LSK MANAGEMENT SERVICES SDN BHD
(640921-P)

AML / CFT POLICY
ANTI-MONEY LAUNDERING ("AML") AND COUNTER FINANCING OF TERRORISM ("CFT") POLICY

Version 1.0 (2020)

Compliance Department
LSK Management Services Sdn. Bhd.
Approved by Board of Directors
1 August 2020

TABLE OF CONTENTS

1. INTRODUCTION

1.1 It is the policy of **LSK Management Services Sdn. Bhd**. (hereinafter referred to as "**LSK**"), registration no. 200401002418 (640921-P), a company incorporated in Malaysia with its registered address at No. 9-6, Jalan USJ 9/5Q, Subang Business Centre, 47620 Subang Jaya, Selangor, Malaysia to prohibit and actively prevent money laundering and any activity that facilitates money laundering or the financing of terrorist or criminal activities.

1.2 The purpose of the AML/CFT Policy is to provide directives to employees and directors of **LSK** on anti-money laundering governance and reiterates **LSK's** commitment to full compliance to the AMLATFPUAA.

1.3 We will comply with all applicable requirements and regulations. Our AML/CFT policies, procedures and internal controls are designed to ensure compliance with all applicable regulations and will be reviewed and updated on a regular basis to ensure appropriate policies, procedures and internal controls are in place to account for both changes in regulations and changes in our business.

1.4 The Policy on Anti-Money Laundering and Counter Financing of Terrorism are issued pursuant to section 66E and section 83 of the Anti-Money Laundering, Anti-Terrorism Financing and Proceeds of Unlawful Act 2001 (AMLATFPUAA).

1.5 The Policy is drawn up in accordance with the AMLATFPUAA and the Financial Action Task Force on Money Laundering's (FATF) Forty Recommendations on Money Laundering and Nine Special Recommendations on Terrorist Financing.

1.6 In addition, the National ML/TF Risk Assessment (NRA) by the National Coordination Committee to Counter Money Laundering (NCC) that assesses and identifies the key threats and sectoral vulnerabilities that Malaysia's financial system and economy is exposed to, has guided the strategies and policies of Malaysia's overall AML/CFT regime. The NRA is the primary tool used for periodic assessment and tracking of effectiveness of the relevant Ministries, law enforcement agencies, supervisory authorities and reporting institutions in preventing and combating ML/TF and proliferation financing.

1.7 In line with the United Nations Security Council Resolutions (UNSCR), reporting institutions are also 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 proliferation financing as well as suppress other forms of armed conflicts or violence against humanity. These obligations have been further elaborated and clarified in accordance with the relevant UNSCR.

1.8 On 31 December 2019, BNM issued the Policy Document on Anti-Money Laundering (AML), Countering Financing of Terrorism (CFT) and Targeted Financial Sanctions (TFS) for Designated Non-Financial Businesses and Professions (DNFBPs) and Non-Bank Financial Institutions (NBFIs) ("2020 Policy Document"). The 2020 Policy Document came into force on 1 January 2020.

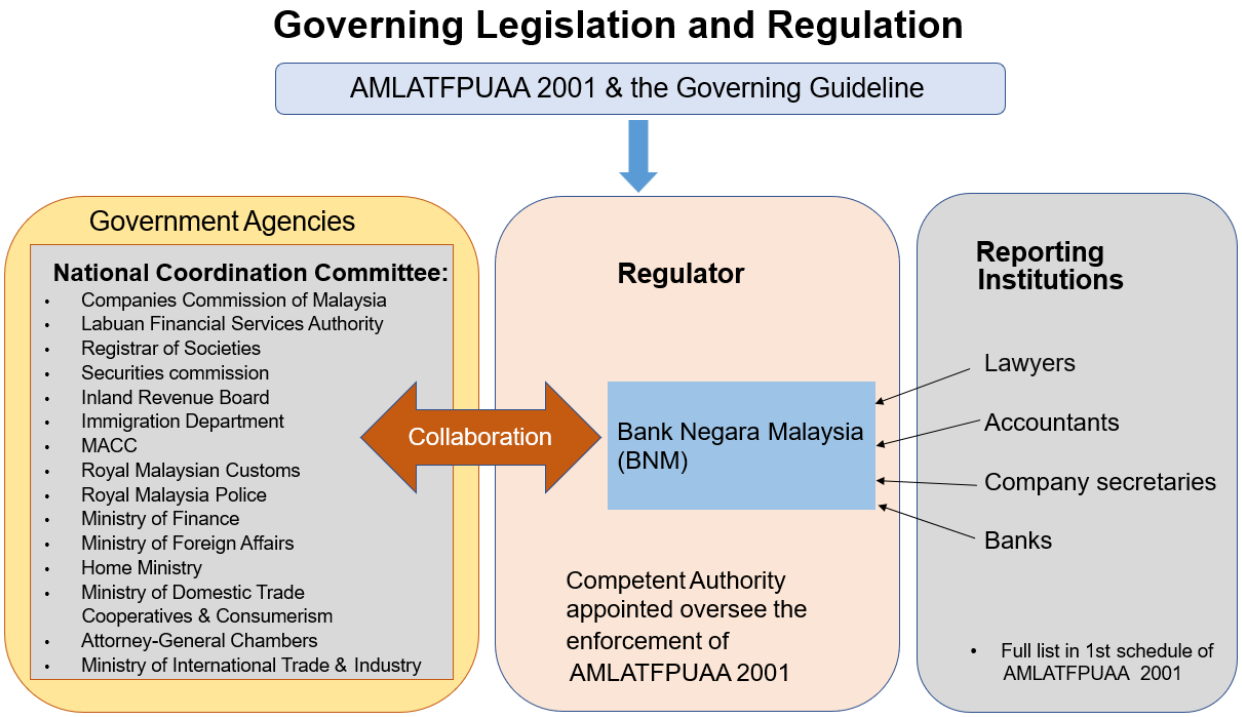
1.9 A reporting institution that is jointly regulated by Bank Negara Malaysia (BNM)

and the Company Secretaries (*persons prescribed by the Minister or licensed by the Registrar of Companies to act as a company secretary of a company pursuant to section 235 of the Companies Act 2016*), is required to comply with BNM Policy and Anti-Money Laundering (AML), Countering Financing of Terrorism (CFT) and Targeted Financial Sanctions (TFS) for Designated Non-Financial Businesses and Professions (DNFBPs) and Non-Bank Financial Institutions (NBFIs) issued by BNM. Where there are differing requirements between the said guidelines, the more stringent requirements shall apply.

1.10 Money laundering is the process of introducing money, property or other assets derived from illegal and criminal activities into the legal financial and business cycle to give it a legitimate appearance. It is a process to clean 'dirty' money in order to disguise its criminal origin. Money Laundering is an offence under the Anti-Money Laundering, Anti-Terrorism Financing and Proceeds of Unlawful Activities Act 2001 (AMLATFPUAA).

1.11 This AML/CFT Policy applies to all employees and directors of **LSK.** All employees at the company are required to strictly abiding by the policy. Any breach of this Policy will be a serious matter, may result in disciplinary action, including dismissal and could result in an employee becoming personally liable to criminal prosecution.

An electronic version of this Policy is available at www.lskmgnt.com.my.



2. SCOPE

2.1 The Policy establishes the general framework to manage and prevent the risks of **LSK**'s businesses from being used as a conduit for money laundering and terrorism financing activities. All **LSK** employees are required to adhere to the requirements of this Policy when carrying out their daily responsibilities.

2.2 The Guidelines applies to all **LSK**'s business units and the standards set out in these guidelines are the minimum requirements for businesses or entities in **LSK**.

3. DEFINITIONS

3.1 Money Laundering

3.1.1 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.

3.1.2 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 three basic stages are:

a) **Placement:** During placement, "dirty" money (generally in the form of cash) derived from criminal activities is placed in the financial system.; and

b) **Layering:** To conceal the illegal origin of the placed funds and thereby make them more useful to criminals, the funds must be moved, dispersed, and disguised. Layering is the process of disguising the source of the funds through layers of financial transactions.; and

c) **Integration:** Once the funds are layered and can no longer be traced back to their criminal origins, they are integrated into the financial system and now appear "clean" and available for use by criminals. If layering has been successful, integration places the laundered money back into the economy and financial system in such a way that they appear as clean and legitimate.

3.2 Terrorism Financing

3.2.1 Terrorist financing involves dealing with money or property that may be used for financing terrorist activities. The funds and property may be from either legitimate or criminal sources. They may be small amounts.

The methods used by terrorists to move money are substantially the same as those used by other criminals, such as the following:

Traditional financial institutions: Financial institutions are vulnerable to abuse by terrorists. Despite doing all that is required with respect to CDD, transactions related to the financing of terrorism may fail to set off any alarms or "red flags." For example, accounts can be opened, and small withdrawals and deposits which are less than any legal reporting requirements can be made.

Alternative remittance systems: Unregulated remittance systems such As *hawala* and *hundi*. These systems often have traditional roots or ethnic Ties and operate in places where the formal finance sector is less established; funds can be transferred without any documentation.

Cash couriers: Cash is smuggled across borders, for example through land crossings and sea shipments where borders are uncontrolled.

False invoicing: False trade invoicing provides a means to transfer money between jurisdictions by overstating the value of the goods or services for which payment is due.

High-value commodities: Commodities like gold and diamonds can also be used to transfer value across borders as both are easy to convert into cash.

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

- 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.

4. CUSTOMER ACCEPTANCE STANDARD

4.1 General

4.1.1 **LSK** are required to develop policy and procedures to address the establishment of business relationship with the customer. The objective is to address different risks posed by each type of customer through profiling.

4.1.2 **LSK** strongly objects to all practices related to money laundering, including dealing in the proceeds of criminal activities and terrorism financing. As a general rule, reasonable degree of due diligence must be carried out in order to understand the business and background of any prospective customer, vendor, third party or business partner that intends to do business with **LSK** to determine the origin and destination of money or assets involved. Any suspected activities relating to money laundering or terrorism financing should be reported immediately to Bank Negara Malaysia and relevant authorities.

4.1.3 **LSK** prohibits all involvement in money laundering activities and terrorism financing either directly or indirectly. The activities may include, but not limited to the following:

a) Payments made in currencies that differ from invoices;
b) Attempts to make payment in cash or cash equivalent (out of Normal business practice)
c) Payments made by third parties that are not parties to the contract; and
d) Payments to or from accounts of third parties that are not parties to the contract.

4.2 Risk Profiling

4.2.1 By implementing a reasonably designed risk-based approach, **LSK** identify the criteria to measure and mitigate potential money laundering and terrorist financing risks.

4.2.2 To assist the overall objective to prevent money laundering and terrorist financing through **LSK**, a risk-based approach; **LSK** determine the low risk clients, high risk clients, high risk products, service and transactions, all actions to be taken related this subject, and pursuance policy related with monitoring activities.

4.2.3 Risk factors to consider

- the origin of the customers and location of business, country on sanctions list (Geographical Location)
- background or profile of the customer, resident or non-resident, company structure, politically exposed persons (PEPs), High net worth individuals, customer from high risk countries
- nature of the customer's business (Product/Service)
- structure of ownership for a corporate customer
- delivery channels- non face to face
- any other information suggesting that the customer is of higher risk

The steps to be taken are as follows:
1. Identify the risks.
2. Assess the risks.
3. Design and put in place controls to manage and reduce risks.
4. Monitor and improve the effective operation of the risk-based controls.

4.2.4 Reflective of the risk profiling conducted, **LSK** should have reasonable measures in its internal policies and procedures, including customer due diligence, to address the different risks posed by each type of customer.

4.2.5 Following the initial acceptance of the customer, **LSK** should continuously monitor each customer's transaction activity pattern to ensure it is in line with the customer's profile. Unreasonable differences should prompt **LSK** to reassess the customer's risk profile.

4.2.6 For customer assessed at normal risk, continue business as usual and keep customer information up to date. For customer assessed at higher risk, need to conduct Enhanced Customer Due Diligence (ECDD), to ask for their source of funds/wealth and seek management prior to conduct business.

Determine the risk parameters for customer profiling:

Example 1 for all sectors:

Risk Factor	Examples	Formulated Parameters
Customer	Higher risk customer	• Number of higher risk customers more than 20% of total customer base for a year • Number of politically exposed person (PEP) customers who are high risk is more than 5% of total customers
	Local and foreign customers	• Percentage of local and foreign customer for a year
	Companies with nominee shareholders or shares in bearer form	• Percentage of such companies against total non-individual customer base
Transactions and Distribution Channels	Cash intensive or other forms of anonymous transactions	• High volume of cash transactions above RM50,000 within a year • High volume of anonymous/proxy transactions exceeding RM50,000 per transaction within a year
	Percentage of non-face-to-face transactions	• Non-face-to-face transactions exceeding 50% of total transactions
	Frequency and amount of cash payments	• Cash transactions above RM10,000
	Wide array of e-banking	• More than 30% of new accounts are opened via internet, mail or

	products and services	telephone without prior relationship
Findings of the NRA	Sectors identified as highly vulnerable to ML/TF risks	• Number of customers with occupation or nature of business from highly vulnerable sectors identified under the NRA

4.3 New Products and Business Practices

4.3.1 Reporting institutions are required to identify and assess the ML/TF risks that may arise in relation to the development of new products and business practices, including new delivery mechanisms and the use of new or developing technologies for both new and pre-existing products.

4.3.2 Reporting institutions are required to:

- undertake risk assessment prior to the launch or use of such products, practices and technologies; and
- take appropriate measures to manage and mitigate the risks.

5. KNOW YOUR CUSTOMER (KYC)- CUSTOMER DUE DELIGENCE (CDD)

5.1 General

Customer due diligence (CDD) at the point of establishing business relationship

5.1.1 The “Know Your Customer” (KYC) principle is instrumental in the prevention against money laundering and terrorist financing. Knowing ours customer is an essential element in our line of work. By obtaining information on the source of the funds transacted by customers, **LSK** can protect itself from being used to conceal illegally-obtained funds. **LSK** Due Diligence (in terms of requirements, acceptance level and how frequently information is reviewed) is connected to Customer Risk ratings.

5.1.2 Section 16 of the AMLATFPUAA among others clearly sets out customer identification requirements for reporting institutions. A reporting institution is expected to obtain satisfactory evidence of the identity and legal existence of the customer and beneficial owner at the point of establishing the business relationship.

5.1.3 **LSK** management is responsible to implement the appropriate CDD procedures relevant to the nature of their business transactions. **LSK** management should adopt a risk-based approach when deciding the degree of CDD to apply. Risks are assessed at the outset of a business relationship and updated regularly.

5.1.4 As a general principle, **LSK** are required to conduct customer due diligence (CDD) procedures when:

- at the start of a new business relationship;
- it has any suspicion of money laundering or terrorism financing activities regardless of the amount transacted;
- carrying out cash or occasional transaction that involves a sum in excess of the amount specified by Bank Negara Malaysia under its sectoral guidelines or relevant circular;
- it has any doubt about the adequacy or authenticity of previously obtained information.

The CDD procedures should minimally include:-

5.1.5 The customer due diligence undertaken by the reporting institution should at least comprise the following:

- identify and verify the customer (including foreign body corporate) and verify such customer's identity using reliable, independent source of documents, data or information;
- identify and verify beneficial ownership and control of such transaction;
- obtain information on the purpose and intended nature of the business relationship/transaction; and
- conduct on-going due diligence and scrutiny, to ensure the information provided is updated and relevant.
- understand and, where relevant, obtain information on the purpose of opening an account and the intended nature of the business relationship; and
- 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 maintained by *Ministry of Home Affairs (MOHA)* and *United Nations Security Council (UNSC)*.

5.1.6 Sanctions List Screening

The documentation and information provided by the customers will be verified and evaluated by the Compliance Officer. Customers who have one or several risk factors and those who the Compliance Officer considers to do so, will have to provide more documentation and information so that the Compliance Officer can decide whether or not to accept them as customers.

Before deciding about whether or not a customer should be accepted, and in order to comply with the customer acceptance policy stated in this section, the Compliance Officer will check all persons, natural or legal entities, using the watchlists. If a customer is found to be on one of the watchlists, all ties of that potential customer with The Company will be terminated and Compliance Officer will submit suspicious transaction report (STR) form to the Financial Intelligence Unit in Bank Negara Malaysia on the next working day. If any potential customer is included in the PEPs list, the Compliance Officer's approval will be necessary.

Screening **LSK** clients' names against the **MOHA** and **UNSCR Sanctions Lists for Terrorism, Proliferation and Other UN-Sanctions Regimes**

1) **MOHA: Ministry of Home Affairs**
http://www.moha.gov.my/index.php/en/maklumat-perkhidmatan/membanteras-pembiayaan-keganasan2/senarai-kementerian-dalam-negeri

2) **UNSCR: United Nations Security Council Resolutions (Terrorism)**
https://www.un.org/sc/suborg/en/sanctions/1267/aq_sanctions_list
https://www.un.org/sc/suborg/en/sanctions/1988/materials

3) **UNSCR: United Nations Security Council Resolutions (Proliferation of Weapons of Mass Destruction)**
https://www.un.org/sc/suborg/en/sanctions/1718/materials
https://www.un.org/en/sc/2231/list.shtml

4) **UNSCR: United Nations Security Council Resolutions (Other UN-Sanctions Regimes)**
htttps://www.un.org

5.1.7 Maintenance of Sanctions List

UNSCR List

- Reporting institutions are required to maintain a sanctions database on the UNSCR List.

- Reporting institutions must ensure that the information contained in the sanctions database is updated and effected without delay upon the publication of the UNSC or its relevant Sanctions Committee's designation in the UN website.

- Reporting institutions may refer to the Consolidated UNSCR List published in the following UN website:

  https://www.un.org

- The UNSCR List shall remain in the sanctions database until the delisting of the specified entities by the relevant Sanctions Committee is published in the UN website.

Domestic List

- Reporting institutions are required to keep updated with the Domestic List as and when published in the *Gazette.*

- Reporting institutions are required to maintain a sanctions database on the Domestic List.

- Reporting institutions must ensure that the information contained in the sanctions database is updated and effected without delay upon publication in the *Gazette.*

- Reporting institutions may refer to the Domestic List published in the following website:

  http://www.federalgazette.agc.gov.my

- The Domestic List shall remain in the sanctions database until the delisting of the specified entities is published in the *Gazette*.

5.1.8 Unwillingness of the customer to provide the information requested and to cooperate with the reporting institution's customer due diligence process may itself be a factor of suspicion.

5.1.9 In certain special circumstances where the risks of money laundering and financing of terrorism are low or where measures are already in place to effectively manage such risk, the reporting institution may allow its customer due diligence process to be

conducted not later than 14 days (or the period specified in the Sectoral Guidelines, where applicable) after the business relationship has been established to permit some flexibilities for its customer to furnish the relevant documents.

5.1.10 A customer who fails to provide evidence of his identity must not be allowed to engage in business relations with the reporting institution. Additional measures must be undertaken to determine whether to proceed with the business relationship, where initial checks failed to identify the customer or give rise to suspicions that the information provided is false.

5.1.11 If failure to satisfactorily complete CDD, a reporting institution must not commence any business relation, or execute any transaction, or in the case of existing customers, must terminate such business relationship, if the customer fails to comply with the CDD requirements.

5.1.12 A reporting institution must also consider lodging a STR in relation to such customer with the FIED.

5.2 Individual Customers

5.2.1 **LSK Current CDD Practices**

Obtain at least the following information and documents to perform identification and verification:

For individuals:

- Name
- IC/Passport no.
- Permanent & mailing address
- Date of birth
- Nationality
- Occupation type
- Name of employer/nature of self-employment/nature of business
- Contact number (home office or mobile)
- Purpose of transaction
- Beneficial owner, if any

For companies/businesses:

- Company/business name
- Business registration number
- Business address/registered Address
- Nature of business

- Directors & shareholders/beneficial owners' details

5.2.2 To verify the client's identity using reliable and independent source documents, information and data

5.2.3 **LSK** should substantiate the above required information by requiring the individual to furnish the original and make a copy of the following documents:

- NRIC for Malaysian/permanent resident; or
- Passport for foreigner.

5.2.4 Where there is any doubt, **LSK** should request the customer to produce other supporting identification documents, preferably bearing a photograph of the customer, issued by an official authority, to enable the customer's identity to be ascertained.

5.3 Corporate Customers

5.3.1 In conducting customer due diligence on a corporate customer. To understand the ownership and control structure in order to detect any unusual circumstances concerning the changes to the company/business structure or ownership.

5.3.2 **LSK** should require the company/business to furnish the original and make a copy each of the following documents:

- Memorandum & Articles of Association/Certificate of Incorporation/Limited Liability Partnership (LLP);
- Identification document of Directors/Shareholders'/Partners
- Obtain the Constitution and corporate documents (Form 24/Form 49, Super Form & Annual Return may be accepted)
- Board of Directors' Ciurcular Resolution
- Authorisation for any person to represent the company; and
- Identification document of the person authorised to represent the company in its dealing with the reporting institution.

5.3.3 Where there is any doubt, **LSK** should:

- conduct a basic search or enquiry on the background of such company to ensure that it has not been, or is not in the process of being, dissolved or liquidated; and
- verify the authenticity of the information provided by the company with the Companies Commission of Malaysia.

5.4 Clubs, Societies and Charities

5.4.1 In conducting customer due diligence on a club, society or charity, **LSK** should require the club, society or charity to furnish the relevant constituent documents (or other similar documents) including certificate of registration and

Furnish the following documents:

- relevant constituent documents (or other similar documents).
- the identification of the office bearer.
- authorisation for any person to represent the club, society or charity.

Where there is any doubt as to the identity of persons referred to the above paragraphs, the reporting institution shall verify the authenticity of the information provided by such person with the Registrar of Societies, Companies Commission of Malaysia, *Bahagian Hal Ehwal Undang-Undang, Jabatan Perdana Menteri* or any other relevant authority.

5.5 Legal Arrangements

5.5.1 **Legal arrangement**, refers to express trusts or other similar legal arrangements.

Legal person, refers to any entity other than a natural person that can establish a permanent customer relationship with a reporting institution or otherwise own property. This includes companies, bodies corporate, government-linked companies (GLCs), foundations, partnerships, or associations and other similar entities.

GLC refers to an entity where the government is the majority shareholder or single largest shareholder and/or has the ability to exercise and influence major decisions such as appointment of board members and senior management.

5.5.2 For customers that are **legal persons**, reporting institutions are required to understand the nature of the customer's business, its ownership and control structure.

LSK is required to identify its customers and verify their identity through the following information:

- **name, legal form and proof of existence**, such as Certificate of Incorporation/Constitution/Partnership Agreement (certified true copies/duly notarised copies, may be accepted) or any other reliable references to verify the identity of the customer;
- **the powers that regulate and bind the customer** such as directors' resolution, as well as the names of relevant persons having a Senior Management position; and
- **the address of the registered office** and, if different, a principal place of business.

5.5.3 Reporting institutions are required to identify and verify the person authorised to represent the company or business either by means of a letter of authority or directors' resolution when dealing with such person.

5.5.4 Reporting institutions are required to identify and take reasonable measures to verify the identity of beneficial owners according to the following sequence:

a) the identity of the natural person(s) who ultimately has a controlling ownership interest in a legal person. At a minimum, this includes identifying the directors/shareholders with equity interest of more than twenty-five percent/partners;
b) to the extent that there is doubt as to whether the person(s) with the controlling ownership interest is the beneficial owner(s) referred to in paragraph 5.5.4(a) or where no natural person(s) exert control through ownership interests, the identity of the natural person (if any) exercising control of the legal person through other means; and
c) where no natural person is identified under paragraphs 5.5.4(a) or (b), the identity of the relevant natural person who holds the position of Senior Management.

5.5.5 For the purpose of paragraph 5.5.4(b), exercising control of the legal person through other means may include exercising control through nominees or another person who has the right to appoint or remove any member of the Board of the legal person.

5.5.6 Where there is any doubt as to the identity of persons referred to under paragraphs 5.5.2, 5.5.3 and 5.5.4, the reporting institution shall:

- conduct a basic search or enquiry on the background of such person to ensure that the person has not been or is not in the process of being dissolved or liquidated, or is a bankrupt; and verify the authenticity of the information provided by such person with the Companies Commission of Malaysia.

5.5.7 Reporting institutions are exempted from obtaining a copy of the Certificate of Incorporation or Constitution and from verifying the identity of directors and shareholders of the legal person which fall under the following categories:

- public listed companies or corporations listed in Bursa Malaysia;
- foreign public listed companies
  a) listed in recognised exchanges;and
  b) not listed in higher risk countries;
- foreign financial institutions that are not from higher risk countries
- an authorised person under the FSA and the Islamic Financial Services Act 2013 (i.e. any person that has been granted a licence or approval)
- persons licensed or registered under the Capital Markets and Services Act 2007
- licensed entities under the Labuan Financial Services and Securities Act 2010 and the Labuan Islamic Financial Services and Securities Act 2010
- prescribed institutions under the Development Financial Institutions Act 2002; or
- licensed entities under the Money Services Businesses Act 2012

5.5.8 Notwithstanding the above, reporting institutions are required to identify and maintain information relating to the identity of the directors and shareholders of legal persons referred to in paragraph 5.5.7 through a public register, other reliable sources or based on information provided by the customer.

Legal Arrangements

5.5.9 For customers that are legal arrangements, reporting institutions are required to understand the nature of the customer's business, its ownership and control structure.

5.5.10 Reporting institutions are required to identify the customer and verify its identity through the following information:

- name, legal form and proof of existence, or any reliable references to verify the identity of the customer
- the powers that regulate and bind the customer as well as the names of relevant persons having a Senior Management position;and
- the address of the trustee's registered office and if different, a principal place of business

5.5.11 Reporting institutions are required to identify and take reasonable measures to verify the identity of beneficial owners through the following information

- for trusts, the identity of the settlor, the trustee(s), the protector (if any), the beneficiary or class of beneficiaries, and any other natural person exercising ultimate effective control over the trust (including through the chain of control/ownership); or
- for other types of legal arrangements, the identity of persons in equivalent or similar positions

5.5.12 Reporting institutions may rely on a third party to verify the identity of the beneficiaries when it is not practical to identify every beneficiary

5.5.13 Where reliance is placed on third parties under paragraph 5.5.12, reporting institutions are required to comply with paragraph 16 on Reliance on Third Parties

5.5.14 Legal arrangements can be used to avoid customer due diligence on the beneficiary of such transaction and disguise the source of funds involved. The reporting institution needs to establish whether the customer is acting on behalf of another person as a party to a legal arrangement, for example, a trustee or nominee.

5.5.15 The reporting institution should take reasonable measures to understand the relationship among the relevant parties in handling a trustee or nominee business and obtain satisfactory evidence of its legal status, the identity of the said trustee, settlor or nominee, authorized signatories, beneficiaries and the nature of their capacity and duties as trustee or nominee.

5.5.16 It shall be reasonable for the reporting institution to rely on the trustee or nominee to verify or confirm the identity of the beneficial owners. For this purpose, the reporting institution should require a written undertaking from the trustee or nominee that identification documents of the beneficiaries have been obtained, recorded and retained. In addition, such documentation needs to be made available promptly to the reporting institution upon request.

5.6 Beneficial Ownership and Control

5.6.1 Beneficial owners (BO) are always natural persons who ultimately own or control a legal entity or arrangement.

5.6.2 As the Companies Act 2016 [Act 777] (CA 2016) defines BO as “the ultimate owner of the shares and does not include a nominee of any description”, a clarification is required to ensure that a company is able to identify the natural persons who ultimately owns or have control over the company. To this end, the definition of BO must also be read together with section 8 of the CA 2016.

5.6.3 **LSK** should conduct customer due diligence on any natural person who ultimately owns or controls the customer's transaction if it suspects a transaction is conducted on behalf of a beneficial owner and not the customer who is conducting such transaction.

5.6.4 a) Identify and take reasonable measures to verify beneficial owner (BO)

- Identity of the natural person who ultimately has a controlling ownership interest in a legal person identification of directors/shareholders with equity interest of more than 20%;
- Proper authorisation for persons authorised to represent the company (letter of authority/ directors' resolution); and
- NRIC / Passport to identify the authorised person(s)

b) If there is a doubt on the controlling interest -the identity of the natural person exercising control through other means

c) Where there is no natural person is identified, to identify relevant natural person who holds the position of senior management of the corporation.

5.6.5 **NTITIES WHICH ARE EXEMPTED FROM THE BO REPORTING FRAMEWORK**.

The following companies and limited liability partnerships are exempted from the BO reporting framework:

<u>Companies</u>

a) Companies which are licensed by Bank Negara Malaysia under the Financial Services Act 2013 [*Act 758*], Islamic Financial Services Act 2013 [*Act 759*], a prescribed development financial institution under the Development Financial Institutions Act 2002 [*Act 618*] or a licensed money services business under the Money Services Business Act 2011 [*Act 731*];

b) Persons regulated under the securities laws as follows:
- Entity licensed or registered under the Capital Markets and Services Act 2007 [*Act 671*] (CMSA 2007);
- Stock exchange, derivatives exchange, clearing house and central depository approved under the securities laws;
- Recognised self-regulatory organisation (SRO) under the CMSA 2007; and

- Private retirement scheme administrator approved under the CMSA 2007;

c) Companies whose shares are quoted in a stock exchange, either local or foreign exchange;

d) Companies whose shares are deposited in the central depository pursuant to the Securities Industry (Central Depositories) Act 1991 [*Act 453*]. The exemption under this subparagraph (d) only applicable if all the shares in a company remain deposited with the central depository.

e) Government-linked companies in Malaysia;

f) State-owned corporations and companies in Malaysia;

Limited liability partnerships

The only limited liability partnerships which are exempted from the BO reporting framework are those which are licensed or regulated under the laws stated under paragraph 5.6.5 (a) or (b) above, if any.

5.6.6 In the event, **LSK**'s corporate customer is a public company which is subjected to regulatory disclosure, it would not be necessary for the reporting institution to identify or verify the identity of any shareholder.

5.7 Reliance on intermediaries for CDD

5.7.1 The reporting institution who uses the services of intermediaries to introduce business may rely on the customer due diligence conducted by such intermediaries. However, the ultimate responsibility of customer due diligence remains with the reporting institution.

5.7.2 In facilitating effective oversight, the relationship between the reporting institution and its intermediaries should be governed by an arrangement/agreement that clearly specifies the rights, responsibilities and expectations of all parties. At the minimum, the reporting institution must be satisfied that the intermediary:

- has an adequate customer due diligence process;
- has a reliable mechanism to verify customer identity;
- can provide the customer due diligence information and make copies of the relevant documentation available immediately upon request; and

- where appropriate, is properly regulated and supervised by the respective authorities.

5.7.3 In addition, customer due diligence procedures should be performed, either on the reporting institution's own records or via copy of records obtained from the introducing entity.

5.8 Non-face-to-face Business Relationship

5.8.1 The reporting institution should pay special attention in establishing and conducting business relationship via information communication technology, for example, the internet, post, fax or telephone. Any business relationship/transaction that avoids face- to-face contact without proper customer identification and verification may be subject to abuse by money launderers and financiers of terrorism in gaining access to the economic system.

5.8.2 The reporting institution should only establish business relationship upon completion of the customer due diligence process conducted through face-to-face interaction.

5.8.3 The reporting institution is also required to establish appropriate measures for customer verification that should be as stringent as that for face-to-face customers and implement monitoring and reporting mechanisms to identify potential money laundering and financing of terrorism activities.

5.8.4 Reporting institutions shall take measures to identify and verify the customer's identity through any of the following:

- establishing independent contact with the customer;
- verifying the customer's information against reliable and independent sources to confirm the customer's identity and identifying any known or suspected ML/TF risks associated with the customer; or
- requesting, sighting and maintaining records of additional documents required to perform face-to-face customer verifications.

5.9 Foreign Politically Exposed Persons (PEPs)

5.9.1 Refers to:

a) **foreign PEPs** – individuals who are or who have been entrusted with prominent public functions by a foreign country. For example, Heads of State or Government, senior politicians, senior government, judicial or military officials, senior executives of state owned corporations and important

political party officials;

b) **domestic PEPs** – individuals who are or have been entrusted domestically with prominent public functions. For example, Heads of State or Government, senior politicians, senior government (includes federal, state and local government), judiciary or military officials, senior executives of state owned corporations and important political party officials; or

c) persons who are or have been entrusted with a prominent function by an international organisation which refers to members of senior management. For example, directors, deputy directors and members of the Board or equivalent functions.

The definition of PEPs is not intended to cover middle ranking or more junior individuals in the foregoing categories. Immediate family members of PEPs (such as spouses, children, parents, and siblings) or close associates of PEPs. Close associate of PEP are also included in this category as the same risks are involved as with PEPs themselves;

Family members of PEP

Refers to individuals who are related to a PEP either directly (consanguinity) or through marriage. A family member in this context includes:

- parent;
- sibling;
- spouse;
- child; or
- spouse's parent,

for both biological or non-biological relationships.

Close associate of PEP

Refers to any individual closely connected to a politically exposed person (PEP), either socially or professionally. A close associate in this context includes:

- extended family members, such as relatives (biological or non-biological relationship);
- financially-dependent individuals (e.g. persons salaried by the PEP such as drivers, bodyguards, secretaries);
- business partners or associates of the PEP;
- prominent members of the same organisation as the PEP;

- individuals working closely with the PEP (e.g. work colleagues or providing professional services); or close friends.

5.9.2 The concern placed in dealing with PEPs lies with the possibility of such PEPs abusing their public powers for their own illicit enrichment, especially in countries where corruption is widespread.

5.9.3 Company is required to take appropriate measures to establish the source of wealth and source of funds of such person

5.9.4 The reporting institution should have, in addition to their respective customer due diligence process, a risk management framework to determine whether current or new customers are PEPs. In establishing whether or not the customer is a PEP, the reporting institution should at least gather sufficient and appropriate information from the customer and through publicly available information.

5.9.5 Once a PEP is identified, the reporting institution should take reasonable and appropriate measures to establish the source of wealth and funds of such person.

5.9.6 The decision to enter into or continue business relationships with PEPs should be made by the Senior Management of the reporting institution.

5.9.7 In addition, the reporting institution should conduct enhanced on-going due diligence on PEPs throughout its business relationships with such PEPs. For such purpose, the reporting institution should note that business relationships with family members or close associates of PEPs involve similar reputational risks to those with PEPs themselves.

5.10 Enhanced Customer Due Diligence measures (ECDD)

Where nominee services are provided, such business relations must be subjected to enhanced CDD and enhanced on-going due diligence. Nominee services refer to nominee shareholding, directorship or partnership services, where applicable.

Higher risk customers

5.10.1 **Enhanced Customer Due Diligence measures (ECDD)**
Customers considered high-risk, are subject to enhanced due Diligence (ECDD).

The Company shall conduct enhanced due diligence on higher risk customers or when establishing a business relationship with customers:

- Whom are suspected of money laundering or financing of terrorism
- Where there are doubts about the reliability or adequacy of previously obtained information

5.10.2 Unwillingness of customer to cooperate may itself be a factor of suspicion. It is the Company's policy to get the sufficient identification evidence.

5.10.3 Enhanced due diligence should include at least:

- Obtaining more detailed information from the customer and through publicly available information, in particular, on the purpose of transaction and source of funds; and
- Obtaining approval from the Senior Management of the reporting institution before establishing the business relationship with the customer.

Higher risk refers to circumstances where the reporting institutions assesses the ML/TF risks as higher, taking into consideration, and not limited to the following factors:

a) **Customer risk factors**

Example:

- the business relationship is conducted in unusual circumstances (e.g. significant unexplained geographic distance between the reporting institution and the customer);
- non-resident customers;
- legal persons or arrangements that are personal asset- holding vehicles;
- PEPs;
- companies that have nominee shareholders or shares in bearer form;
- businesses that are cash-intensive / cash based businesses;
- the ownership structure of the company appears unusual or excessively complex given the nature of the company's business;
- high net worth individuals;
- Unregulated industries;
- persons from locations known for their high rates of crime (e.g. drug producing, trafficking, smuggling);
- circumstances, businesses or activities identified by the FATF as having higher ML/TF risks;
- Countries or jurisdictions with inadequate AML/CFT laws and regulations such as the Non-Cooperative Countries and

Territories (NCCT);
- legal arrangements that are complex (e.g. nominee relationships, trust or layering with legal persons); and
- persons who match the red flag criteria of the reporting institutions.

b) **Country or geographic risk factors**:
- countries identified by credible sources, such as mutual evaluation or published follow-up reports, as having inadequate AML/CFT systems;
- countries subject to sanctions, embargos or similar measures issued by, for example, the United Nations;
- countries identified by the FATF, other FATF-style regional bodies or other international bodies as having higher ML/TF risks;
- countries identified by credible sources as having significant levels of corruption or other criminal activities; and countries or geographic areas identified by credible sources as providing funding or support for terrorist activities, or that have designated terrorist organisations operating within their country.

c) **Product, service, transaction or delivery channel risk factors**:
- anonymous transactions (which may include cash);
- non face-to-face business relationships or transactions;
- payment received from multiple persons and/or countries that do not match the person's nature of business and risk profile;
- payment received from unknown or unrelated third parties; and nominee services.

5.11 Higher Risk Countries

Refers to countries that are called by the FATF or the Government of Malaysia that pose a risk to the international financial system.

5.11.1 Reporting institutions are required to conduct enhanced CDD for business relationships and transaction with any person from countries identified by the FATF or the Government of Malaysia that pose a risk to the international financial system.

5.11.2 Where ML/TF risks are assessed as higher risk, reporting institutions are required to conduct enhanced CDD for business relationships and transactions with any person from countries identified by the FATF or the Government of Malaysia as having strategic AML/CFT deficiencies and have not made sufficient progress in addressing those deficiencies.

5.11.3 In addition to the enhanced CDD requirement under Paragraph

5.11.1 reporting institutions are required to apply appropriate countermeasures, proportionate to the risk, for higher risk countries listed as having on-going or substantial ML/TF risks, as follows:

- limiting business relationship or financial transactions with identified countries or persons located in the country concerned;
- conduct enhanced external audit, by increasing the intensity and frequency, for branches and subsidiaries of the reporting institution or financial group, located in the country concerned;
- submit a report with summary exposure to customers and beneficial owners from the country concerned to the Financial Intelligence and Enforcement Department, Bank Negara Malaysia as the Competent Authority and Supervision and Enforcement Department

5.12 Existing customers

5.12.1 The reporting institution should take the necessary measures to ensure that the record of existing customers, including its customer's profile remains updated and relevant. In addition, further evidence in identifying the existing customers should be obtained to ensure compliance with the reporting institution's current customer due diligence standards.

5.12.2 The reporting institution should conduct regular reviews on existing records of customers, especially when:

- a significant transaction is to take place;
- there is a material change in the way the account is operated;
- the customer's documentation standards change substantially; or
- it discovers that the information held on the customer is
- insufficient.

5.12.3 In circumstances other than those mentioned in paragraph5.12.2, the reporting institution, based on risk assessment, may require additional information consistent with the reporting institution's current customer due diligence standards from those existing customers that are considered to be of higher risk.

6. RECORDS KEEPING

6.1 Retention Period

6.1.1 **LSK** must keep record of all transactions and ensure they are up to date and relevant. The records must at least include the following information for each transaction:

- Documents 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 pertaining 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.
- Keep all KYC information, copies of ID documents, transaction details and any analysis of STRs filed/submitted

6.1.2 Scope of record keeping extended to include accounts, business correspondence and documents relating to an account, business relationship, transaction or activity with a customer as well as result of any analysis taken.

6.1.3 **LSK** is required to retain, for at least seven (7) years after the transaction has been completed or after the business relations with the customer have ended. 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.

6.1.4 In situations where the records are subject to on-going investigations or prosecution in court, they shall be retained beyond the stipulated retention period until it is confirmed by the Financial Intelligence Unit in Bank Negara Malaysia, that such records are no longer needed.

6.1.5 Failing to comply, a fine of up to RM3 million or imprisonment to a term not exceeding 5 years would be imposed.

6.2 Audit Trail

6.2.1 **LSK** must ensure that the retained documents and records are able to create an audit trail on individual transactions that are traceable by Bank Negara Malaysia, the relevant supervisory and law enforcement agencies.

6.2.2 In addition, the records kept must enable the reporting institution to establish the history, circumstances and reconstruction of each transaction.

The records shall include at least:

- the identity of the customer;
- the identity of the beneficiary;
- the type of transaction (e.g., deposit or withdrawal);
- the form of transaction (e.g., by cash or by cheque);
- the instruction and the origin and destination of fund transfers; and
- the amount and type of currency.
-

6.3 Format

6.3.1 **LSK** should retain the relevant document in the form that is acceptable under section 3 of the Evidence Act 1950, secure and retrievable, upon request, in a timely manner.

6.4 Management Information System

6.4.1 A management information system (MIS) is an information used for decision- making, and for the coordination, control, analysis, and visualization of information in an organization.

6.4.2 The MIS may be integrated with the reporting institution's information system that contains its customer's normal transaction or business profile, which is accurate, up-to-date and reliable.

6.4.3 In supporting the monitoring activity of Customer's profile and transaction in order to run effectively, an information system has been created and developed that is able to monitor, identify, analyze, and supply the report with the characteristic of transaction based on risk made by a Customer.

6.4.4 **LSK** computerized business by using ABSS accounting software (previously known as MYOB). ABSS is an Australian multinational corporation that provides tax, accounting and other business services software to small and medium businesses.

7. ON GOING MONITORING

7.1 On-Going Due Diligence

7.1.1 A reporting institution shall conduct ongoing due diligence and scrutiny of its customers throughout the course of the business relationship. All findings must be documented and made available to Bank Negara Malaysia and the relevant supervisory authority upon request. Such measures shall include–

a) monitoring and detecting patterns of transactions undertaken throughout the course of that business relationship to ensure that the transactions being conducted are consistent with the reporting institution's knowledge of the customer, its business, and risk profile, including where necessary, the source of funds; and

b) ensuring that documents, data or information collected under the CDD process is kept up-to-date and are relevant, by undertaking periodic reviews of existing records, particularly for higher risk categories of customer.

7.1.2 A reporting institution must apply CDD measures to existing customers on the basis of materiality and risk, and conduct due diligence on such existing relationship at appropriate times, taking into account whether and when CDD measures have previously been undertaken and the adequacy of the data verified.

7.1.3 A reporting institution must monitor the customers' accounts on a regular basis for suspicious transactions. One method is to 'flag' accounts with suspicious transactions for monitoring purpose.

7.1.4 A reporting institution should consider reclassifying a customer as higher risk and consider lodging a suspicious transaction report (STR) with the FIED under the following circumstances:

- Following initial acceptance of the customer, the pattern of account activity of the customer is inconsistent and does not fit in with the reporting institution's profile knowledge of the customer;
- The transaction appears unusual and not in line with the customer's normal trading pattern; or
- There is a material change in the way the account is operated.
- does not have any apparent economic purpose; or
- casts doubt on the legality of such transactions, especially

with regard to complex and large transactions or involving higher risk customers

7.1.5 While extra care should be exercised in such cases, the reporting institution must weigh all the circumstances of the particular situation and assess whether there is a higher than normal risk of ML/TF and consider whether to refuse to do any business with such customers.

7.1.6 The frequency of the ongoing CDD shall commensurate with the level of ML/TF risks posed by the customer based on the risk profile and nature of transactions.

7.1.7 A reporting institution is required to undertake a renewed CDD when:-

- there is a suspicion of ML/TF risks; or
- there is a doubt about the veracity or adequacy of previously obtained identification data.

7.1.8 An effective customer due diligence process would enable the reporting institution to detect related money laundering and financing of terrorism transactions at the point of customer contact (based on the front-line staff's *ad hoc* report). Generally, most detection would be made through analysing the transaction patterns or activities of the customer.

7.2 Other Developments on AML- AML WORLD BODY (FATF & APG)

7.2.1 The Financial Action Task Force (FATF) (established in 1989) is an inter- governmental body whose purpose is the development and promotion of policies, both at national and international levels, to combat money laundering and terrorist financing.

7.2.2 The Task Force is therefore a "policy-making body" which works to generate the necessary political will to bring about national legislative and regulatory reforms in these areas.

7.2.3 The FATF monitors members' progress in implementing necessary measures, reviews money laundering and terrorist financing techniques and counter- measures, and promotes the adoption and implementation of appropriate measures globally.

7.2.4 Malaysia is a member of FATF and a member of Asia Pacific Group (APG) on money laundering. APG plays similar role as FATF but at a regional level.

7.2.5 FATF has established and revised 40 recommendations in 1996 for combating AML worldwide.

7.2.6 It has further introduced 9 special recommendations in 2001 to address financing of terrorism activities following Sept 11 incident.

7.2.7 In Feb 2012, FATF has revised its recommendations to 40 recommendations, to strengthen global safeguard and further protect the integrity of the financial system.

8. SUSPICIOUS TRANSACTION REPORTING

8.1 General

8.1.1 Reporting institutions are required to promptly submit a suspicious transaction report (STR) to the Financial Intelligence and Enforcement Department, Bank Negara when any of its employees suspect or have reason 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, regardless of the amount:

- appears unusual;
- has no clear economic purpose;
- appears illegal;
- involves proceeds from an unlawful activity; or
- indicates that the customer is involved in ML/TF.

8.1.2 Reporting institutions must provide the required and relevant information that gave rise to doubt in the suspicious transaction report form, which includes but is not limited to the nature or circumstances surrounding the transaction and business background of the person conducting the transaction that is connected to the unlawful activity.

8.1.3 Reporting institutions must establish a reporting system for the submission of suspicious transaction reports.

8.1.4 *Examples of Transactions that May Trigger Suspicion*

Designated Non-Financial Businesses and Professions (DNFBPs)

1. Transactions that appear inconsistent with a customer's known profile or unusual deviations from normal transaction or relationship.

2. Transactions that require the use of complex and opaque legal entities and arrangements.

3. Transaction with entity established in jurisdictions with weak or absent AML/CFT laws and/or secrecy laws.

4. A customer who is reluctant to provide evidence of his identity or where the customer is a corporate entity, evidence of its place of incorporation and the identity of its major shareholders and its director(s) or relevant officer(s).

5. A customer is a known or suspected triad member, drug trafficker or terrorist, or where the customer has been introduced by any such persons.

6. Any situation where the identity of the customer is difficult to be determined.

7. The entry of matching buys and sells in particular securities, creating illusion of trading. Such trading does not result in a bona fide market position, and might provide 'cover' for a money launderer.

8. Buying and selling of a security with no discernible purpose or in circumstances, which appear unusual.

9. Larger or unusual settlements of securities transactions in cash form.

8.2 Reporting mechanisms

8.2.1 When faced with an abnormal or suspicious transaction or activity, a member of the staff faced with a customer, transaction, or situation that he or she feels is suspicious must:

- immediately seek the advice of the department manager who will decide whether to accept the transaction or whether to immediately submit the details to the compliance officer to

enable him or her to take a decision;

- as far as technically possible, delay execution of the transaction to enable a decision to be made;
- take note of all information available on the proposed transaction, and photocopy documents submitted, if possible;
- never mention in any manner whatsoever the actual reason for the delay or reluctance to execute the transaction requested;
- remain evasive about the internal decision-making procedures, with respect to the transaction in question; and
- not recontact the customer, except where necessary to protect the interests of the NBFI, or in exceptional circumstances, and that too as per the direction of the compliance officer.

8.2.2 **Compliance Officer Procedures**

When the Compliance Officer receives a suspicious transaction report, he or she will log it, allocate a reference number, and acknowledge receipt. He or she will then undertake sufficient inquiries to determine whether, in his or her judgment, the concerned transaction is suspicious. This action must be undertaken promptly.

The Compliance Officer may review

- the account opening records and CDD and other information obtained from the customer,
- historical transaction patterns, and
- any previous suspicious transaction reports.

The Compliance Officer may discuss the report with

- the members of the staff and/or the senior management, or
- other members of the management, as appropriate.

The Compliance Officer must

- document his or her inquiries and the reason for deciding to/not to forward the suspicious transaction report to the financial intelligence unit.

8.2.3 The reporting institution should appoint one Compliance Office officer at the Senior Management level to be responsible for the submission of suspicious transaction reports to the Financial Intelligence Unit in Bank Negara Malaysia. The appointed Compliance Officer is the single point of reference for the Financial Intelligence Unit in Bank Negara Malaysia with regards to AML/CFT matters.

8.2.4 Reporting institutions are required to ensure that the Compliance

Officer is responsible for channeling all internal suspicious transaction reports received from the employees to the Compliance Officer.

8.2.5 Reporting institutions are required to have in place policies on the duration upon which internally generated suspicious transaction reports must be reviewed by the Compliance Officer, including the circumstances when the timeframe can be exceeded, where necessary.

8.2.6 Upon receiving the Internal Suspicion Report, the Compliance Officer shall evaluate the grounds for suspicion and if suspicion is confirmed he or she shall submit a suspicious transaction report to the Financial Intelligence Unit in Bank Negara Malaysia on the next working day through any of the following channels:-

Mail : **Director**
Financial Intelligence and
Enforcement Department Bank
Negara Malaysia
Jalan Dato' Onn
50480 Kuala Lumpur
(To be opened by addressee only)

Fax : **+603- 2693 3625**
E-mail : **str@bnm.gov.my**
Online: **https://bnmapp.bnm.gov.my/fins2**

8.2.7 The Compliance Officer must ensure that the suspicious transaction report is submitted within the next working day, from the date the Compliance Officer establishes the suspicion.

8.2.8 Reporting institutions must ensure that in the course of submitting the suspicious transaction report, utmost care must be undertaken to ensure that such reports are treated with the highest level of confidentiality. The Compliance Officer has the sole discretion and independence to report suspicious transactions.

8.2.9 Reporting institutions must ensure that the suspicious transaction reporting mechanism is operated in secured environment to maintain confidentiality and preserve secrecy. Hence, the

Compliance Officer must be given the independence to report suspicious transactions to the Financial Intelligence Unit in Bank Negara Malaysia without the need to go through any elaborate approval process.

8.2.10 Where a suspicious transaction report has been lodged, reporting institutions are not precluded from making a fresh suspicious transaction report when a new suspicion arises.

8.2.11 The reporting institution should ensure that its Compliance Officer is authorised to cooperate with the Financial Intelligence Unit in Bank Negara Malaysia in providing such additional information and documentation as it may request and to respond promptly to any further enquiries with regards to any suspicious transaction report.

8.2.12 The reporting institution should ensure that the suspicious transaction reporting mechanism is operated in a secured environment to maintain confidentiality and preservation of secrecy. Except for the purposes permitted in section 79 of the AMLATFPUAA, the disclosure of any information or matter which has been obtained by any person within the reporting institution, in the performance of his duties or the exercise of his functions is an offence under the AMLATFPUAA.

8.3 Triggers for submission of suspicious transaction report

8.3.1 Reporting institutions are required to establish internal criteria ("red flags") to detect suspicious transactions.

8.3.2 Reporting institutions may be guided by examples of suspicious transactions provided by other corresponding competent authorities, supervisory authorities and international organisations.

8.3.3 Reporting institutions must consider submitting a suspicious transaction report when any of its customer's transaction or attempted transaction fits the reporting institution's list of "red flags".

8.3.4 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 Compliance Officer immediately – via an Internal Suspicion Report:-

Examples of "Red Flags" – Possible Suspicious Transactions

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

8.4 Internally Generated Suspicious Transaction Reports

8.4.1 The reporting institution must ensure that the compliance officer maintains a complete file on all internally generated suspicious transaction reports and any supporting documentary evidence regardless that such reports have been submitted to the Financial Intelligence Unit in Bank Negara Malaysia.

8.4.2 The reporting institutions must undertake reasonable measures to ensure that all its employees involved in conducting or facilitating the customerís transaction are aware of these reporting procedures and that failure to report suspicious transaction when they have reasonable grounds to believe that the transaction is ìsuspiciousî is an offence under the AMLATFPUAA.

8.5 Other Reporting Obligations

8.5.1 **Data Compliace Report (DCR)**

Reporting institutions are required to submit the following reports to the Financial Intelligence and Enforcement Department, Bank Negara Malaysia, as and when applicable:

- Data and Compliance Report issued by Bank Negara Malaysia; and
- any other report as may be specified by Bank Negara Malaysia.

9. COMBATING THE FINANCING OF TERRORISM

9.1 General

9.1.1 Where relevant, the references to a customer in this Paragraph include a beneficial owner and beneficiary.

9.1.2 The reporting institution should ensure that the existing suspicious transaction reporting system and mechanism for the identification of suspicious transactions are extended to cover financing of terrorism.

9.1.3 Reporting institutions are required to keep updated with the various resolutions. The United Nations Security Council (UNSC) has passed various resolutions pursuant to UNSC Resolution 1267 (1999) to require sanctions against individuals and entities belonging or related to the Taliban, Usama bin Laden and the Al-Qaida organization. Reporting institutions are required to maintain a list of individuals and entities (the Consolidated List) for this purpose. The updated UN List can be obtained at: https://www.un.org/sc/suborg/en/sanctions/1267/aq_sanctions_list

9.1.4 Reporting institutions are required to maintain a database of names and particulars of listed persons in the UN Consolidated List and such orders as may be issued under sections 66B and 66C of the AMLATFPUAA by the Minister of Home Affairs.

9.1.5 In ensuring efficient detection of suspected financing of terrorism, the reporting institution should maintain a database of names and particulars of terrorist in the UN Consolidated List and such orders as may be issued under sections 66B and 66C of the AMLATFPUAA by the Minister of Internal Security. In addition, the reporting institution may also consolidate their database with the other recognized lists of designated persons or entities issued by other jurisdictions.

9.1.6 The reporting institution should ensure that the information contained in the database are updated and relevant, and made easily accessible to its employees at the head office, branch or subsidiary for the purpose of identifying suspicious transactions.

9.1.7 Reporting institutions are required to ascertain potential matches with the Consolidated List to confirm whether they are true matches to eliminate “false positive”. The reporting institutions are required to make further inquiries from the customer or counter-party (where relevant) to assist in determining whether the match is a true match.

9.1.8 Reporting institutions are required to submit a suspicious transaction report when there is an attempted transaction by any of the persons listed in the Consolidated List or orders made by the Minister of Home Affairs under section 66B or 66C of the

AMLATFPUAA.

9.1.9 The reporting institution should conduct regular checks on the names of new and existing customers against the names in the database. If there is any name match, the reporting institution should take reasonable and appropriate measures to verify and confirm the identity of its customer. If the customer's name fully matched any name in the database, the reporting institution should immediately:

a) submit a suspicious transaction report to inform the Financial Intelligence Unit in Bank Negara Malaysia;
b) reject the customer, if the transaction has not commenced; and
c) freeze the customer's transaction, if it is an on-going customer.

10. AML/CFT COMPLIANCE PROGRAMME

10.1 Policies, Procedures and Controls

10.1.1 Internal policies, procedures and controls (" **IPPCs** "). to prevent activities related to money laundering and financing of terrorism. It is the duty of the Board of Directors to maintain adequate oversight of the overall AML/CFT measures undertaken by the reporting institution and the duty of the Senior Management to ensure that the Board of Directors is updated with timely information.

10.1.2 To ensure effective implementation, the Board of Directors should define the lines of authority and responsibilities for implementing the AML/CFT measures and ensuring that there is a separation of duty between those implementing the policies and procedures and those enforcing the controls. In line with this, the Board of Directors should ensure the compliance officer is appointed for effectiveness in assessing and evaluating the controls to prevent money laundering and the financing of terrorism.

10.1.3 The Company has established and maintained appropriate and risk-sensitive IPPCs concerning all of the following matters:

- CDD measures (including simplified and enhanced) and on-going monitoring (including enhanced on-going monitoring);
- appropriate compliance management arrangements including monitoring, carrying out regular review assessment, updates and the internal communication of the IPPCs to ensure that they are adequate and they manage the money laundering and

financing of terrorism risks effectively;

- making of suspicious transaction reports;
- risk assessment and management;
- appointment of a professional, third party service provider to conduct the CDD measures;
- appointment of an internal AML/CTF compliance offer;
- responding to the relevant authority's feedback as and when enquired and
- only if required by applicable laws, training of directors, and employees of the Company.

10.1.4 The IPPCs in paragraph 10.1.3 include those which:

- provide for the identification and scrutiny of complex or unusually large transactions; unusual patterns of transactions which have no apparent economic or visible lawful purpose;
- unusual patterns of transactions which are not related to the business activities of the customer for which the entity was originally set up to conduct; and any other activity which the Company regards as particularly likely by its nature to be related to money laundering or the financing of terrorism;

- specify the taking of additional measures, where appropriate and necessary, to prevent the development of new products and new business practices, including new delivery mechanisms, for money laundering and the financing of terrorism and proliferation; and the use of new or developing technologies, for both new and pre-existing products, for money laundering and the financing of terrorism; and determine whether a customer, connected party, beneficial owner, or agent is a PEP.

10.1.5 Senior management shall be actively involved in the approval process of the Company's anti money laundering and counter financing of terrorism IPPCs.

10.1.6 The Board of Directors should review and assess the AML/CFT policies and procedures in line with changes and developments in the reporting institution's products and services, technology as well as trends in money laundering and the financing of terrorism. The Senior Management is responsible to implement the necessary changes to the AML/CFT policies and procedures with the approval of the Board of Directors in ensuring that the current policies are sound and appropriate.

10.1.7 The Board of Directors and the Senior Management should ensure that there is adequate AML/CFT training provided for

its employees, including promoting employees' awareness of their AML/CFT obligations.

10.2 Staff Integrity

10.2.1 The company must request the Curriculum vitae (CV) with Personal and/or Professional background before recruiting the employee.

10.2.2 The employee assessment system should include evaluation of an employee's personal information, including criminal records, employment and financial history as part of the recruitment process.

10.2.3 At the same time, the Compliance Department must control that the name of the applicant or employee is not recorded on the bankruptcy list Malaysia.

10.2.4 Supervisors/managers must know the staff in their department and report any substantial change in the financial situation or in the spending habits of the employees working directly under them.

10.2.5 In order to ensure the integrity of **LSK**'s payroll, supervisors /managers must monitor their staff's behavior that is to adequately screen its employees.so as to identify and report any situations that might be considered suspicious.

The following are examples of situations to watch out for:

- Sudden and significant changes in their standard of living.
- Lifestyle and spending habits that aren't consistent with their salary, financial position or level of indebtedness.
- If employee refuses to take time off for no apparent reason.
- Employees who don't allow other colleagues to assist certain customers.
- If employee suspiciously receives gifts or gratuities on a regular basis.
- Employees who are reluctant to accept any promotions or changes in their activities.
- Employees who stay at the office after working hours or that go to the office at odd times for no reasonable explanation.

10.2.6 In addition, unusual activities in operations on behalf and to the order of employees will be identified through the Entity's monitoring process, and will be evaluated based on the profile and remuneration of the employees.

10.3 Compliance Officer

10.3.1 A reporting institution shall appoint a Compliance Officer at management level. This is a management position held by a person of trust. He/she to carry out his/her AML/CFT responsibilities and can effectively discharge it. He/she will be in charge of the application of the internal programmes and procedures, including proper maintenance of records and reporting of suspicious transactions. The compliance officer will have full access to any and all information and/or documentation they deem necessary in order to fulfil their duties.

10.3.2 The Compliance Officer must have sufficient stature, authority and seniority within the reporting institution to participate and be able to effectively influence decisions relating to AML/CFT matters.

10.3.3 The minimum criteria relating to a Compliance Officer:

- probity, personal integrity and reputation;
- competency and capability; and
- financial integrity.

10.3.4 In general, the Compliance Officer acts as the reference point for the AML/CFT matters, including employees training and reporting of suspicious transactions.

10.3.5 All reporting institutions under the Anti-Money Laundering, Anti-Terrorism Financing and Proceeds of Unlawful Activities Act 2001 (AMLATFPUAA) are required to inform, in writing, the Financial Intelligence Unit in Bank Negara Malaysia (BNM), within ten working days, on the appointment or change in the appointment of the Compliance Officer including such details as his/her name, designation, office address, office telephone number, fax number, e-mail address and such information as may be required by Bank Negara Malaysia pursuant to paragraph 11.5.13 of the Anti-Money Laundering, Countering Financing of Terrorism and Targeted Financial Sanctions for DNFBPs and NBFIs (AML/CFT and TFS for DNFBPs and NBFIs).

10.3.6 The reporting institution should ensure that the roles and responsibilities of the Compliance Officer are clearly defined and documented. The Compliance Officer should ensure the

following:

- the reporting institution's compliance with the AML/CFT requirements;
- implementation of the AML/CFT policies;
- the appropriate AML/CFT procedures, including customer acceptance policy, customer due diligence, record-keeping, on-going monitoring, reporting of suspicious transactions and combating the financing of terrorism are implemented effectively;
- the AML/CFT mechanism is regularly assessed to ensure that it is effective and sufficient to address any change in money laundering and financing of terrorism trends;
- the channel of communication from the respective employees to the Compliance Officer and subsequently to the compliance officer is secured and that information is kept confidential;
- all employees are aware of the reporting institution's AML/CFT measures, including policies, control mechanism and the channel of reporting;
- establish and maintain relevant internal criteria (red-flags) to enable identification and detection of suspicious transactions;
- To investigate reports of unusual transactions, as well as those detected in the centralized monitoring process
- internal generated suspicious transaction reports by compliance officers are appropriately evaluated before submission to the Financial Intelligence Unit in Bank Negara Malaysia; and
- the identification of money laundering and financing of terrorism risks associated with new products or services or arising from the reporting institution's operational changes, including the introduction of new technology and processes.
- It is important and imperative that the Compliance Officer

appointed by the reporting institution has the necessary knowledge, expertise and required authority to effectively discharge his/her responsibilities, including knowledge on AML/CFT obligations required under the relevant laws and regulations, the latest developments in money laundering and financing of terrorism techniques, the AML/CFT measures undertaken by the industry and timely access to customer due diligence documentation and other relevant information.

- compliance with any other obligations that are imposed under the AMLATFPUAA, subsidiary legislation and relevant instruments.

- To keep **LSK** informed and updated about any legal matters and regulations that affect **The Company** in its management of the prevention against money laundering.

10.4 Staff Training & Communications

10.4.1 The Board of Directors and Senior Management team to ensure that there is adequate training provided including promoting staff awareness on individual AML/CFT obligations and penalties if they failed to discharge their duties properly under the Act.

10.4.2 This policy also serves as the basis for staff training.

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

10.5 Independent Audit

10.5.1 The Board of Directors is responsible to ensure regular independent audit of the internal AML/CFT measures to determine their effectiveness and compliance with the AMLATFPUAA, the AMLATFPUAA Regulations and the relevant guidelines on AML/CFT issued by Bank Negara Malaysia as well as the requirements of the relevant laws and regulations of other supervisory authority, if any.

10.5.2 Reporting institutions may appoint internal or external auditors to carry out the independent audit function. The Board of Directors should ensure that the roles and responsibilities of the auditor are clearly defined and documented. The roles and responsibilities of the auditor should at least include:

- checking and testing the compliance with, and effectiveness of, the AML/CFT policies, procedures and controls; and
- assessing whether current measures are in line with the latest developments and changes of the relevant AML/CFT requirements.

10.5.3 The Board shall determine and ensure the frequency and scope of independent audits conducted commensurate with the ML/TF risks and vulnerabilities assessed by the reporting institution.

10.5.4 The scope of the independent audit shall include, at a minimum:

- acompliance with the AMLATFPUAA, its subsidiary legislation and instruments issued under the AMLATFPUAA;
- compliance with the reporting institution's internal AML/CFT policies and procedures;
- adequacy and effectiveness of the AML/CFT Compliance Programme; and
- reliability, integrity and timeliness of the internal and regulatory reporting and management of information systems.

10.5.5 In determining the frequency of the independent audit, reporting institutions may be guided by the following circumstances:

- structural changes to the business of the reporting institutions such as mergers and acquisition;
- changes to the number or volume of transactions reported to the Financial Intelligence and Enforcement Department, Bank Negara Malaysia;
- introduction of new products and services or new delivery channel; or
- previous non-compliance under the AMLATFPUAA which resulted in supervisory and/or enforcement action taken against the reporting institution.

10.5.6 Reporting institutions shall comply with any additional requirements on the frequency and scope of the independent audit as specified by the competent authority.

10.5.7 The auditor must submit a written audit report to the Board to highlight the assessment on the effectiveness of established AML/CFT measures and inadequacies in internal controls and procedures including recommended corrective measures.

10.5.8 Reporting institutions must ensure that such audit report

including audit findings and the necessary corrective measures undertaken are made available to the competent authority, upon request.

10.5.9 The auditor must submit a written report on the audit findings to the Board of Directors, which should be used to highlight inadequacies of any internal AML/CFT measures and controls and the Board of Directors should ensure that necessary steps are taken to rectify the inadequacies, if any.

10.5.10 The reporting institution should ensure that such audit findings and reports are submitted to the Financial Intelligence Unit in Bank Negara Malaysia within two weeks of their submission to its Board of Directors.

11. NON-COMPLIANCE WITH PROVISIONS UNDER AMLA

11.1.1 Due diligence in the compliance with standards for the prevention of money laundering will be considered as yet another element to be evaluated when appraising employee performance. Non compliance to the Prevention Against Money Laundering and Terrorist Financing Policies is detrimental to **LSK**, authorities, officers and employees. Since the reputation of its staff is directly link to the reputation of the company, any infringement will have a double impact. In addition, any breach or infringement of the Prevention Against Money Laundering and Terrorist Financing Policies will mean that staff might be subject to internal disciplinary measures and that **LSK**, authorities and officials may be subject to penalties.

11.1.2 Enforcement action can be taken against the reporting institutions including its Directors, Officers, and Employees for any non-compliance with provision under the following sections of the AMLATFPUAA;

a. **Section 86** of the AMLATFPUAA provides that any person who contravenes any provision of the AMLATFPUAA, or regulations made under the AMLATFPUAA, or any specification or requirement made, or any order in writing, direction, instruction, or notice given, or any limit, term, condition or restriction imposed, in the exercise of any power conferred under or pursuant to any provision of the AMLATFPUAA commits an offence and shall, on conviction, if no penalty is expressly provided for the offence under the AMLATFPUAA or the regulations, be liable to a fine not exceeding one million ringgit RM1,000,000.00.

Section 86	
Description	***Implication***
For penalty that is not expressly provided for any offences under AMLATFPUAA	<RM1 million

b. **Section 22** of the AMLATFPUAA requires that an officer of a reporting institution takes all reasonable steps to ensure its compliance with the reporting obligation under Part IV of the AMLATFPUAA. Failure of a reporting institution to comply with any of the requirements will result in Bank Negara Malaysia taking the appropriate enforcement action, including obtaining a Court order against any or all of the officers or employees of the reporting institution on terms that the Court deems necessary to enforce compliance.

Notwithstanding any Court order, the Financial Intelligence Unit in Bank Negara Malaysia may direct or enter into an agreement with the reporting institution to implement any action plan to ensure compliance with Part IV of the AMLATFPUAA. Failure of an officer to take reasonable steps to ensure compliance with Part IV of the AMLATFPUAA, or failure of a reporting institution to implement any action plan as agreed to ensure compliance, will result in the officer or officers being personally liable to a fine not exceeding one million ringgit RM1,000,000.00 or to imprisonment for a term not exceeding three years or to both, and in the case of a continuing offence, a further fine may be imposed on the reporting institution not exceeding three thousand ringgit RM3,000 for each day during which the offence continues after conviction.

Section 22	
Description	***Implication***
Officer of a Reporting Institution shall take all reasonable steps to ensure compliance with AMLATFPUAA	≤ RM1 million or ≤ 3 years imprisonment or both

- in the case of continuing offence, a further fine but < RM3K for each day or part thereof during which the offence continues to be committed.

Section 92 of the AMLATFPUAA further empowers Bank Negara Malaysia to compound, with the consent of the Public Prosecutor, any offence under the AMLATFPUAA or its regulations by accepting from the person reasonably suspected of having committed the offence such amount not exceeding 50% of the amount of the

maximum fine for that offence, including the daily fine, if any, in the case of a continuing offence.

Section 92	
Description	***Implication***
Further empowers BNM to compound in cases of continuing offence	Compound rate of ≤ 50% of the maximum fine amount

a. **Section 66E(5)** of the AMLATFPUAA provides that any institution that fails or refuses to comply with or contravenes any direction or guidelines issued to it by the relevant regulatory or supervisory authority; or discloses a direction or guideline issued to it in contravention of **section 66E(4)**, commits an offence and shall on conviction be liable to a fine not exceeding one million ringgit RM1,000,000.00.

Section 66E(5) & Section 66E(4)	
Description	***Implication***
Section 66E(5) provides that any institution that fails or refuses to comply with or contravenes any direction or guidelines issued to it by the relevant regulatory or supervisory authority or discloses a direction or guideline issued to it in contravention of **Section 66E(4)**	Liable upon conviction Compound rate <RM1 million

12. RESPONSIBILITY FOR THE POLICY

12.1 This Policy is reviewed and approved by the Board of Directors and its Audit & Compliance Committee and oversight of this Policy has been delegated to the Audit & Compliance Committee, which monitors the effectiveness of and compliance with this Policy.

12.2 The Board of Directors and the **LSK** Management team set the tone at the top providing leadership and support for the Policy and take responsibility for its effectiveness within their business units. **LSK** Management is responsible for the implementation of the Policy and all communication and training activities in relation to the Policy to ensure that those reporting to them are made aware of, and understand this Policy.

13. EFFECTIVE DATE

13.1 The Policy is approved by the Board of Directors and effective as of **1 August 2020**.

LOO HOCK LONG
Director
LSK Management Services Sdn. Bhd.
Date: 01 Aug 2020

LSK Management Services Sdn Bhd reserves the right to amend this policy and guidelines.

Appendix I

ACRONYMS

Unless otherwise defined, all words used in this Policy shall have the following and the same meaning as defined in the AMLATFPUAA:

AMLATFPUAA
Anti-Money Laundering, Anti-Terrorism Financing and Proceeds of Unlawful Activities Act 2001

AML/CFT
Anti-Money Laundering and Counter Financing of Terrorism

APG
Asia Pacific Group

BNM
Bank Negara Malaysia

BO
Beneficial Owner

CA 2016
Companies Act 2016 [Act 777]

CDD
customer due diligence

CMSA 2007
Capital Markets and Services Act 2007 [*Act 671*]

CRP
Customer Risk Profiling

DCR
Data Compliace Report

DNFBPs
Designated Non-Financial Businesses and Professions

ECDD
Enhanced Customer Due Diligence

FATF
Financial Action Task Force

FIED
Financial Intelligence and Enforcement Department

GLCs
Government-linked companies

ID
Identification Card

IPPCs
Internal policies, procedures and controls

KYC
Know Your Customer

ML/TF
Money Laundering / Terrorist Financing

NCC
National Coordination Committee

NCCT
Non-Cooperative Countries and Territories

NRA
National Risk Assessment

NBFIs
Non-Bank Financial Institutions

PEPs
Politically exposed persons (PEPs)

RIs
Reporting institutions

SRO
self-regulatory organisation

STR
suspicious transaction report

TFS
Targeted Financial Sanctions

UNSCR
United Nations Security Council Resolutions