TSA GROUP BERHAD
[Registration No. 202201010003 (1455700-A)]
(Incorporated in Malaysia)

ANTI-MONEY LAUNDERING AND COUNTERING FINANCING OF TERRORISM STANDARD OPERATING PROCEDURES

REVISION HISTORY

Version	Effective Date
1	3 November 2022

IMPLEMENTATION DATE

Version	Effective Date
1	23 November 2022

1.0 INTRODUCTION

1.1 TSA Group Berhad ("TSA" or "the Company") and its subsidiary companies (collectively known as "TSA Group" or "the Group") is committed to complying with Anti-Money Laundering, Anti-Terrorism Financing and Proceeds of Unlawful Activities Act 2001 ("AMLATFA 2001") and its related regulations, especially in relation to prevention and detection of money laundering and terrorist financing activities. The Company's commitment is demonstrated through this Anti-Money Laundering and Countering Financing of Terrorism ("AML/CFT") Standard Operating Procedures ("SOP").

1.2 This SOP serves as a guiding framework in providing relevant stakeholders an overview of the organisation's approach towards AML/CFT governance.

1.3 This SOP is in line with the following legislations and standards:

- Anti-Money Laundering, Anti-Terrorism Financing and Proceeds of Unlawful Activities Act 2001 ("AMLATFA 2001");
- Company Act 2016;
- Strategic Trade Act 2010 ("STA");
- Strategic Trade (Restricted End-Users and Prohibited End-Users) Order 2010;
- Financial Services Act 2013 ("FSA");
- United Nations Security Council Resolutions ("UNSCR");
- Applicable international standards and guidelines issued by the Financial Action Task Force on Money Laundering ("FATF"); and
- Anti-Money Laundering, Countering Financing of Terrorism and Targeted Financial Sanctions for Designated Non-Financial Businesses and Professions ("DNFBPs") & Non-Bank Financial Institutions ("NBFIs") issued by Bank Negara Malaysia ("BNM") ("AML/CFT and TFS for DNFBPs and NBFIs").

2.0 SCOPE & APPLICATION

2.1 Section 19(1) of AMLATFA 2001 provided that reporting institution who carries out the specified activities are required to adopt, develop and implement programmes, policies, procedures and controls in relation to anti-money laundering and countering financing of terrorism. The following are the specified activities:

- Non-bank Financial Institutions
- Moneylenders
- Pawnbrokers
- Trust Companies
- Dealers in Precious Metals or Precious Stones ("DPMS")
- Lawyers
- Accountants
- Company Secretaries
- Registered Estate Agents

Paragraph 11.1 of AML/CFT and TFS for DNFBPs and NBFIs allows application of simplification or exemption of Compliance programme requirement in the event where definition and criteria of a small-sized reporting institution are satisfied. Sector of the specified activities and the criteria of small-sized reporting institutions are provided overleaf.

Sector		Criteria
• Non-bank Financial Institutions • Moneylenders • Pawnbrokers • Trust Companies		• Total annual sales turnover of less than RM 3 million; AND • Total number of employees less than 30.
• Dealers in Precious Metals or Precious Stones ("DPMS")	• Companies or businesses carrying on retail business	• Total annual sales turnover of less than RM 10 million; AND • Total number of employees less than 30.
	• Companies or businesses carrying on wholesale business, i.e. business to business dealings only	• All such businesses are subject to the exemptions and simplification of AML/CFT Compliance Programme.
• Lawyers • Accountants		• Number of practising certificate holders of 5 and below
• Company Secretaries		• 5 members and below of a body prescribed by the Minister under section 235(2)(a) of Companies Act 2016; or • 5 persons and below licensed as company secretary by the Companies Commission of Malaysia; or • 5 persons and below with any combination of the above.
• Registered Estate Agents		• Total annual fees of less than RM 3 million

2.2 In view of the requirement above and as part of TSA's commitment in fulfilling its obligations, this SOP is specifically formulated based on the requirement in relation to DPMS to guide the following key stakeholders:

- Board of Directors ("the Board") of TSA;
- Employee of the Company; and
- Business partners, suppliers, contractors, consultants, agent, representatives, associates, clients and any other party engaging in transaction or performing work or services for or on behalf of the Company.

The standards set out in this SOP shall serves as the minimum requirement and should be strictly adhered to, when DPMS activities are undertaken by TSA Group.

2.3 This SOP outlines the general framework in managing and preventing the risks of TSA's daily business activities from being used as a channel for money laundering and terrorism financing activities. In view of the evolving money laundering and terrorism financing risks, the Company have proposed that areas of higher risk are subject to enhanced controls, while areas of low risk are accorded some policy accommodation so as to ensure the appropriate focus is preserved.

2.4 In ensuring compliance is maintained at all times, this SOP is circulated to all officers and personnel of the Group. The SOP is posted on TSA's corporate website for external stakeholders' reference.

3.0 DEFINITION

3.1 Money Laundering

(a) In general terms, money laundering 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.

(b) Pursuant to Section 4 of AMLAFTA 2001, money laundering means the act of a person who:
- Engages, directly or indirectly, in a transaction that involves proceeds of any unlawful activity;
- Acquires, requires, possesses, disguises, transfers, converts, exchanges, carries, disposes, uses, removes from or brings into Malaysia proceeds of any unlawful activity; or
- 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 any unlawful activity.

(c) Money laundering is distinguished into 3 stages, during which there may be numerous transactions that could alert a business unit to the money laundering activities. These stages are:
- **Placement**: Physical disposal of proceeds derived from unlawful activities;
- **Layering**: Separation of the illegal proceeds/ benefits of unlawful activities from their sources through transactions that disguise the audit trail and provide anonymity; and
- **Integration**: Integrating the laundered proceeds into financial system as legitimate funds.

3.2 Financing of Terrorism

(a) Financing of terrorism generally refers to performing transactions involving funds or properties that may or may not be owned by terrorist, or that have been, or are intended to be, used to assist the commission of terrorism.

(b) Pursuant to Section 3 (1) of AMLAFTA 2001, "terrorism financing offence" means any offence under Section 130N, 130O, 130P or 130Q of the Penal Code, which essentially includes:
- Providing or collecting property for terrorist acts;
- Providing services for terrorism purposes;
- Arranging for retention or control of terrorist property; or
- Dealing with terrorist property.

3.3 "Reporting Institution" refers to any person, including branches and subsidiaries outside Malaysia of that person, who carries on any activity listed in the First Schedule of AMLAFTA 2001.

3.4 "UNSCR List" refers to names and particulars of persons as designated by the United Nations Security ("UNSC") or its relevant Sanctions Committee to the relevant UNSCR and deemed as specified entities by virtue of Section 66C (2) of the AMLAFTA 2001.

3.5 "Domestic List" refers to names and particulars of specified entities as declared by the Minister of Home Affairs under the relevant subsidiary legislation made under Section 66B (10) of the AMLAFTA 2001.

3.6 Politically Exposed Person ("PEP") is an individual who is or who has been entrusted with prominent public function.

4.0 AML/CFT COMPLIANCE PROGRAMME

4.1 Policies, Procedures and Controls

(a) The Board and Senior Management are aware of the risk of money laundering and terrorism financing associated with TSA's business products and services, and understand the AML/CFT measures required by applicable laws, regulation and industry best practices as well as the importance of implementing AML/CFT measures to prohibit abuse by money launderers and financiers of terrorism.

(b) Relevant roles and responsibilities of the Board with regards to AML/CFT are as follows:
- Maintain adequate oversight over overall AML/CFT measures undertaken by the Company and ensure the Company's SOP is kept up-to-date to meet the relevant regulatory requirements;
- Implement effective internal controls over activities relating to AML/CFT;

- Ensure the Company has, at minimum, policies and procedures on AML/CFT;
- Set minimum standards and approve policies regarding AML/CFT measures within the Company, including those required for customer due diligence, record-keeping, on-going monitoring, reporting of suspicious transactions and combating financing of terrorism;
- Assess the implementation of approved AML/CFT policies through regular reviews and audits;
- Define the lines of authority and responsibilities for implementing AML/CFT measures and ensure there is a separation of duty between the implementation of such policies and procedures and the oversight and enforcement of such implementation; and
- Review and assess AML/CFT policies and procedures in line with changes and developments in the Company's products and services, technology as well as trends in money laundering and financing of terrorism activities.

(c) Relevant roles and responsibilities of Senior Management with regards to AML/CFT are as follows:
- Ensure material and pertinent information is updated to the Board on a timely basis;
- Ensure internal controls are in place and are implemented effectively, including the mechanism to monitor and detect complex and unusual transactions;
- Assist the Board in formulating appropriate AML/CFT policies and ensure such policies address the risks associated with ineffective AML/CFT measures in view of its business nature, complexity and volume of transactions undertaken;
- Ensure the AML/CFT procedures formulated are practical and can be implemented effectively;
- Implement the necessary changes to the AML/CFT policies and procedures with approval from the Board to ensure the current policies and procedures are appropriate, sound and pragmatic; and
- Ensure the integrity of employees are preserved at all times including implementing an appropriate employee assessment system to screen employees, evaluating employee's personal information (including criminal records, employment and financial history) as well as their independence and determining potential conflict of interest position arising, if any.
- Ensure adequate AML/CFT training is provided to employees, including raising employees' awareness of their AML/CFT obligations.

4.2 Employee Training and Awareness Programmes

(a) Awareness and training programmes on AML/CFT should be undertaken by the Company for all employees. The training conducted for employees must be appropriate for their level of responsibilities and should be able to facilitate the detection of money laundering and terrorism financing activities as well as the risk of other associated activities identified by the Company.

(b) The Company should ensure that proper channel of communication is in place to effectively communicate AML/CFT policies and procedures to all levels of employees.

(c) AML/CFT measures includes policies and procedures, control mechanism, actions and reporting channels that must be made available to employees and such measures should be in line with the relevant guidelines on AML/CFT issued by BNM and the Company's AML/CFT SOP.

(d) The scope of training should include the following:
- General background on money laundering and financing of terrorism in the country and the region;
- Latest AML/CFT developments and activities such as transaction modes and schemes;
- Risk profiles and risk assessment;
- Requirements and obligations to detect, monitor and report suspicious transactions;
- Methods and protocols for customer due diligence;
- Procedures for escalating and addressing AML/CFT matters and issues;
- Consequences for non-compliance with AML/CFT requirements and obligations; and
- Record keeping and retention.

(e) Awareness and training programme with special emphasis should be conducted for employees who are exposed to higher risk of encountering potential money laundering and financing terrorism transactions or activities, for example, employees who deal directly with customers.

(f) All awareness and training programmes conducted must be recorded, including details of date, duration, attendance and nature of training given. Such records should be kept for a period of at least 6 years.

4.3 Independent Audit

(a) The Board is responsible for ensuring regular independent audits are conducted on TSA's internal AML/CFT processes and controls with a view to determine their adequacy and effectiveness in complying with the AMLAFTA 2001, the relevant guidelines on AML/CFT issued by BNM as well as other applicable laws and regulations.

(b) The Company may engage audit function that are in-house or external professional services firm to conduct the independent audits required. However, such audit should not be carried out by the Company's compliance function or officer.

(c) Scope of the independent audit may include the following:
- Policies, procedures, controls, resources and system for complying with relevant AML/CFT regulations and obligations;
- Reliability, integrity and timeliness of the internal and regulatory reporting and management of information systems; and
- Current measures and protocols necessary in view of the latest developments in the operating environment and changes to the relevant AML/CFT requirements.

(d) A written audit report on the audit findings may be submitted to the Board so that necessary action can be taken to rectify any deficiencies or inadequacies found.

5.0 FOREIGN BRANCHES AND SUBSIDIARIES

The Company should ensure its foreign branches and subsidiaries apply AML/CFT measures in a manner that is consistent with the AML/CFT requirements in Malaysia and also, to extent that host country laws and regulations permit.

6.0 CUSTOMER DUE DILIGENCE

6.1 The Company is required to conduct due diligence ("CDD") on its customers and persons conducting transaction when:
- establishing new business relations;
- Carrying out cash transactions involving an amount equivalent to RM50,000 and above, including in situations where the transaction is carried out in a single transaction or through several transactions in a day that appear to be linked;
- they have any suspicion of money laundering or terrorism financing activities, regardless of the amount transacted; and
- they have any doubt about the adequacy or authenticity of previously obtained information.

Due diligence assessment is to be conducted in accordance with requirement set forth in the Anti-Bribery and Anti-Corruption Compliance and Monitoring Framework.

6.2 Senior Management must ensure that satisfactory evidence is obtained for CDD and proper records are retained. Such evidence must be substantiated by reliable and independent source documents.

6.3 CDD undertaken by the Company should at a minimum include the following protocols:

- Identify the customer and verify customer's identity against reliable, independent source documents, data or information;
- Verify that any person acting on behalf of a customer is so authorised, and identify and verify the identity of that person;
- Identify and verify beneficial ownership and control over such transaction;
- Understand and obtain information on the purpose and intended nature of the business relationship/ transaction; and
- Carry out scrutiny with due care to ensure the information provided is updated, relevant and valid.

6.4 Customer who is unwilling to provide information requested or to cooperate with TSA's CDD process may itself be a factor of suspicion. Any suspicious transaction detected should be reported to Senior Management as well as to the Board.

6.5 Customers can be categorised into individual customer, corporate customer as well as clubs, societies and charities. The information and documents required for each type of CDD are set out in the table below:

Type of Customer	Information Required	Documents Required
Individual Customer (Including Resident and Non-Resident)	• Full name; • National registration identity card ("NRIC") number/ passport number; • Residential and mailing address; • Date of birth; • Nationality; • Occupation; • Name of employer or nature of self-employment or nature of business; • Contact number; and • Purpose of transaction.	• NRIC for Malaysian/ permanent residents; or • Passport for foreigners.
Corporate Customer	• Company name; • Company registration number; • Background of the company; • Mailing address of the company • Nature of business; and • Key contact person/ representative and contact number.	• Memorandum/ Article/ Certificate of Incorporation/ Partnership; • Identification document of transacting representative/ director/ shareholder; • Authorisation for any person to represent the company; and • Identification document of the person authorised to represent the company in its dealing with the TSA.

Type of Customer	Information Required	Documents Required
Clubs, Societies and Charities	• Name of clubs, societies or charities; • Mailing address of clubs, societies or charities; • Nature of clubs, societies or charities; • Key contact person/ representative and contact number.	• Certificate of registration; • Identification document of transacting representative/ office bearer; • Authorisation for any person to represent the clubs, societies or charities; and • Other relevant documents.

6.6 Upon obtaining the required information and documents, approval from Senior Management is required prior to entering into any business transaction or establishing any business relationship with the customer.

6.7 In enhancing the CDD measures and to mitigate the money laundering and terrorism financing risks, the following actions are to be undertaken:

- Obtaining additional information on the nature of the business relationship and the intended value of transaction;
- Where relevant, obtain additional information on the beneficial owner of the transacting company (e.g. occupation, volume of assets, information available through public databases);
- Inquire the reason for the intended transactions; and
- Require the first payment to be carried out through an account in the customer's name with a bank that is subjected to similar CDD measures to ensure the validity and traceability of customer's bank account.

6.8 For any business relationship and transaction with any person from higher risk countries, counter measures to be introduced may include the following as required by FATF:

- Limiting the business relationship or financial transaction with the identified person or persons located in the country concerned;
- Review and amend, or if necessary, terminate corresponding business relationships with related company/ financial institutions in the country concerned, where necessary; or
- Conduct enhanced reviews and audits on the identified person's background.

6.9 In addition, credit assessment may be required to be carried out to examine customer's ability in making payment <u>if credit is requested by a customer</u>. The following steps should be taken in conducting credit assessment:

(a) The Company is to conduct background checks (i.e. company profile, nature of business, financial positions, personal feedback) as customer evaluation

for every new customer, similarly as CDD protocols. Credit Application Form shall be completed by customer and sent back to TSA. The completed Credit Application Form and relevant supporting documents from the background checks is to be submitted to Senior Management for review and approval.

(b) Ensure that the customer has no conflict of interest against the Company. Conflict of interest declaration is to be conducted in accordance with requirement set forth in the Anti-Bribery and Anti-Corruption Compliance and Monitoring Framework.

(c) Credit limits and credit terms of each customer are to be approved by the Company's authorised personnel. For revision in credit limits of existing customers, the credit limits will be based on the initial credit assessment and volume of trade undertaken to date.

(d) Periodic review on customers' payment performances and sales volume should be conducted and documented on a yearly basis to identify if there is a need to amend the credit terms or credit limits assigned.

6.10 TSA should conduct on-going CDD throughout its business relationship with customer in ensuring continuous application of TSA's AML/CFT compliance programme.

6.11 Considerations of on-going CDD that should be undertaken by TSA comprises the following:

- Scrutinise transactions undertaken throughout the course of the relationship; and
- Ensure documents, data or information collected under the CDD process are kept up-to-date and relevant, by undertaking reviews of existing records particularly for higher risk customers.

6.12 The frequency in implementing on-going due diligence should commensurate with the level of money laundering and terrorism of financing risks posed by the customer based on the risk profiles, nature, value of transaction and the customer's country of origin.

7.0 CUSTOMER ACCEPTANCE

7.1 Prior to accepting a customer the following information are to be considered in determining the level of money laundering and terrorism of financing risk posed:

- Results of CDD;
- Results of enhanced CDD (where applicable);
- Results of credit assessment on customers; and
- Risk appetite of TSA

7.2 Upon considering the above information, Senior Management shall make appropriate decision, especially in respect of whether to accept the customer for any business engagement.

7.3 Subsequent to the acceptance of a customer, TSA shall continuously monitor the new customer's transaction activity and engagement pattern with a view to detect any abnormal transactional pattern or behaviour.

8.0 USE OF INTERMEDIARY & AGENT

8.1 During the normal course of business, the Company may engage the services of intermediary or agent in order to secure new customer or business. In this regard, TSA is required to examine the potential money laundering and terrorism financing risk posed in the engagement of intermediary or agent.

8.2 Money laundering and terrorism financing risk may occur through two (2) primary money laundering techniques as follow:

- Trade-based money laundering where criminals utilise cross-border transactions to obscure the source or destination of funds; and
- Third party payments where money is given to or received from an entity other than the intermediary or agent in order to transfer funds without utilising traditional banking routes, which may be subjected to tighter financial controls.

8.3 The Company is to conduct appropriate AML/CFT due diligence prior to engaging any intermediary or agent so as to ensure they are not involved in money laundering and terrorism financing activities. Due diligence assessment is to be conducted in accordance with requirement set forth in the Anti-Bribery and Anti-Corruption Compliance and Monitoring Framework.

8.4 The following considerations are to be taken into account when carrying out AML/CFT due diligence on intermediary or agent:

- Background of the intermediary or agent;
- Financial positions of the intermediary or agent;
- Verification against Ministry of Home Affairs ("MOHA"), United Nations Security Council Resolutions ("UNSCR") (Terrorism) as well as UNSCR (Proliferation of Weapons of Mass Destruction);
- Origin and location of operations of the intermediary or agent;
- Whether the intermediary or agent has conflict of interest against the Company; and
- Whether the intermediary or agent is a PEP.

8.5 Senior Management is to review the outcome of such considerations and decide whether to accept and approve the engagement of the intermediary or agent.

8.6 In order to facilitate effective oversight, the relationship between the Company and its intermediary or agent should be governed by an agreement/contract that clearly specifies the rights, responsibilities and expectations of parties involved. At the minimum, TSA must be satisfied that the intermediary or agent:

- Has adequate customer due diligence process;
- Has reliable mechanism to verify a customer's identity;
- Able to provide customer due diligence information and make copies of the relevant documentation available to TSA immediately upon request; and
- Where appropriate, the intermediary or agent is properly regulated and supervised by the respective authorities.

9.0 RECRUITMENT

9.1 An employee AML/CFT evaluation is to be carried out in the recruitment process to screen employee's background in order to identify and minimise the Company's exposure to the risk of engaging personnel with any history of involvement in money laundering and terrorism financing.

9.2 The Company is responsible to screen and re-screen any employee whose roles are able to facilitate money laundering and terrorism financing activities. This includes:

- History of the employees;
- Financial standing;
- Behavioural patterns; and
- Employment track record.

9.3 Such evaluation includes identifying and verifying employees' identities, checking whether the employees have criminal record, past involvement in money laundering and terrorism financing activities and country of origin (high-risk countries), including scrutinising their employment history and deciding whether they are suitable for such position and whether they will pose a risk to the Company subsequently.

9.4 Mandatory background check is to be conducted to ensure the employee is free from any involvement in money laundering and terrorism financing activities. Such background check comprises the following:

- Police check;
- Screen the employee's name against MOHA, UNSCR (Terrorism) as well as UNSCR (Proliferation of Weapons of Mass Destruction);
- Conflict of interest declaration; and
- PEP screening.

9.5 Results of the employee's AML/CFT evaluation and background checks conducted should be reviewed and approved by Senior Management on recruitment.

9.6 Upon recruitment, TSA is to provide the appropriate AML/CFT awareness or induction training to the new employee.

10.0 MATERIAL ASSET ACQUISITION

10.1 TSA is to conduct due diligence prior to acquiring any material asset. Such due diligence should be conducted on the following:

- Background of vendor;
- Origins and history of asset;
- Terms and conditions of transactions;
- Cross border risks; and
- Other considerations

10.2 Acquiring a material asset is generally considered as a capital expenditure ("CAPEX") which may include the following:

- Land and building;
- Office Renovation;
- Motor vehicle;
- Furniture and fitting;
- Office equipment; and
- Computer hardware and software.

10.3 TSA may purchase a new or used asset. Prior to purchasing a new asset, the Company is to identify the origins of the asset, check on manufacturer's background (to determine involvement in money laundering and terrorism financing activities) and to assess the terms of trade. Due diligence assessment is to be conducted in accordance with requirement set forth in the Anti-Bribery and Anti-Corruption Compliance and Monitoring Framework.

10.4 Where the asset to be acquired is an used asset, TSA is to examine the history of such asset, scrutinize its past owners, source of funds of previous owners as well as ascertain the reason for its disposal.

10.5 Upon obtaining the relevant information required, Head of Department is to determine if the asset purchase is free of any money laundering and terrorism financing risk or association before allowing the proposed acquisition to be presented to Senior Management for review and approval.

11.0 CASH THRESHOLD REPORT

11.1 Cash transactions refer to transactions involving physical currencies (i.e. domestic or foreign currency) and bearer negotiable instruments such as travelers' cheques and cash cheques but excludes bank drafts, cheques and electronic transfers. Such transactions are also included withdrawal of cash from accounts or exchange of bearer negotiable instruments for cash.

11.2 The cash threshold report shall be submitted to Senior Management.

11.3 The cash threshold reports are applicable to customers and person carrying out transaction in single or multiple cash transactions within the same account in a day for the amount equivalent to RM25,000 and above.

11.4 The Company should ensure that any cash transaction must NOT be offset against one another. Where there are deposit and withdrawal transactions, the amount must be aggregated and should NOT be offset.

12.0 SUSPICIOUS TRANSACTION REPORT

12.1 TSA has established a reporting mechanism to promptly submit every suspicious transaction report which fits the Company's description of "red flags" to the Senior Management, whenever the employee suspects or has reasonable grounds to suspect that the transaction or attempted transaction involves proceeds from an unlawful activity or the customer is involved in money laundering or financing of terrorism activities.

12.2 The Company must consider submitting a suspicious transaction report when any of the customer's transactions or attempted transactions fits the Company's description of "red flags".

12.3 Example of "red flags" defined are listed below:

- Reluctance to provide detailed information on the source of income;
- Repayment of loan instalments with multiple cash transactions;
- Large cash transaction with no history of prior business experience;
- Early settlement of loan through multiple fund transfers from third party or foreign bank accounts;
- Multiple cash repayments that were structured below the reporting requirements to avoid detection;
- Shielding the identity of beneficial owners;
- Transaction appears illegal or is not economically justified considering the customer's business or profession; and
- Etc.

12.4 Reporting Mechanism

(a) All internal suspicious transaction reports received from employees must be channelled directly to the Senior Management.

(b) Upon receiving any internal suspicious transaction report, Senior Management should evaluate the grounds for suspicion. If the suspicion is confirmed, the suspicious transaction report may be submitted to the Financial Intelligence Unit in Bank Negara Malaysia ("BNM"). In cases where Senior Management decides that there are no reasonable grounds for suspicion, the decision made should be documented and ensure that it is supported by the relevant documents filed.

(c) Senior Management may submit suspicious transaction report to Financial Intelligence Unit in BNM through any of the following:

No.	Mode	To Whom
1.	Mail	The Director, Financial Intelligence Unit Bank Negara Malaysia

		Jalan Dato' Onn 50480 Kuala Lumpur (To be opened by addressee only)
2.	Fax	+603-2691 6108
3.	E-mail	str@bnm.gov.my
4.	Online	https://bnmapp.bnm.gov.my/fins2

(d) Senior Management must ensure that in the course of submitting such report utmost care is undertaken to ensure it is treated with highest level of confidentiality.

(e) The Company should ensure that the Senior Management is authorised to cooperate with Financial Intelligence Unit in BNM providing additional information and documentation as and when requested, and to respond promptly to any further enquiries with regards to the suspicious transaction report submitted. Moreover, TSA also should ensure the suspicious transaction reporting protocols are operated in a secured environment to maintain confidentiality and preservation of secrecy.

13.0 RECORD KEEPING

13.1 TSA should keep the relevant records including any financial accounts, files, agreements, business correspondence and documents relating to transactions, especially those obtained during CDD process. Such relevant records must be retained, for at least six (6) years, in a form that is admissible as evidence in court pursuant to the Evidence Act 1950, and ensure such records are available to the competent authority or supervisory authorities and law enforcement agencies on a timely manner.

13.2 The Company should ensure the records are up to date and at least include the following information for each transaction:

- Document relating to the identification of the customer in whose name the account is opened or transaction is executed;
- The identification of the beneficial owner or the person on whose behalf the account is opened or transaction is executed;
- Records of the relevant account with regards to the transaction executed;
- The type and details of transaction involved;
- The origin and the destination of the funds, where applicable; and
- Any other information as required by the authorities.

13.3 In situation where the records are subjected to on-going investigation or prosecution in court, such records shall be retained beyond the stipulated retention period until the Company is informed by the relevant law enforcement agency that such records are no longer required.

14.0 MANAGEMENT INFORMATION SYSTEM

14.1 Adequate manual or electronic management information system ("MIS") to complement TSA's CDD process must be in place. The MIS must commensurate with the size, nature and complexity of the Company's operations and money laundering and terrorism financing risks profile.

14.2 The MIS shall provide timely information on a regular basis so as to enable the Company to detect irregularities and/ or any suspicious activity. Such information provided should include, at minimum, information on multiple transactions over a certain period, large transactions, anomalies in transaction patterns, customer's risk profile and transactions exceeding any internally specified thresholds.

14.3 The MIS should be part of the Company's information system that contains its customer's normal transaction/ business profile, which is accurate, updated and reliable.

15.0 COMBATING THE FINANCING OF TERRORISM

15.1 TSA should ensure that the existing suspicious transaction reporting system and mechanism for identification of suspicious transactions are extended to consider terrorism financing.

15.2 In line with the UNSCR, TSA is required to adhere to and implement sanctions imposed on designated countries and persons to combat terrorism, terrorism financing, proliferation of weapons of mass destruction and financing of other forms of armed conflicts or violence against humanity.

15.3 A sanctions database on the UNSCR List is required to be maintained by the Company and ensure it is updated and effected without delay upon publication of the United National Sanction Committee ("UNSC") and its relevant Sanctions Committee's designation in the United Nation ("UN") website. The Company may obtain the Consolidated UNSCR List published on the following UN website - "https://www.un.org"

15.4 Domestic List also should be updated on a timely manner by the Company and ensure the sanction database on Domestic List is well maintained. Such Domestic List can be obtained from the following website - "http://www.federalgazette.agc.gov.my"

15.5 The Company should ensure that the information contained in the database are updated and relevant, and are easily accessible to employees for the purpose of identifying suspicious transaction.

15.6 Regular checking on the names of new and existing customers against the names in the database should be carried out. If there is any matching in name, the Company should take reasonable and appropriate measures to verify and confirm the customer's identity. If the customer's identity has a full match against the database, immediate action such as the following should be undertaken:

- Report to the Financial Intelligence Unit in BNM;
- Reject customer, if the transaction has not commenced; and
- Freese the customer's transaction, if it is an on-going customer.

Where the Company suspects that a transaction is terrorist-related, suspicious transaction report shall be made to the Financial Intelligence Unit in BNM.

16.0 RISK ASSESSMENT ON MONEY LAUNDERING AND TERRORIST FINANCING

16.1 TSA may take appropriate steps to identify, asses and understand its money laundering and terrorist financing risks at the company level, in relation to its customers, countries or geographical areas, products, services, transactions or delivery channels and other relevant risk factors.

16.2 In assessing money laundering and terrorist financing risks, the following processes shall in place:
- Documenting risk assessments and findings;
- Considering all relevant risk factors before determining the level of overall risk and the appropriate level and type of mitigation to be applied;
- Keeping the assessment up-to-dated through a periodic review; and
- Having appropriate mechanism to provide risk assessment information to the competent authority or supervisory authority.

16.3 The Company risk profiling on its customer and assign a money laundering and terrorist financing risk rating that is commensurate with its risk profile.

16.4 After the initial acceptance of the customer, TSA is to regularly review and update the customer's risk profile based on its level of money laundering and terrorist financing risks.

16.5 The risk assessment report which included money laundering and terrorist financing risk profile and the effectiveness of risk control and mitigation measures should be submitted to Senior Management and the Board for review. The frequency of reporting shall be commensurate with the level of risks involved and the Company's operating environment.

17.0 POLICY REVIEW

The SOP shall be reviewed by the Board at least once every 3 years. Any material changes required shall be proposed to the Board for approval so as to ensure the SOP's continued relevance and effectiveness pursuant to the Company's AML/CFT obligations and to comply with applicable laws, regulations and requirements.

18.0 EFFECTIVE DATE

This policy has been reviewed and approved by the Board for implementation on 3 November 2022.