KJTS GROUP BERHAD

(202201020004) (1465701-T)
(Incorporated in Malaysia)

ANTI-MONEY LAUNDERING, COUNTERING FINANCING OF TERRORISM AND COUNTERING PROLIFERATION FINANCING POLICY

1. DEFINITION

AMLA 2001	means Anti-Money Laundering, Anti-Terrorism Financing and Proceeds of Unlawful Activities Act 2001
AML/CFT/CPF	means Anti-Money Laundering, Counter Financing of Terrorism and Counter Proliferation Financing Policy
AML/CFT/CPF Guidelines	means Guidelines on Prevention of Money Laundering, Countering Financing of Terrorism, Countering Proliferation Financing and Targeted Financial Sanctions for Reporting Institutions in the Capital Market issued by SC
CDD	means customer due diligence
KJTS Group	means KJTS Group Berhad (Registration No. 202201020004 (1465701-T)), its direct and indirect subsidiaries, associated, affiliated and related companies (both local and international), whether present or future
KJTS Reporting Entities	means any KJTS Group entity(ies) which fall under the definition of "Reporting Institutions" as described in the First Schedule of the AMLA 2001
ML/TF/PF	means Money Laundering, Terrorism Financing and Proliferation Financing
Policy	means this Anti-Money Laundering, Countering Financing of Terrorism And Countering Proliferation Financing Policy prepared by KJTS Group
SC	means the Securities Commission Malaysia
TFS-TF	means Targeted Financial Sanctions relating to Terrorism Financing
UNSC	means United Nations Security Council
UNSCR	means United Nations Security Council Resolution

2. INTRODUCTION

2.1. KJTS Group, are committed to fully comply with:

2.1.1. the Anti-Money Laundering, Anti-Terrorism Financing and Proceeds of Unlawful Activities Act 2001 ("**AMLA 2001**"); and

2.1.2. any and all other applicable Anti-Money Laundering, Counter Financing of Terrorism and Countering Proliferation Financing ("**AML/CFT/CPF**'') laws, regulations, guidelines, notices, and circulars issued by Bank Negara Malaysia or any other regulatory authority in jurisdictions where KJTS Group operate, from time to time.

2.2. The purpose of this Anti-Money Laundering, Counter Financing of Terrorism and Countering Proliferation Financing Policy ("**Policy**") is to provide guidance to all employees of KJTS Group concerning how to strengthen anti-money laundering governance.

2.3. This Policy complements and should be read in conjunction with our Anti-Bribery and Corruption Policy, Code of Conduct & Ethics and our Whistleblowing Policy, copies of which can be obtained from our website at https://www.kjts.com.my/site/corporate-governance

3. SCOPE

3.1. This Policy establishes the general framework to manage and prevent the risks of KJTS Group's businesses from being used as a conduit for money laundering, terrorism financing or proliferation financing activities. All KJTS Group's employees are required to adhere to the requirements of this Policy when carrying out their daily responsibilities.

3.2. This Policy applies to all KJTS Group's business units or entities especially any entities which fall under the definition of "Reporting Institutions" as described in the First Schedule of the AMLA 2001 ("**KJTS Reporting Entities**"). The standards set out in this Policy are the minimum requirements across all KJTS Group's businesses.

4. GENERAL DESCRIPTION OF MONEY LAUNDERING

4.1. In principle, money laundering generally involves proceeds of unlawful activities that are related directly or indirectly, to any serious offence, that is processed through transactions, concealments, or other similar means, so that they appear to have originated from a legitimate source.

4.2. The process of money laundering comprises three stages, during which there may be numerous transactions that could alert a reporting institution to the money laundering activities. These stages are:

4.2.1. **Placement**: the physical disposal of benefits of unlawful activities by introducing illegal funds (generally in the form of cash) into the financial system;

4.2.2. **Layering**: the separation of benefits of unlawful activities from their source by creating layers of financial transactions designed to disguise the audit trail; and

4.2.3. **Integration**: where integration schemes place the laundered funds back into the economy so that they re-enter the financial system appearing to be legitimate business funds.

4.3. **The Money Laundering Offence**

Pursuant to Section 4 of the AMLA 2001, a money laundering offence is committed when a person:

4.3.1. engages, directly or indirectly, in a transaction that involves proceeds of an unlawful activity or instrumentalities of an offence;

4.3.2. acquires, receives, possesses, disguises, transfers, converts, exchanges, carries, disposes of or uses proceeds of an unlawful activity or instrumentalities of an offence;

4.3.3. removes from or brings into Malaysia, proceeds of an unlawful activity or instrumentalities of an offence; or

4.3.4. conceals, disguises or impedes the establishment of the true nature, origin, location, movement, disposition, title of, rights with respect to, or ownership of, proceeds of an unlawful activity or instrumentalities of an offence.

4.4. **Penalty for Money Laundering Offences**

The penalty for a money laundering offence is, upon conviction, imprisonment for a term not exceeding fifteen (15) years and a fine of not less than five (5) times the sum or value of the proceeds of an unlawful activity or instrumentalities of an offence at the time the offence was committed or five (5) million ringgit, whichever is the higher.

5. GENERAL DESCRIPTION OF TERRORISM FINANCING

5.1. Financing of terrorism generally refers to carrying out transactions involving funds or property, whether from a legitimate or illegitimate source, that may or may not be owned by terrorists, or those have been, or are intended to be used to assist the commission of terrorist acts, and/or the financing of terrorists and terrorist organisations.

5.2. Section 3(1) of the AMLA 2001 defines a "terrorism financing offence" as any offence under section 130N, 130O, 130P or 130Q of the Penal Code, which are essentially:

5.2.1. providing or collecting property for terrorist acts;

5.2.2. providing services for terrorism purposes;

5.2.3. arranging for retention or control of terrorist property; or

5.2.4. dealing with terrorist property.

6. GENERAL DESCRIPTION OF PROLIFERATION FINANCING

6.1. In response to growing concerns over the proliferation of nuclear, biological and chemical weapons and their means of delivery which continue to pose a significant threat to international peace and security, the United Nations Security Council ("**UNSC**") has intensified efforts to strengthen its global sanctions regime in order to prevent, suppress and disrupt proliferation of weapons of mass destruction and its financing.

6.2. As is the case with other UNSC sanctions programmes, targeted financial sanctions on countries and specifically identified individuals and entities (i.e. designated persons) is the primary aspect of its overall sanctions regime to effectively disrupt financial flows across known proliferation networks.

6.3. Recommendation 7 of the Financial Action Task Force Standards requires countries to implement Targeted Financial Sanctions relating to Terrorism Financing ("**TFS-TF**") made under UNSCRs. Under this standard, countries are required to implement targeted financial sanctions without delay to comply with UNSCRs relating to the prevention, suppression and disruption of the proliferation of weapons of mass destruction and its financing.

6.4. Proliferation financing refers to the act of raising, moving, or making available funds, other assets or other economic resources, or financing, in whole or in part, to persons or entities for purposes of weapons of mass destruction proliferation, including the proliferation of their means of delivery or related materials (including both dual-use technologies and dual-use goods for non-legitimate purposes).

6.5. TFS-TF are applicable to persons designated by the UNSC or the relevant committees set up by the UNSC. Designation or listing criteria are:

6.5.1. person engaging in or providing support for, including through illicit means, proliferation- sensitive activities and programs;

6.5.2. acting on behalf of or at the direction of designated person;

6.5.3. owned or controlled by designated person; and

6.5.4. person assisting designated person in evading sanctions or violating UNSCR provisions.

7. POLICY STATEMENT

7.1. KJTS Group adopts a zero-tolerance approach to all forms of money laundering, terrorism financing, and proliferation financing. As a general principle, commercially reasonable due diligence must be conducted to understand the nature, background, and legitimacy of any prospective or existing customer, vendor, third party, or business partner intending to engage in business with KJTS Group. This includes taking reasonable steps to identify the source and destination of funds or assets involved in any transaction.

7.2. KJTS Group's employees should remain vigilant and report any actual or suspected activity involving money laundering, terrorism financing, or related offences to Bank Negara Malaysia and other relevant authorities without delay, in accordance with applicable laws and internal reporting procedures.

7.3. KJTS Group prohibits all involvement in money laundering activities, terrorism financing and proliferation financing either directly or indirectly. Such activities may include, but not limited to the following:

7.3.1. payments made in currencies that differ from invoices, without a legitimate and documented reason;

7.3.2. attempts to make payment in cash or cash equivalents (out of normal business practice);

7.3.3. payments made by third parties who are not contractually engaged with KJTS Group; and

7.3.4. payments to or from bank accounts held by third parties who are not parties to the contract.

7.4. KJTS Reporting Entities must ensure full compliance with the obligations stipulated under Part IV of the AMLA 2001, which include the requirements to:

7.4.1. implement AML/CFT/CPF risk management that commensurate with the level of money laundering, terrorism financing and proliferation financing risks;

7.4.2. conduct customer due diligence;

7.4.3. keep proper record on the customer and transactions;

7.4.4. implement AML/CFT/CPF compliance programme;

7.4.5. report suspicious transaction report (STR); and

7.4.6. report cash threshold report (CTR) for cash transaction exceeding the amount specified, where applicable.

8. RISK-BASED APPROACH APPLICATION

8.1. KJTS Reporting Entities must take appropriate steps to identify, assess and understand its Money Laundering, Terrorism Financing and Proliferation Financing ("**ML/TF/PF**") risks, in relation to its customers, countries or geographical areas and products, services, transactions or delivery channels, and other relevant risk factors.

8.2. The risk assessment processes must incorporate the following:

8.2.1. documenting the risk assessments and findings;

8.2.2. considering all the relevant risk factors before determining the level of overall risk and the appropriate level and type of mitigation to be applied;

8.2.3. keeping the reporting institution's risk assessment up-to-date, considering changes in surrounding circumstances affecting the reporting institution;

8.2.4. having a scheduled periodic assessment or as and when specified by the SC; and

8.2.5. having appropriate mechanisms to provide risk assessment information to the SC.

8.3. KJTS Reporting Entities are required to:

8.3.1. have policies, procedures and controls, which are approved by the board of directors, to enable it to manage and mitigate effectively the ML/TF/PF risks that have been identified and assessed;

8.3.2. monitor the implementation of those policies, procedures and controls and to enhance them if necessary; and

8.3.3. take enhanced measures to manage and mitigate the risks where higher risks are identified.

8.4. The risk control and mitigation measures implemented must commensurate with the risk profile of the particular customer or type of customer.

9. CUSTOMER DUE DILIGENCE

9.1. As a general principle, KJTS Group is required to perform customer due diligence ("**CDD**") procedures when:

9.1.1. at the start of a new business relationship;

9.1.2. it has any suspicion of money laundering, terrorism financing or proliferation financing activities regardless of the amount transacted; or

9.1.3. it has any doubt about the adequacy or authenticity of previously obtained information.

9.2. The management team of KJTS Group is responsible to implement the appropriate CDD procedures relevant to the nature of their business transactions. KJTS Reporting Entities' management team should adopt a risk-based approach when deciding on the degree of CDD to apply. Risks are assessed at the outset of a business relationship and updated regularly.

The CDD procedures could include:

9.2.1. identifying the customer (including foreign body corporate) and verifying such customer's identity using reliable, independent source of documents, data or information;

9.2.2. verifying that any person purporting to act on behalf of the customer is authorised, and identifying and verifying the identity of that person;

9.2.3. identifying and take reasonable measures to verify the identity of the beneficial owner(s), using relevant information or data obtained from reliable sources;

9.2.4. in the case of a customer who is a trust, to ensure that trustees or persons holding equivalent positions in similar legal arrangements disclose their status or function in the legal arrangement when establishing business relations.

9.2.5. understand and, where relevant, obtain information on the purpose of opening an account and the intended nature of the business relationship; and

9.2.6. maintain an updated and current database of designated persons and entities listed in global and local sanctions lists to enable it to detect suspected financing of terrorism and proliferators, including but not limited to:

(a) the United Nations Security Council Consolidated List;

(b) Malaysia's Ministry of Home Affairs List (and equivalent lists specific to relevant jurisdictions);

(c) other applicable sanctions lists, such as:

(i) The Office of Foreign Assets Control (OFAC) List (United States);

(ii) The European Union Sanctions List;

(iii) The United Kingdom Sanctions List (administered by the Office of Financial Sanctions Implementation);

(iv) relevant regional or national sanctions lists in jurisdictions where the organisation operates; and

(d) where necessary, performing appropriate background checks, where practical and relevant, on the names of individuals or entities of customers to ensure that transactions are not entered with those listed on the sanction lists above.

9.3. If there is any name match pursuant to Paragraph 9.2.6 above, reasonable and appropriate measures must be taken to verify and confirm the identity of its customer. Upon such confirmation, the following steps must be taken immediately:

9.3.1. reject the customer, if the transaction has not commenced; and

9.3.2. notify the SC.

10. SUSPICIOUS TRANSACTION REPORTING

10.1. If any suspicious money laundering or financing of terrorism activities are detected or any attempted transaction fits the list of "Red Flags" as in the table below, these transactions must be reported to the Chairman of ARMC immediately via an written report.

10.2. Examples of "Red Flags" – Possible Suspicious Transactions:

10.2.1. reluctance to provide detailed information of the source of income;

10.2.2. large cash transaction with no history of prior business experience;

10.2.3. shielding the identity of the beneficial owners;

10.2.4. the transaction appears illegal or is not economically justified considering the customer's business or profession;

10.2.5. repayment of loan instalments with multiple cash transactions;

10.2.6. early settlement of loan by multiple transferring of funds from third party or foreign bank accounts; and

10.2.7. multiple cash repayments that were structured below the reporting requirements to avoid detection.

10.3. Upon receiving the written report as stated in Paragraph 10.1 above, the Chairman of ARMC shall evaluate the grounds for suspicion within 5 working days and if suspicion is confirmed, the Chairman of ARMC shall submit a suspicious transaction report to the Financial Intelligence and Enforcement Department in Bank Negara Malaysia and notify the SC within the next working day through any of the following modes:

Contact Details

No.	Mode	To Whom
1	**Mail**	The physical forms should be placed in a sealed envelope and addressed to the following: The Director, Financial Intelligence and Enforcement Department (FIED) Bank Negara Malaysia Jalan Dato' Onn 50480 Kuala Lumpur (To be opened by addressee only)
3	**E-mail**	str@bnm.gov.my
4	**Others (where and if available)**	FIED's Financial Intelligence System (FINS 2.0) (https://fins.bnm.gov.my)

Contact Points

Securities Commission Malaysia **Executive Director** Surveillance, Authorisation and Supervision Securities Commission Malaysia, 3 Persiaran Bukit Kiara, Bukit Kiara, 50490 Kuala Lumpur **Tel:** 03-6204 8000 **Website:** www.sc.com.my

11. TRAINING & COMMUNICATIONS

11.1. Further information on AML/CFT/CPF can be obtained from Bank Negara Malaysia's website at http://amlcft.bnm.gov.my/index.html.

11.2. In addition, KJTS Reporting Entities are responsible for providing adequate training to its employees to ensure compliance to the requirements of the **AMLA 2001** and **AML/CFT/CPF Guidelines**.

12. RECORDS KEEPING AND RETENTION OF RECORDS

12.1. KJTS Reporting Entities must keep record of all transactions and ensure that they are up to date and relevant. The records must at least include the following information for each transaction:

12.1.1. documents relating to the identification of the customer in whose name the account is opened or transaction is executed;

12.1.2. the identification of the beneficial owner or the person on whose behalf the account is opened or transaction is executed;

12.1.3. records of the relevant account pertaining to the transaction executed;

12.1.4. the type and details of transaction involved;

12.1.5. the origin and the destination of the funds, where applicable; and

12.1.6. any other information as required by the authorities.

12.2. KJTS Group are generally required to retain, for at least seven (7) years, the records of transactions, relevant customer due diligence information and other relevant records including agreements, financial accounts, business correspondences and documents relating to the transactions in a form that is admissible as evidence in court and make such documents available to authorities and law enforcement agencies in a timely manner.

13. RESPONSIBILITY FOR THE POLICY

13.1. This Policy is reviewed and approved by the board of directors and the Chairman of ARMC. The accountability and oversight for establishing this Policy has been delegated to the Chairman of ARMC, which monitors the effectiveness of implementation of this Policy.

13.2. The board of directors sets the tone at the top, providing leadership and support for the Policy. While KJTS Group is not currently subject to the reporting obligations under the AMLA 2001, the Board takes ultimate responsibility for the supervision, monitoring, and ensuring adherence to ethical business practices and compliance with internal policies designed to mitigate potential money laundering, terrorism financing, and proliferation financing risks.

13.3. The board of directors shall ensure regular independent audits to assess the effectiveness of the internal AML/CFT/CPF policies and procedures, which are tailored to the company's business activities. Any findings and any necessary corrective measures to be undertaken must be tabled to the board of directors.

13.4. The Chairman of ARMC must have necessary knowledge, expertise and the required authority to discharge his/her responsibilities effectively, including knowledge on the relevant laws and regulations and the latest AML/CFT/CPF developments.

13.5. KJTS Reporting Entities are to nominate and appoint Chairman of ARMC who will be responsible for compliance of the AML/CFT/CPF internal programmes, policies and procedures.

14. POLICY VIOLATION

14.1. Violation of this policy will lead to disciplinary action including dismissal and possible criminal proceedings under applicable law.