilities as set out therein. Accountable institutions can be split into two distinct categories: Primary and Secondary accountable institutions.
Primary Accountable Institution	These institutions are responsible for verifying and keeping records of the identities of their counterparties.
Secondary Accountable Institutions	These institutions rely on the compliance of the Primary Accountable Institutions and, therefore, are not required to verify the identities of the Primary Accountable Institution's counterparties.
Act	Financial Intelligence Centre Act No. 38 of 2001 (also known as 'FICA'), as amended by the Financial Intelligence Centre Amendment Act of 2017.
Counterparty Due Diligence	The steps and procedures taken to identify and verify counterparties. For the purposes of acronyms, the process is also referred to as 'CDD'.
Enhanced Due Diligence	exercise is to source additional information to that which is obtained during the EDD process on high-risk counterparties.

Financial Intelligence Centre	The Financial Intelligence Centre is South Africa's centre for gathering, analysis and dissemination of financial intelligence. It was established to identify proceeds of crime and to combat money laundering and the financing of terrorism. Its primary role is to protect the integrity of the country's financial system. For the purposes of acronyms, the centre is also referred to as "FIC".
Financial Sector Conduct Authority	Under the 'Twin Peaks' model that introduces two parallel regulators within the financial sector, the Financial Sector Conduct Authority (FSCA) acts as a dedicated financial market conduct regulator. Its primary goal is to protect financial counterparties through supervising market conduct. Whereas the Prudential Authority's primary goal is to protect insurance counterparties. The FSCA was formerly known as the Financial Services Board of South Africa, or 'FSB'.
Law enforcement agencies	Financial Intelligence Centre, South African Police, National Prosecuting Authority, National intelligence agencies, South African Revenue Services, the Independent Police Investigative Directorate, Special Investigative Unit and supervisory bodies including the Financial Sector Conduct Authority and Prudential Authority
MLRO	Money Laundering Reporting Officer; at TCTA, the Assistant Compliance Officer performs this role.
Money Laundering	Any process that gives the proceeds of unlawful activities the appearance of originating from a legitimate source.
PIP	Prominent Influential Persons refer to individuals who are, or were in the past, entrusted with prominent functions in a country and includes their immediate family members and known close associates. PIPs can be split into two distinct categories: Foreign Prominent Public Officials and Domestic Prominent Influential Persons.
Foreign Prominent Public Officials	Individuals who hold or have held prominent positions during the preceding 12 months in a foreign country.
Domestic Prominent Influential Persons	Individuals who hold or have held (including acting positions exceeding 6 months) prominent positions within the Republic of South Africa.
POCA	Prevention of Crime Act No 24 of 1999, which stipulates criminal and civil offences, and penalties.
Tipping-off	Any instance where an individual within TCTA (including its stakeholders) discloses information that could prejudice an investigation into money laundering to someone outside of the approved reporting chain.

3. A BRIEF LOOK AT ANTI-MONEY LAUNDERING & FICA

3.1 Money laundering is the manipulation of illegally acquired wealth in order to obscure its true nature or source. The goal of money laundering is to place illegal money in the formal financial system without arousing suspicion. Secondly, to transfer and move money around in a series of complex transactions, so it becomes difficult to trace its original source.

The bellow mentioned Acts were enacted to prevent money laundering:

- **FICA (FINANCIAL INTELLIGENCE CENTRE ACT (Act No. 38 Of 2001)):**

  This Act provides for the establishment of the Financial Intelligence Centre and it creates obligations for accountable institutions to comply with. It also regulates the reporting of terrorist related activities and makes non-compliance with the Act a criminal offence.

- **POCA (PREVENTION OF ORGANISED CRIME ACT (Act No. 121 Of 1998)):** This act deals with money laundering, racketeering and criminal and civil forfeiture. POCA sets out money laundering offences. It also creates a general reporting obligation for businesses coming into possession of suspicious transactions.

- **POCDATARA (PROTECTION OF CONSTITUTIONAL DEMOCRACY AGAINST TERRORISM AND RELATED ACTIVITIES (Act No. 33 Of 2004)):** This act provides for new reporting obligations under FICA. The reporting of suspicious and unusual transactions was extended to cover transactions relating to property which is connected to an offence relating to the financing of terrorist and related activities, or to the financing of terrorist related activities.

It is the responsibility of the Accountable Institution to:

- Guard against crime and unlawful practices
- Report alleged or attempted crimes and unlawful or unethical activities to persons in authority without protecting any party involved.
- The accountability and responsibility for the effective management of anti-money laundering procedures lies with the Senior management (Key Individual) and may be delegated to responsible employees.

4. RISK MANAGEMENT & COMPLIANCE PROGRAMME

4.1 The Risk Management & Compliance Programme (RMCP) outlines the measures TCTA, and its stakeholders use to identify, assess, monitor, mitigate and manage any risks related to money laundering and the financing of terrorism.

TCTA JOHANNESBURG STOCK EXCHANGE (JSE) ACTIVITIES

4.2 TCTA transacts in bonds on the JSE's Interest Rate market as part of its mandate to fund and manage the debt of the Lesotho Highlands Water Project (LHWP). To this end, the organization has issued several bonds on the Bond Exchange of South Africa (BESA) and its successor, the JSE, over the years. TCTA engages in both outright sales and purchases of bonds (sells bonds to fund itself and buys them back when it has excess funds or as part of its debt management strategy). It further conducts Repo (buy and sell-back) transactions for short-term funding and to provide liquidity in its bonds.

4.3 TCTA only engages in bond trading with members of the JSE. Therefore, it relies on the AML/CTF policies and procedures of the JSE for the assessment and verification of the counterparties from which it sells and purchases its bonds. While TCTA counts on third-party assurance measures, it will conduct periodic reviews to safeguard continued compliance with the Act.

4.4 TCTA counterparties are JSE members who have been screened and verified by the JSE for FICA purposes, for this reason, TCTA will place reliance on JSE to make sure that all the counterparties doing business with TCTA are FICA compliant.

COUNTERPARTY RISK RATING

4.4 Due to the broad scope of the counterparty base, it is not practical to determine whether prospective counterparties intend to establish long-term business relationships or conclude single transactions with TCTA. Many counterparties may very well conclude a 'single' transaction in that they invest in a specified instrument or bond. Given this reason, TCTA focuses on CDD and the associated reporting obligations for the specific counterparties.

4.5 TCTA shall treat prospective or new counterparties as high risk until circumstances dictate otherwise.

4.6 Factors that will escalate a counterparty's risk rating include, but are not limited to, the following:

i) A counterparty's unreasonable resistance or unwillingness to provide requested CDD documentation;

ii) Inconsistencies between provided CDD documentation and counterparty information on record;

iii) Suspicious account activity and/or transactions;

iv) Being flagged against sanction watch lists; and

v) Being identified as a PIP or as a family member or associate of a PIP.

PRINCIPLE OF 'GOOD FAITH'

4.7 TCTA extends 'good faith' to new and existing counterparties because it deems them to have legitimate sources of funds and business reasons for making use of the organization's services. Unless evidence demands otherwise, TCTA will always extend 'good faith' to counterparties.

4.8 In a similar vein, when a counterparty withdraws business from TCTA, the organization shall continue to extend 'good faith', based on the assumption that there are honest and legitimate reasons for the decision. Where appropriate, counterparty agreements may require certification that they will be responsible for their reporting obligations and that their initial and subsequent funds are not the proceeds of criminal activities.

4.9 TCTA will not establish relationships with any individual or entity that will expose its reputation to risk. The organization does this to protect its good name and those of its counterparties.

4.10 If TCTA suspects a counterparty of illegal activities, upon investigation, it may deem this a violation of the 'good faith' it has extended. The organization reserves the right to end business relationships with existing counterparties if they violate 'good faith' in this manner. The decision to terminate a relationship will be made by the Executive Committee (EXCO). Moreover, TCTA will report its suspicions to the relevant law enforcement agencies.

4.11 Employees involved in ending a business relationship must work on the case with the TCTA MLRO who will liaise with law enforcement agencies before communicating TCTA's intention to terminate an association with a counterparty.

COUNTERPARTY DUE DILIGENCE

4.12 Prospective counterparties desiring to transact with TCTA are required to complete the application form/s to facilitate their investments. Each application form requires several

supporting documents to be provided about the prospective counterparty's identity. Acceptable forms of verification ground TCTA's CDD processes.

4.13 Upon receipt of the completed applications and supporting documents, the information is reviewed to ensure consistency, completeness, and accuracy.

4.14 Should TCTA be dissatisfied with the provided documentation or have any doubts as to the identity of a prospective counterparty, it shall not establish a business relationship with them. The same would apply if the organization note any inconsistencies or should the prospective counterparty be unwilling to provide the required supporting documents. Subject to the circumstances involved, TCTA reserves the right to file a Suspicious & Unusual Transaction Report with the Financial Intelligence Centre.

4.15 After the initial application and acceptance, TCTA will screen a counterparty against several watch lists on an ongoing basis to identify:

i) Sanctioned individuals;

ii) Organised crime and threat finance; and

iii) Politically Influential Person relationships.

FAILURE TO CONDUCT COUNTERPARTY DUE DILIGENCE PROCESSES

4.19 Any accountable institution failing to comply with the CDD requirements, as set out in the Act, shall be subject to an administrative sanction.

PROMINENT INFLUENTIAL PERSONS

These categories of people must be given special treatment in terms of FICA. People falling into this category are those listed in Annexure1. If we are dealing with Foreign Influential Persons, or their family members or known close associates, these people are automatically high risk and additional client due diligence steps must be taken before establishing a business relationship or entering into a single transaction with such a person. The purpose of the PIP EDD exercise is to source additional information to that which is obtained during the CDD process on high-risk clients. The output of the PIP EDD process must enable EXCO to determine if the PIP should either be on-boarded as a counterparty, or the counterparty relationship exited, as the case may be.

4.20 Since PIPs are viewed as high-risk, TCTA may introduce at its discretion additional measures to assess whether a potential or existing counterparty or their beneficial owner is a PIP.

4.21 Additional procedures include:

i) EXCO's approval for establishing relationships with a PIP. If such sanction was received in the past, to continue with the business relationship new approval must be sought;

ii) Establish the source of wealth or funds of a PIP; and

iii) Continue screening identified PIPs against the sanction watch lists.

5. REPORTING SUSPICIOUS ACTIVITIES

REPORTING OBLIGATIONS

5.1 TCTA has a legal duty to protect the confidentiality of its counterparties. However, the organization will release to law enforcement agencies information that they require while reporting and investigating suspicious business activities. It will monitor its counterparty transactions for suspicious activity to discharge this responsibility.

5.2 TCTA will not hesitate to report knowledge or suspicion of criminal conduct were obligated to do so. The organization recognises that failing to do so is an offence. In reporting suspicious and illegal activities, TCTA will fully use of the protection legislation affords reporters. This legislation protects any reporting entity. They cannot be charged with assisting criminal endeavours.

5.3 The MLRO will serve as TCTA's primary contact when meeting with law enforcement agencies. When meeting with the agencies, the MLRO must include the Chief Risk Officer, Executive Manager: Project Finance and Treasury, Treasury Manager and Compliance Officer.

5.4 TCTA will introduce procedures to reduce the risk of an employee tipping-off a counterparty or any other person with whom they are in contact. Tipping-off is a criminal offence that carries heavy penalties for TCTA (as an accountable institution) and the offending employee (in their individual capacity).

PROTECTION WHEN MAKING REPORTS

5.5 No action, criminal or civil, can be brought against TCTA (as an accountable institution) or any of its employees (as individuals) for complying in good faith with the Act.

5.6 Any person who has made, initiated, or contributed to a report in terms of the Act is not obligated to give evidence in criminal proceedings.

5.7 The identity of any person who has made, initiated, or contributed to a report in terms of the Act will not be admissible as evidence in criminal proceedings unless the person testifies at those proceedings.

POLICY AND PROCEDURE

5.8 TCTA will implement a strict reporting process for suspicious activity that may be identified during the ordinary course of business. This process is laid out in detail in the pages that follow. Any deviation from this process will require the approval of the Board of Directors.

STAGE 1

5.9 Stage one of the process requires employees to identify suspicious activities. What makes a transaction abnormal or suspicious? Put simply, it is any transaction that has been structured unusually.

STAGE 2

5.10 Stage two requires that the employee complete an 'Anti-Money Laundering Report'. The employee must explain his/her reasons for suspecting a given transaction in detail.

5.11 Once the report has been completed, the employee should present it to their Executive Manager. They will discuss the facts, review the report and, where appropriate, add more information about the counterparty or transaction if relevant to the matter under consideration. Employees involved in discussing the report must sign it to confirm that they suspect the transaction. If an employee suspects the Executive to be involved with the suspicious activity under consideration, the MLRO should be contacted immediately. If the MLRO is suspected, the employee should engage with the Chief Risk Officer or the Chief Executive Officer.

5.12 Suspicions must not be discussed with anyone other than those mentioned above. Once the reporting process has begun, it must be followed through to completion, even if the original suspicion does not exist anymore. The MLRO will keep all reports on file for record-keeping and referral purposes.

5.13 It is vital, regardless of whether the suspicions are proven true or not, that no mention of these suspicions is made to the counterparty. Any discussion of this nature risks a tipping-off offence. Employees should always neither confirm nor deny the existence

of a report to a counterparty or third party. Any correspondence that could indicate the existence of a report should not be placed in the counterparty's file.

5.14 Once the report has been completed, it must be presented to the MLRO who will acknowledge its receipt in writing. The employee will then receive guidance from the MLRO on how to proceed with the counterparty in question. If the counterparty demands that subsequent transactions be executed, the situation must be discussed with the MLRO before any action is taken. In certain cases, the MLRO may decide to allow transactions to continue in order not to raise the counterparty's suspicions. Regardless, the MLRO should be kept informed of all dealings with the counterparty.

STAGE 3

5.15 Stage three of the process is handled exclusively by the MLRO. The MLRO must decide, based on the employee's report and available information (including additional enquiries), whether the transaction has remained suspicious. If the MLRO feels that the transaction has remained suspicious, the MLRO will make an official report to the relevant law enforcement agencies all reports made to law enforcement agencies will be kept in a 'Money Laundering Reporting Register' for record-keeping and referral purposes.

5.16 The initiating employee will receive an acknowledgement signed by the MLRO confirming that their legal obligations in terms of this policy have been met. If the employee has not received a confirmation within one week of submitting the initial report, the MLRO should be contacted immediately.

NON-DISCLOSURE OF REPORTS

5.17 When the MLRO files a report about suspicious transactions with the Financial Intelligence Centre, any person involved in its compilation and submission must not disclose its nature or any information related to it to anyone.

RECORD KEEPING RELATED TO REPORTS

5.18 Records are kept providing an audit trail and adequate evidence to law enforcement agencies during their investigations. However, these records will only be provided at the request of law enforcement agencies.

5.19 All records will be kept for at least five (5) years from the date of the last transaction on the account.

5.20 Records will be stored in line with TCTA Records Management Policy and Records Management Procedure, whereby they will be kept either as a soft copy or hard copy

on-site for a limited period of three (3) years and thereafter will be transferred to an off-site secured facility for the remainder of retention period.

5.21 Upon expiry of the retention period the documents will be destroyed, and a destruction register will be maintained in line with the approved policy and procedure.

5.22 The documents will not be destroyed without the approval of the Compliance Officer.

6. TIPPING-OFF

6.1 Any employee of TCTA who discloses information to someone outside the internal reporting chain, potentially prejudicing an investigation into money-laundering activities, will be guilty of 'tipping-off'.

6.2 The internal reporting chain of TCTA is as follows:

i) The employee/s who became aware of the suspicious activities.

ii) The Executive Manager

iii) The MLRO

iv) The Law Enforcement Agencies

6.3 Any employee found to have deliberately acted against the provisions of this Policy—including tipping-off counterparties—will be subject to the internal disciplinary procedures of TCTA, and the potential penalties as detailed in the legislation.

6.4 For employees to be guilty of 'tipping-off', they must have known of or suspected that a money-laundering investigation was about to be conducted. TCTA shall deem an employee to have been aware of a pending investigation if:

i) A disclosure has been made or is about to be made to a person in the internal reporting chain: or;

ii) A court order has been served or is about to be served by a law enforcement agency compelling the production of documents and/or information.

6.5 If an employee makes a general enquiry, requesting additional information from a counterparty before a person in the internal reporting chain is notified or a court order is received, he/she will not have committed a tipping-off offence. This is specifically in relation to enquiries regarding the identity of a counterparty or the nature of a transaction.

7. STAFF TRAINING

INTERNAL TRAINING PROGRAMME

7.1 TCTA employees, whether permanent or part-time, will receive anti-money laundering training necessary for their job function. The Compliance Department will provide training to ensure that all employees have been made aware of the offences detailed in the legislation for non-reporting, tipping-off and consciously or unconsciously assisting money launderers. They have further been made aware of their responsibilities, both as individuals within their respective business units and as employees of TCTA.

7.3 All employees are required to sign a register when attending the training sessions. Each employee attending the session will receive a copy of the latest version of this Policy. The signed register will be kept in the Compliance Department.

7.4 Due to employee movement, ongoing training is necessary to maintain awareness of anti-money-laundering processes. TCTA will regularly offer refresher courses for the benefit of new and existing employees alike.

DISCIPLINARY PROCEEDINGS

7.5 Any employee of TCTA who contravenes the requirements and provisions outlined in this Policy shall be subject to internal disciplinary proceedings and administrative sanctions/penalties, as the Act may require.

8. OTHER REPORTABLE ACTIVITIES

CASH THRESHOLD REPORTING

8.1 Cash transactions exceeding R25 000 will be automatically reported to the MLRO.

CROSS-BORDER CONVEYANCE AND ELECTRONIC TRANSFER REPORTING

8.2 Cross-border conveyance and electronic transfers to and from the Republic of South Africa over R25 000 will automatically be reported to the MLRO.

TERRORIST PROPERTY REPORTING

8.3 Any property connected to an offence relating to the financing of terrorist and related activities will be automatically reported to the MLRO.

8.4 Counterparty records will be checked against the United Nations Security Council Sanctions list. Those that are listed for offences related to the financing of terrorist and related activities will be automatically reported to the MLRO.

9. RECORD KEEPING

DOCUMENTATION RETENTION

9.1 TCTA will keep documentation detailing transfers in and out of counterparty accounts, including supporting documents. These documents will be kept on file as soft copy or hard copy, on-site in TCTA for a period of three (3) years and transferred to an off-site facility for the remainder of the period, to retain an audit trail for the money transfers and, should the need ever arise, to provide adequate evidence for law enforcement agencies during their investigations.

9.2 If TCTA receives a court order requiring documents or other information for the use of law enforcement agencies, employees must cooperate and help the MLRO in complying.

9.3 Documents will be kept on file according to the time dictated by legislation. The minimum retention periods for documentation are:

i) Opening Account Records – These records will be kept on a permanent file for as long as the business relationship continues between the counterparty and TCTA and/or its associates. Should the relationship be ended, documents will be kept on file for at least five years after the last transaction or closure of the account.

ii) Account Transaction Records – At least 5 years.

iii) 'Individual' or Stand-alone Transaction Records – At least five (5) years after the transaction was completed.

iv) MLRO register of Reports and supporting documentation – At least five (5) years.

v) Training Records relating to Anti-Money Laundering – At least five (5) years.

9.4 If TCTA knows of a money-laundering investigation that is being conducted by law enforcement agencies it shall keep all records relating to the counterparty and the relevant account on file, until the investigating authorities advise otherwise. The MLRO will manage such incidents, should they occur.

RETRIEVAL OF DOCUMENTS

9.6 TCTA will keep a copy of the RMCP and make it available, upon request, to the FIC or a supervisory body which provides regulatory or supervisory functions. Such copy will be made available for inspection within a reasonable period from the date it is requested or when TCTA is served with a directive to do so. An electronic version will be posted on TCTA SharePoint for employees and website for external stakeholders at www.tcta.co.za.

DESTRUCTION OF DOCUMENTS

9.7 No documentation regarding the procedures outlined above will be destroyed until they have been archived in line with the TCTA Records Management Policy and the National Archives Act and the destruction is authorised by the MLRO.

10. ROLES AND RESPONSIBILITIES

TCTA is an Accountable Institution in terms of FICA and is required to adhere to the regulations issued by the Financial Intelligence Centre. It is also required to report to the Financial Intelligence Centre on the implementation of this Anti-Money Laundering Policy and processes, cash reporting and suspicious transactions reporting.

10.1 THE BOARD

The Board has ultimate responsibility to ensure development and implementation of TCTA's anti-money laundering and prevention of terrorist financing framework. The Board has an oversight role designed to ensure that, inter alia, there is compliance with all the relevant laws, regulations, and international standards. Such compliance should assist in the detection of suspicious transactions and permit the creation of an audit trail if an investigation is deemed necessary.

The Board should be ensuring that:

10.1.1 TCTA is expected to comply with the provisions and the requirements FICA and Regulations;

10.1.2 When the service providers and/or consultants are engaged by TCTA, TCTA retains full responsibility for compliance with the legislation, regulations and international standards.

10.1.3 The Board should therefore demonstrate their commitment to an effective anti-money laundering programme by:

10.1.3.1 understanding the statutory duties place upon them, the employee and TCTA itself;

10.1.3.2 approving the Anti-Money Laundering Policies and Procedures that are appropriate for the investigation of risks;

10.1.3.3 ensuring that TCTA appoints a Compliance Officer to manage the organization's risk of non-compliance with FICA;

10.1.3.4 ensuring that TCTA complies with its statutory responsibilities as it relates to FICA. This includes reviewing the reports from the Compliance Officer, internal audit, external auditors on the operations and effectiveness of compliance systems.

10.2 THE CHIEF EXECUTIVE OFFICER (CEO)

10.2.1 The CEO responsibility is to effectively manage TCTA anti-money laundering regime/programme across the organization;

10.2.2 Ensure that proper processes are in place and necessary approvals are obtained when new business relationships are established;

10.2.3 The CEO is responsible to assign/delegate responsibilities to ensure effective management of the identified anti-money laundering risks within TCTA;

10.2.4 Allocate roles and responsibilities to manage and monitor risks;

10.2.5 Ensure that all the employees and departments in the organization comply with anti-money laundering policy.

10.2.6 Promote awareness of anti-money laundering so that is becomes embedded throughout the organization; and

10.2.7 Ensure that the EXCO incorporate the requirements of the Anti-Money Laundering Policy into their Division's operational processes.

10.3 THE CHIEF RISK OFFICER

The accountability and responsibility for effective management of the anti-money laundering procedures within TCTA lies with the Chief Risk Officer (CRO) and executed by the Compliance Officer.

It is the responsibility of the management to ensure that:

10.3.1 All employees can identify suspicious and unusual transactions, and

10.3.2 Know how to report these transactions;

10.3.3 Identification and verification of the counterparties by the employees as required by FICA are complied with;

10.3.4 Records of the identification and verification documents are kept as required by FICA by the employees who are required to comply with this requirement;

10.3.5 To obtain information to reasonably enable the accountable institution to determine whether future transactions that will be performed during the business relationship

concerned are consistent with the institution's knowledge of that prospective client, including information describing—

a) the nature of the business relationship concerned;

b) the intended purpose of the business relationship concerned; and

c) the source of the funds which that prospective client expects to use in concluding transactions during the business relationship concerned.

10.3.6 Conduct enhanced ongoing monitoring of the business relationship.

10.3.7 Employees receive training to enable them to comply with the legislation and the internal controls applicable to them.

10.4 COMPLIANCE

The Compliance Officer has a responsibility to complete reports to Financial Intelligence Centre relating to cash receipts (above the regulated amount), suspicious and unusual transactions, and activities relating to financing of activities suspected to be linked to terrorism.

TCTA employees and consultants are protected from civil or criminal actions when complying with the provisions of FICA regarding the reporting of cash transactions and suspicious or unusual activities including the financing of terrorist activities. Employees making reports and providing additional information, in good faith, may not be compelled to give evidence in court or have their identity revealed unless they decide to give evidence in court.

11. MONEY LAUNDERING REPORTING OFFICER DETAILS

11.1 The details of the MLRO are:

Email: **AOlukunle@tcta.co.za**

Tel: 012-683 1317

11.2 if the MLRO is not available, please forward queries to smabaso@tcta.co.za for the attention of the Compliance Officer.

12. POLICY MONITORING AND REVIEW (AMENDMENTS & DISTRIBUTION)

This Policy may be updated periodically in line with changes to legislation or to better improve the anti-money-laundering processes of TCTA. An updated version of the

policy will be made available to employees and stakeholders either through internal communications or the TCTA website.