GUIDELINES ON
ANTI-MONEY LAUNDERING AND COUNTER FINANCING OF TERRORISM (AML/CFT)

BANKING SECTOR

TABLE OF CONTENTS

PART A OVERVIEW

PART B AML/CFT REQUIREMENTS

PART A OVERVIEW

1. Introduction

1.1 Money laundering and terrorism financing (ML/TF) continues to be an on-going threat which has the potential to adversely affect the country's reputation and investment climate which may lead to economic and social consequences. The globalisation of the financial services industry and advancement in technology has posed challenges to regulators and law enforcement agencies as criminals have become more sophisticated in utilising reporting institutions to launder illicit funds and use them as conduits for ML/TF activities.

1.2 Since the formation of the National Coordination Committee to Counter Money Laundering (NCC), efforts have been undertaken to effectively enhance the Anti-Money Laundering and Counter Financing of Terrorism (AML/CFT) compliance framework of reporting institutions resulting in the introduction of the Standard Guidelines on AML/CFT and the relevant Sectoral Guidelines. While these efforts have addressed the ML/TF risks and vulnerabilities, there is a need to continuously assess the effectiveness of our AML/CFT framework to ensure that it continues to evolve in line with developments in international standards and the global environment.

1.3 Besides bringing the recommendation up to date in addressing new and emerging threats, the 2012 revision of the International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation (FATF 40 Recommendations), sought to clarify and strengthen many of its existing obligations as well as to reduce duplication of the Recommendations. One of the new Recommendations introduced is on the obligation of countries to adopt a risk-based approach in identifying, assessing and understanding the countries' ML/TF risks, which places further expectation on reporting institutions to assess and mitigate ML/TF risks.

1.4 The AML/CFT – Banking Sector Guidelines is based on the principle that reporting institutions must conduct their business in conformity with high ethical standards and be on guard against undertaking any business transaction that is or may be connected with or may facilitate ML/TF. This is aim to ensure integrity and soundness of the Labuan International Business Financial Centre (LIBFC) and Malaysian financial system are safeguarded.

2. Objective

2.1 This guidelines is formulated in accordance with the provisions of the Anti-Money Laundering and Anti-Terrorism Financing Act 2001 (AMLATFA) and the FATF 40 Recommendations and is intended to ensure that reporting institutions understand and comply with the requirements and obligations imposed on them.

3. Scope

3.1 This guidelines sets out the:

(a) obligations of reporting institutions with respect to the requirements imposed under the AMLATFA;

(b) requirements imposed on reporting institutions in implementing a comprehensive risk base approach in managing ML/TF risks; and

(c) roles of the reporting institutions' Board of Directors and Senior Management in putting in place the relevant AML/CFT measures.

4. Legal Provisions

4.1 This guidelines is issued pursuant to:

(a) Sections 13, 14, 15, 16, 17, 18, 19, 20, 66E and 83 of the AMLATFA; and

(b) Section 4B of the Labuan Financial Services Authority Act 1996 (LFSAA).

5. Applicability

5.1 This guidelines is applicable to:

(a) Reporting institutions carrying on the following activities listed in the First Schedule of the AMLATFA.

(i) Labuan banking business, Labuan investment banking business and Labuan financial business as defined under Section 86 of the Labuan Financial Services And Securities Act 2010 (LFSSA);

(ii) Islamic banking business, Labuan Islamic investment banking business and Labuan Islamic financial business as defined under Section 60 of the Labuan Islamic Financial Services And Securities Act 2010 (LIFSSA); and

(iii) any other persons as specified by the Labuan FSA.

(b) branches and subsidiaries of reporting institutions referred to in Paragraph 5.1(a) which carries on any activity listed in the First Schedule of the AMLATFA; and

(c) all products and services offered by reporting institutions referred to in Paragraph 5.1(a).

5.2 The requirement of this AML/CFT – Banking Sector is applicable to Labuan licensees operating as foreign branches, subsidiaries and offices, wherein they are required to comply with the policies and procedures as implemented by their head office. However, if policies and procedures as implemented by their head office are inconsistent with the requirements of this document or less stringent than stated on this document, the requirements prescribed herein on this document shall prevail.

5.3 Where the institutions are subject to more than one AML/CFT matters issued pursuant to Section 83 of the AMLATFA, the more stringent requirements shall apply.

6. Effective Date

6.1 This AML/CFT – Banking Sector Guidelines will be effective from 30 December 2013.

7. Compliance Date

7.1 Compliance to the requirements outlined in this guidelines shall take effect immediately, unless otherwise specified by the Labuan FSA.

8. Guidelines Superseded

8.1 This guidelines supersedes:

(a) The Standard Guidelines on Anti-Money Laundering and Counter Financing of Terrorism (AML/CFT) issued on 4 January 2007; and

(b) The Anti-Money Laundering and Counter Financing of Terrorism (AML/CFT) Sectoral Guidelines 1 for Offshore Financial Institutions Licensed and Registered under Offshore Banking Act 1990 issued on 4 January 2007.

9. Relationship with Existing Policies

9.1 This guidelines shall be read together with other relevant policy documents, circulars and directives issued by Labuan FSA relating to compliance with AML/CFT requirements.

10. Definition and Interpretation

10.1 The terms and expression used in this document shall have the same meanings assigned to it in the AMLATFA, LFSSA, and LIFSSA as the case may be, unless otherwise defined in this document.

10.2 For the purpose of this Guidelines on AML/CFT – Banking Sector, the following definitions and interpretations apply:

"accurate"	Refers to information that has been verified for accuracy.
"Bank / BNM "	Refers to Bank Negara Malaysia.
"beneficial owner"	Refers to any natural person(s) who ultimately owns or controls a customer and/or the natural person on whose

	behalf a transaction is being conducted. It also includes those natural persons who exercise ultimate effective control over a legal person or arrangement. Reference to "ultimately owns or control" or "ultimate effective control" refers to situations in which ownership or control is exercised through a chain of ownership or by means of control other than direct control.
"beneficiary"	Depending on the context: In trust law, a beneficiary refers to the person or persons who are entitled to the benefit of any trust arrangement. A beneficiary can be a natural or legal person or arrangement. All trusts (other than charitable or statutory permitted non-charitable trusts) are required to have ascertainable beneficiaries. While trusts must always have some ultimately ascertainable beneficiary, trusts may have no defined existing beneficiaries but only objects of a power until some person becomes entitled as beneficiary to income or capital on the expiry of a defined period, known as the accumulation period. This period is normally co-extensive with the trust perpetuity period which is usually referred to in the trust deed as the trust period. In wire transfer, refers to the natural or legal person or legal arrangement identified by the originator as the receiver of the requested wire transfer. In clubs, societies and charities, refers to the natural persons, or groups of natural persons who receive charitable, humanitarian or other types of services of the clubs, societies and charities.

"beneficiary account"	Includes trust accounts, nominees accounts, fiduciary accounts, accounts opened for companies with nominee shareholders, accounts for mutual fund and fund managers, accounts for personal asset holding vehicles, pooled accounts, accounts opened by professional third parties and other relevant accounts.
"beneficiary institutions"	Refers to the institution which receives the wire transfer from the ordering institution directly or through an intermediary institution and makes the fund available to the beneficiary.
"Board of Directors"	Refers to a governing body or a group of directors. A director includes any person who occupies a position of a director, however styled, of a body corporate or unincorporated. (a) a corporation, the same meaning assigned to it in Subsection 2(1) of the Labuan Companies Act 1990 (LCA); (b) a sole proprietorship, means the sole proprietor; and (c) a partnership, means the senior or equity partners.
"Core Principles"	Refers to the Core Principles for Effective Banking Supervision issued by the Basel Committee on Banking Supervision, Objectives and Principles for Securities Regulation issued by the International Organisation of Securities Commissions and the Insurance Core Principle issued by the International Association of Insurance Supervisors.
"correspondent bank"	Refers to the reporting institution in Malaysia that provides or intends to provide correspondent banking services.
"cover payment"	Refers to a wire transfer that combines a payment message sent directly by the ordering reporting institution to the beneficiary institution where the routing of the funding instruction (the cover) are carried out or performed through one or more intermediary institutions.

"cross-border wire transfer"	Refers to any wire transfer where the ordering reporting institution and beneficiary institutions are located in different countries. This term also refers to any chain of wire transfer in which at least one of the institutions involved is located in a different country.
"customer"	Refers to both account holder and non-account holder, and the term also refers to a client.
"customer due diligence"	Refers to any measures undertaken pursuant to section 16 of the AMLATFA.
"domestic wire transfers"	Refers to any wire transfer where the ordering institution and beneficiary institutions are located in Malaysia. This term therefore refers to any chain of wire transfer that takes place entirely within the borders of Malaysia, even though the system used to transfer the payment message may be located outside Malaysia.
"family members"	Refers to legal spouse, children (including legally adopted or step child), parents, siblings, in-laws, or relatives that might benefit from the relationship.
"financial group"	Refers to a group that consists of a holding company incorporated in Malaysia or of any other type of legal person exercising control and coordinating functions over the rest of the group for the application of group supervision under the Core Principles, together with branches and/or subsidiaries that are subject to AML/CFT policies and procedures at the group level.
"Government-linked company"	Refers to a corporate entity that may be private or public (listed on a stock exchange) where the government owns an effective controlling interest, or is owned by any corporate entity where the government is a shareholder.
"higher risk"	Refers to circumstances where the reporting institutions assess the ML/TF risks as higher, taking into consideration, and not limited to the following factors: (a) Customer risk factors:

	• the business relationship is conducted in unusual circumstances (e.g. significant unexplained geographic distance between the reporting institution and the customer); • non-resident customer; • legal persons or arrangements that are personal asset-holding vehicles; • companies that have nominee shareholders or shares in bearer form; • business that are cash-intensive; • the ownership structure of the company appears unusual or excessively complex given the nature of the company's business; • high net worth individuals; • persons from locations known for their high rates of crime (e.g. drug producing, trafficking, smuggling); • businesses or activities identified by the FATF as having higher risk for ML/TF; • legal arrangements that are complex (e.g. trust, nominee); and • persons who match the red flags criteria of the reporting institutions. (b) Country or geographic risk factors: • countries having inadequate AML/CFT systems; • countries subject to sanctions, embargos or similar measures issued by, for example, the United Nations; • countries having significant levels of corruption or other criminal activity; and • countries or geographic areas identified as providing funding or support for terrorist activities, or that have designated terrorist organisations operating within their country.

	In identifying countries and geographic risk factors, reporting institutions may refer, to credible sources such as mutual evaluation reports, detailed assessment reports, follow up reports and other relevant reports published by international organisations such as the United Nations. (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 fit into the person's nature of business and risk profile; and • payment received from unknown or un-associated third parties.
"higher risk countries"	Refers to countries that are listed by FATF or the Government of Malaysia with either on-going or substantial ML/TF risks or strategic AML/CFT deficiencies that pose a risk to the international financial system.
"home supervisor"	Refers to the Bank Negara Malaysia, Securities Commission and Labuan Financial Services Authority and any other person as defined under Section 28A of Labuan Financial Services Authority Act 1996 (LFSAA).
"intermediary institution"	Refers to the institution in a serial or cover payment chain that receives and transmits a wire transfer on behalf of the ordering institution and the beneficiary institution, or another intermediary institution.
"international organisations"	Refers to entities established by formal political agreements between their member States that have the status of international treaties; their existence is recognised by law in their member countries; and they are not treated as residential institutional units of the countries in which they are located. Examples of international organisations

	include the following: (a) United Nations and its affiliated international organisations; (b) regional international organisations such as the Association of Southeast Asian Nations, the Council of Europe, institutions of the European Union, the Organisation for Security and Co-operation in Europe and the Organization of American States; (c) military international organisations such as the North Atlantic Treaty Organization; and (d) economic organisations such as the World Trade Organization.
"Labuan FSA"	Refers to Labuan Financial Services Authority.
"LIBFC"	Refers to the Labuan International Business and Financial Centre.
"legal arrangement"	Refers to express trusts or other similar legal arrangements.
"legal person"	Refers to any entities other than natural persons that can establish a permanent customer relationship with a reporting institution or otherwise own property. This includes companies, bodies corporate, foundations, partnerships, or associations and other similar entities.
"money services business"	Refers to any or all remittance business.
"ordering institution"	Refers to the institution which initiates the wire transfer and transfers the funds upon receiving the request for a wire transfer on behalf of the originator.
"originator"	Refers to the account holder who allows the wire transfer from that account, or where there is no account, the natural or legal person that places the order with the ordering reporting institution to perform the wire transfer.
"payable through account"	Refers to correspondent accounts that are used directly by third party to transact business on their own behalf.

"person"	Includes a body of persons, corporate or unincorporated.
"politically exposed persons (PEPs)"	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 of 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 of government, senior politicians, senior 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 foreign countries.
"respondent bank"	Refers to bank or reporting institution outside Malaysia to which correspondent banking services in Malaysia are provided.
"satisfied"	Where reference is made to a reporting institution being "satisfied" as to a matter, that reporting institution must be able to justify its assessment to the supervisory authority.
"senior management"	Refers to any person(s) having authority and responsibility for planning, directing or controlling the activities including the management and administration of a reporting institution (Labuan Entity) including Principal Officer.

“serial payment”	Refers to a direct sequential chain of payment where the wire transfer and accompanying payment message travel together from the ordering reporting institution to the beneficiary reporting institution directly or through one or more intermediary reporting institutions (e.g. correspondent banks).
“shell bank”	Refers to a bank that has no physical presence in the country in which it is incorporated and licensed, and which is unaffiliated with a regulated financial group that is subject to effective consolidated supervision. Physical presence means meaningful mind and management located within a country. The existence simply of a local agent or low level staff does not constitute physical presence.
“straight - through processing”	Refers to payment transactions that are conducted electronically without the need for manual intervention.
“third parties”	Refers to reporting institutions that are supervised and monitored by a relevant competent authority and that meet the requirements under Paragraph 20 on Reliance of Third Parties, namely persons or businesses who are relied upon by the reporting institution to conduct the customer due diligence process. Reliance on third parties often occurs through introductions made by another member of the same financial group or by another financial institution. This definition does not include outsourcing or agency relationships because the outsourced person, service provider or agent is regarded as synonymous with the reporting institution.
“unique transaction reference number”	Refers to a combination of letters, numbers, or symbols, determined by the payment service provider, in accordance

	with the protocols of the payment and settlement system or messaging system used for the wire transfer.
"wire transfer"	Refers to any transaction carried out on behalf of an originator through a reporting institution by electronic means with a view to making an amount of funds available to a beneficiary person at a beneficiary institution, irrespective of whether the originator and the beneficiary are the same person.

PART B AML/CFT REQUIREMENTS

11. Applicability to Foreign Branches, Subsidiaries and Offices of Labuan Home-Grown Entities

11.1 Reporting institutions are required to closely monitor the reporting institution's foreign branches, subsidiaries and offices operating in jurisdiction with inadequate AML/CFT laws and regulations as highlighted by the FATF or the Government of Malaysia.

11.2 Reporting institutions are required to ensure that their foreign branches, subsidiaries and offices apply AML/CFT measures consistent with the home country requirements. Where the minimum AML/CFT requirements of the host country are less stringent than those of the home country, the reporting institution must apply the home country requirements, to the extent that host country laws and regulations permit.

11.3 If the host country does not permit the proper implementation of AML/CFT measures consistent with the requirement in Malaysia, the reporting institutions and financial group are required to apply appropriate additional measures to manage the ML/TF risks, and report to Labuan FSA or any of their supervisors in Malaysia on the AML/CFT gaps and additional measures implemented to manage the ML/TF risks arising from the identified gaps.

11.4 In addition, the reporting institution may consider ceasing the operations of the said branch, subsidiary or offices that unable to put in place the necessary mitigating control as required under Paragraph 11.3.

12. Risk-Based Approach Application

12.1 Risk Management Functions

12.1.1 In the context of "Risk-Based Approach", the intensity and extensiveness of risk management functions shall be proportionate to the nature, scale and complexity of the reporting institution's activities and ML/TF risk profile.

12.1.2 The reporting institution's AML/CFT risk management function must be aligned and integrated with their overall risk management control function.

12.2 Risk Assessment

12.2.1 Reporting institutions are required to take appropriate steps to identify, assess and understand their ML/TF risks in relation to their customers, countries or geographical areas and products, services, transactions or delivery channels.

12.2.2 In assessing ML/TF risks, reporting institutions are required to establish internal policies and procedures by having the following processes:

(a) documenting their risk assessments and findings;

(b) considering all the relevant risk factors before determining what is the level of overall risk and the appropriate level and type of mitigation to be applied;

(c) keeping the assessment up-to-date through a periodic review; and

(d) having appropriate mechanisms to provide risk assessment information to the supervisory authority.

12.2.3 Reporting institutions are required to conduct additional assessment as and when required by Labuan FSA and other supervisory authorities.

12.2.4 Reporting institutions may be guided by the results of the National Risk Assessment issued by Bank Negara Malaysia or Labuan FSA in conducting their own risk assessments.

12.3 Risk Control and Mitigation

12.3.1 Reporting institutions are required to:

(a) have policies, controls and procedures to manage and mitigate ML/TF risks that have been identified;

(b) monitor the implementation of those policies, controls, procedures and to enhance them if necessary; and

(c) take enhanced measures to manage and mitigate the risks where higher risks are identified.

12.3.2 Reporting institutions shall conduct independent control testing on their policies, controls and procedures for the purpose of monitoring the implementation thereof under Paragraph 12.3.1(b).

12.4 Risk Profiling

12.4.1 Reporting institutions are required to conduct risk profiling on their customers.

12.4.2 A risk profile must consider the following factors:

(a) customer risk (e.g. resident or non-resident, type of customers, occasional or one-off, legal person structure, types of PEP, types of occupation);

(b) geographical location of business or country of origin of customers;

(c) products, services, transactions or delivery channels (e.g. cash-based, face-to-face or non face-to-face, cross-border); and

(d) any other information suggesting that the customer is of higher risk.

12.4.3 The risk control and mitigation measures implemented by reporting institutions shall commensurate with the risk profile of a particular customer or type of customer.

12.4.4 Upon the initial acceptance of the customer, reporting institutions are required to regularly review and update the customer's risk profile based on their level of ML/TF risks.

12.5 **AML/CFT Risk Reporting**

12.5.1 Reporting institutions shall provide a timely reporting of the risk assessment, ML/TF risk profile and the effectiveness of risk control and mitigation measures to the Board and senior management. The frequency of reporting shall commensurate with the level of risks involved and the reporting institution's operating environment.

12.5.2 The report referred to under Paragraph 12.5.1 may include, the following:

(a) results of AML/CFT monitoring activities carried out by the reporting institution such as level of the reporting institution's exposure to ML/TF risks, break-down of ML/TF risk exposures based on key activities or customer segments, trends of suspicious transaction reports and trends of orders received from law enforcement agencies;

(b) details of recent significant risk events, that occur either internally or externally, modus operandi and its impact or potential impact to the reporting institution; and

(c) recent developments in AML/CFT laws and regulations, and its implications to the reporting institution.

13. Customer Due Diligence (CDD)

13.1 When CDD is required

13.1.1 Reporting institutions are required to conduct CDD on the customer and the person conducting the transaction, when:

(a) establishing business relations;

(b) providing wire transfer services;

(c) it has any suspicion of ML/TF, regardless of any amount; or

(d) it has any doubt about the veracity or adequacy of previously obtained information.

13.2 What is required

13.2.1 The CDD measures undertaken by reporting institutions shall comprise, at least the following:

(a) identify the customer and verify the customer's identity using reliable, independent source documents, data or information;

(b) verify that any person purporting to act on behalf of the customer is so authorised, and identify and verify the identity of that person;

(c) identify the beneficial owner and take reasonable measures to verify the identity of the beneficial owner, using the relevant information or data obtained from a reliable source, such that the reporting institution is satisfied that it knows who the beneficial owner is; and

(d) understand and, where relevant, obtain information on the purpose and intended nature of the business relationship.

13.2.2 In conducting CDD, reporting institutions are required to comply with the requirements on combating the financing of terrorism under Paragraph 29 on Combating the Financing of Terrorism.

13.3 Timing of Verification

13.3.1 Reporting institutions are required to verify the identity of the customer and beneficial owner before, or during, the course of establishing a business relationship or conducting a transaction for an occasional customer.

13.3.2 In certain circumstances where the ML/TF risks are assessed as low and verification is not possible at the point of establishing the business relationship, the reporting institution may complete verification after the establishment of the business relationship to allow some flexibilities for its customer and beneficial owner to furnish the relevant documents.

13.3.3 Where delayed verification applies, the following conditions must be satisfied:

(a) this occurs as soon as reasonably practicable;

(b) the delay is essential so as not to interrupt the reporting institution's normal conduct of business;

(c) the ML/TF risks are effectively managed; and

(d) there is no suspicion of ML/TF risks.

13.3.4 The term "reasonably practicable" under Paragraph 13.3.3(a) shall not be later than ten working days or any other period as may be specified by Labuan FSA.

13.3.5 Reporting institutions are required to adopt risk management procedures relating to the conditions under which the customer may utilise the business relationship prior to

verification, and procedures to mitigate or address the risk of delayed verification.

13.3.6 The measures that reporting institutions may take to manage such risks of delayed verification may include limiting the number, types and/or amount of transactions that can be performed.

13.4 Specific CDD Measures

Individual Customer and Beneficial Owner

13.4.1 In conducting CDD on an individual customer and beneficial owner, the reporting institution is required to obtain at least the following information:

(a) full name;
(b) National Registration Identity Card (NRIC) number or passport number or reference number of any other official documents bearing the photograph of the customer or beneficial owner;
(c) residential and mailing address;
(d) date of birth;
(e) nationality;
(f) occupation type;
(g) name of employer or nature of self-employment/nature of business;
(h) purpose of transaction;
(i) source of wealth (i.e. if the income does not match with the occupation); and
(j) contact number (home, office or mobile).

13.4.2 Reporting institutions can accept any other official documents bearing the photograph of the customer and beneficial owner under Paragraph 13.4.1(b) provided that the reporting institution can be satisfied with the authenticity of the documents which contain the necessary required information.

13.4.3 Reporting institutions shall verify the documents referred to Paragraph 13.4.1(b) by requiring the customer or beneficial owner to furnish the original and make a copy of the said document. However, where biometric identification method is used, verification is deemed to be satisfied.

13.4.4 Where there is any doubt, the reporting institutions are required to request the customer and beneficial owner to produce other supporting official identification documents bearing their photographs, issued by an official authority or an international organisation, to enable their identity to be ascertained and verified.

Legal Persons

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

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

(a) name, legal form and proof of existence, such as Memorandum/Article/Certificate of Incorporation/ Partnership (certified true copies/ duly notarised copies, may be accepted) or any other reliable references to verify the identity of the customer;

(b) 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

(c) the address of the registered office and, if different, from the principal place of business.

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

(a) The identity of the natural person(s) (if any) who ultimately has a controlling ownership interest in a legal person including but not limited to the following:

(i) identification document of Directors/ Shareholders with equity interest of more than twenty five percent/Partners (certified true copy/duly notarised copies or the latest Form 24 and Form 49 as prescribed by the Companies Commission of Malaysia or Form 13 and Form 25 as prescribed by the Registrar of Companies, Labuan FSA or foreign incorporation, or any other equivalent documents for other types of legal person are acceptable);

(ii) authorisation for any person to represent the company or business either by means of a letter of authority or directors' resolution; and

(iii) relevant documents such as NRIC for Malaysian/permanent resident or passport for foreigner, to identify the identity of the person authorised to represent the company or business in its dealing with the reporting institution;

(b) to the extent that there is doubt under as to whether the person(s) with the controlling ownership interest is the beneficial owner(s) referred to in Paragraph 13.4.7(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 13.4.7(a) or (b) above, the identity of the relevant natural person who holds the position of senior management.

13.4.8 Where there is any doubt as to the identity of persons referred to under Paragraphs 13.4.6 and Paragraphs 13.4.7, the reporting institution shall:

(a) 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

(b) verify the authenticity of the information provided by such person with the Labuan FSA, Companies Commission of Malaysia or any other relevant agencies.

13.4.9 Reporting institutions are exempted from obtaining a copy of the Memorandum and Articles of Association or Certificate of Incorporation and exempted from identifying and verifying the directors and shareholders of the legal person which fall under the following categories:

(a) public listed companies or corporations listed in Labuan International Financial Exchange and Bursa Malaysia;

(b) foreign public listed companies:

i. listed in recognised exchanges; and

ii. not listed in higher risk countries;

(c) foreign financial institutions that are not from higher risk countries;

(d) government-linked companies in Malaysia;

(e) state-owned corporations and companies in Malaysia;

(f) an authorised person, an operator of a designated payment system, a registered person, as the case may be, under the Financial Services Act 2013 (FSA) and the Islamic Financial Services Act 2013 (IFSA);

(g) persons licensed or registered under the Capital Markets and Services Act 2007;

(h) licensed entities under the LFSSA and LIFSSA;

(i) prescribed institutions under the Development Financial Institutions Act 2002; or

(j) foreign financial institutions that are not from higher risk countries.

13.4.10 Reporting institutions may refer to the Directives in relation to Recognised Stock Exchanges (R/R6 of 2012) issued by Bursa Malaysia in determining foreign exchanges that are recognised.

Legal Arrangements

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

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

(a) name, legal form and proof of existence, or any reliable references to verify the identity of the customer;

(b) the powers that regulate and bind the customer, as well as the names of relevant persons having a senior management position; and

(c) the address of the registered office, and if different, a principal place of business.

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

(a) 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

(b) for other types of legal arrangements, the identity of persons in equivalent or similar positions.

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

13.4.15 Where reliance is placed on third parties under Paragraph 13.4.14, reporting institutions are required to comply with Paragraph 20 on Reliance on Third Parties.

Clubs, Societies and Charities

13.4.16 In conducting CDD for clubs, societies or charities, reporting institutions shall require the customers to furnish the relevant identification and constituent documents (or other similar documents) including certificate of registration and the identification and verification of the office bearer or any person authorised to represent the club, society or charity, as the case may be.

13.4.17 Reporting institutions are required to take reasonable measures to identify and verify the beneficial owners of the customers.

Counter-Party

13.4.18 Where the reporting institution establishes a relationship with a counter-party, the reporting institution must be satisfied that the counter-party is properly regulated and supervised.

13.4.19 Reporting institutions are required to ensure that the counter-party's CDD process is adequate and the mechanism to identify and verify its customers is reliable.

Beneficiary account

13.4.20 In the case of beneficiary accounts, reporting institutions are required to perform CDD on the beneficiary and the person acting on behalf of the beneficiary, on an individual basis.

13.4.21 In the event that identification on an individual basis cannot be performed, for example where the interests of a group of beneficiaries are pooled together without specific allocation

to known individuals, the reporting institution is required to satisfy itself that the funds in the account are not maintained in the interest of other parties which have no relationship with the account.

13.4.22 Reporting institutions may rely on a third party when they are unable to conduct CDD on the clients of professionals, such as legal firms or accountants acting on behalf of their clients.

13.4.23 Where reliance is placed on third party under Paragraph 13.4.22, reporting institutions are required to comply with Paragraph 20 on Reliance on Third Parties.

13.4.24 In the event where the person acting on behalf of the beneficiary is unable or refuses to provide the information on the identity of the beneficiaries or written undertaking (where applicable), reporting institutions are to comply with Paragraph 23 on Failure to Satisfactorily Complete CDD.

13.5 Enhanced CDD

13.5.1 Reporting institutions are required to perform enhanced CDD where the ML/TF risks are assessed as higher risk. An enhanced CDD, shall include at least, the following:

(a) obtaining CDD information under Paragraph 13.4;

(b) obtaining additional information on the customer and beneficial owner (e.g. volume of assets; other information from public database);

(c) inquiring on the source of wealth or source of funds. In the case of PEPs, both sources must be obtained; and

(d) obtaining approval from the senior management of the reporting institution before establishing (or continuing, for existing customer) such business relationship with the customer. In the case of PEPs, senior management refers

to senior management at the head office or any other person(s)[1] referred by the head office.

13.5.2 In addition to Paragraph 13.5.1, reporting institutions may also consider the following enhanced CDD measures in line with the ML/TF risks identified:

(a) obtaining additional information on the intended level and nature of the business relationship;

(b) updating more regularly the identification data of customer and beneficial owner;

(c) inquiring on the reasons for intended or performed transactions; and

(d) requiring the first payment to be carried out through an account in the customer's name with a bank subject to similar CDD standards.

13.6 On-Going Due Diligence

13.6.1 Reporting institutions are required to conduct on-going due diligence on the business relationship with its customers. Such measures shall include:

(a) scrutinising transactions undertaken throughout the course of that relationship to ensure that the transactions being conducted are consistent with the reporting institution's knowledge of the customer, their 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 relevant, by undertaking reviews of existing records particularly for higher risk customers.

[1] Officers delegated by the senior management who have primary or significant responsibility for the management and performance of the business activities of the Labuan Entity including the Principal Officer.

13.6.2 In conducting on-going due diligence, reporting institutions may take into consideration the economic background and purpose of any transaction or business relationship which:

(a) appears unusual;

(b) is inconsistent with the expected type of activity and business model when compared to the volume of transaction;

(c) does not have any apparent economic purpose; or

(d) casts doubt about on the legality of such transaction especially with regard to complex and large transactions or involving higher risk customers.

13.6.3 The frequency of the on-going due diligence or enhanced on-going due diligence, as the case may be, shall commensurate with the level of ML/TF risks posed by the customer based on the risk profiles and nature of transactions.

13.6.4 Reporting institutions are required to increase the number and timing of controls applied, and to select patterns of transactions that need further examination, when conducting enhanced on-going due diligence.

13.7 **Existing Customer – Materiality and Risk**

13.7.1 Reporting institutions are required to apply CDD requirements to existing customer on the basis of materiality and risk.

13.7.2 Reporting institutions are required to conduct CDD on such existing relationships at appropriate times, taking into account whether and when CDD measures have previously been undertaken and the adequacy of data obtained.

13.7.3 In assessing materiality and risk on the existing customer under Paragraph 13.7.1, reporting institutions shall consider the following circumstances:

(a) the nature and circumstances surrounding the transaction including the significance of the transaction;

(b) any material change in the way the account, transaction or business relationship is operated; or

(c) insufficient information held on the customer or change in customer's information.

14. Politically Exposed Persons (PEPs)

14.1 General

14.1.1 The requirements set out under this paragraph are applicable to family members or close associates of all types of PEPs.

14.2 Foreign PEPs

14.2.1 Reporting institutions are required to put in place a risk management system to determine whether a customer or a beneficial owner is a foreign PEP.

14.2.2 Upon determination that a customer or a beneficial owner is a foreign PEP, the requirements of enhanced CDD as set out under Paragraph 13.5 must be conducted.

14.3 Domestic PEPs or Person entrusted with a prominent function by an international organization.

14.3.1 Reporting institutions are required to take reasonable measure to determine whether a customer or beneficial owner is a domestic PEP or a person entrusted with a prominent function by an international organisation.

14.3.2 If the customer or beneficial owner is assessed as a domestic PEP or a person entrusted with a prominent function by an international organisation, reporting institutions are required to assess the level of ML/TF risks posed by business relationship with the domestic PEP or person entrusted with a prominent function by an international organisation.

14.3.3 The assessment of the ML/TF risks, as specified under Paragraph 14.3.2, shall take into accounts the profile of the customer under Paragraph 12.4.2 on Risk Profiling.

14.3.4 The requirements of enhanced CDD as set out under Paragraph 13.5 must be conducted in respect of domestic PEPs or person entrusted with a prominent function by an international organisation which are assessed as higher risk.

14.3.5 Reporting institutions may apply CDD measures similar to other customer for domestic PEPs or person entrusted with a prominent function by an international organisation if the reporting institution is satisfied that the domestic PEPs or person entrusted with a prominent function by an international organisation are not assessed as higher risk.

15. New Products and Business Practices

15.1 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.

15.2 Reporting institutions are required to:

(a) undertake the risk assessment prior to the launch or use of such products, practices and technologies; and

(b) take appropriate measures to manage and mitigate the risks.

16. Other Products

Private Banking

16.1 Reporting institutions are required to conduct enhanced CDD where the ML/TF risks of private banking customers are assessed as higher risk.

17. Shell Banks

17.1 Reporting institutions shall not establish or have any business relationship with shell banks.

18. Wire transfer

General

18.1 The requirements under this Paragraph are applicable to cross-border wire transfers and domestic wire transfers including serial payments and cover payments.

18.2 Reporting institutions are required to observe the requirements on combating the financing of terrorism under Paragraph 29 in carrying out wire transfer.

18.3 Reporting institutions shall not execute the wire transfer if it does not comply with the requirements specified in this paragraph.

18.4 Reporting institutions are required to maintain all originator and beneficiary information collected in accordance with record keeping requirements under Paragraph 26.

Ordering Institutions

Cross-border wire transfers

18.5 Reporting institutions which are ordering institutions are required to ensure that the message or payment instruction for all cross-border wire transfers are accompanied by the following:

(a) Required and accurate originator information pertaining to:

(i) name;

(ii) NRIC or passport number;

(iii) account number (or a unique reference number if there is no account number) which permits traceability of the transaction;

(iv) address (or in lieu of the address, date and place of birth); and

(v) purpose of transaction;

(b) Required beneficiary information pertaining to:

(i) name; and

(ii) account number (or a unique reference number if there is no account number), which permits traceability of the transaction.

18.6 Where several individual cross-border wire transfers from a single originator are bundled in a batch file for transmission to beneficiaries, the batch file shall contain required and accurate originator information, and full beneficiary information, that is fully traceable within the beneficiary country; and ordering institutions are required to include the originator's account number or unique transaction reference number.

Domestic wire transfers

18.7 Ordering reporting institutions are required to ensure that the information accompanying the wire transfer includes originator information as indicated for cross-border wire transfers, unless this information can be made available to the beneficiary reporting institution and relevant authorities by other means.

18.8 Where the information accompanying the domestic wire transfer can be made available to the beneficiary institution and relevant authorities by other means, the ordering institution shall include only the originator's account number or if there is no account number, a unique identifier, within the message or payment form, provided that this account number or unique identifier will permit the transaction to be traced back to the originator or the beneficiary. Ordering institutions are required to provide the information within three working days of receiving the request either from the beneficiary institution or from the relevant authorities and must provide the information to law enforcement agencies immediately upon request.

Intermediary Institutions

18.9 For cross-border wire transfers, intermediary institutions are required to retain all originator and beneficiary information that accompanies a wire transfer.

18.10 Where the required originator or beneficiary information accompanying a cross-border wire transfer cannot be transmitted due to technical limitations, intermediary institutions are required to keep a record in accordance with record keeping requirements under Paragraph 26.

18.11 Intermediary institutions are required to take reasonable measures, which are consistent with straight-through processing, to identify cross-border wire transfers that lack the required originator information or required beneficiary information.

18.12 Intermediary institutions are required to have effective risk-based policies and procedures for determining:

(a) when to execute, reject, or suspend a wire transfer lacking required originator or required beneficiary information; and

(b) the appropriate follow-up action.

Beneficiary Institutions

18.13 Beneficiary institutions are required to take reasonable measures, including post-event monitoring or real-time monitoring where feasible, to identify cross-border wire transfers that lack required originator information or required beneficiary information.

18.14 For cross-border wire transfers, beneficiary institutions are required to verify the identity of the beneficiary, if the identity has not been previously verified, and maintain this information in accordance with record keeping requirements under Paragraph 26.

18.15 Beneficiary institutions are required to have effective risk-based policies and procedures for determining:

(a) when to execute, reject, or suspend a wire transfer lacking required originator or required beneficiary information; and

(b) the appropriate follow-up action.

19. Correspondent Banking

19.1 Reporting institutions providing correspondent banking services to respondent banks are required to take the necessary measures to ensure that it is not exposed to the threat of ML/TF through the accounts of the respondent banks such as being used by shell banks.

19.2 In relation to cross-border correspondent banking and other similar relationships, reporting institutions are required to:

(a) gather sufficient information about a respondent bank to understand fully the nature of the respondent's bank's business, and to determine from publicly available information the reputation of the respondent bank and the quality of supervision, including whether it has been subject to a ML/TF investigation or regulatory action;

(b) assess the respondent bank's AML/CFT controls having regard to AML/CFT measures of the country or jurisdiction in which the respondent bank operates;

(c) obtain approval from the senior management [2] prior to establishing new correspondent banking relationships; and

(d) clearly understand the respective AML/CFT responsibilities of each institution.

[2] Refers to any person(s) having authority and responsibility for planning, directing or controlling the activities including the management and administration of a reporting institution (Labuan Entity) including Principal Officer.

19.3 In relation to “payable-through accounts”, reporting institutions are required to satisfy themselves that the respondent bank:

(a) has performed CDD obligations on its customers that have direct access to the accounts of the reporting institution; and

(b) is able to provide relevant CDD information to the reporting institution upon request.

19.4 Reporting institutions shall not enter into, or continue, correspondent banking relationships with shell banks. Reporting institutions are required to satisfy themselves that respondent banks do not permit their accounts to be used by shell banks.

19.5 Reporting institutions are required to pay special attention to correspondent banking relationship with respondent banks from countries highlighted by the FATF or Government of Malaysia as insufficiently implementing the internationally accepted AML/CFT measures.

20. Reliance on Third Parties

Customer Due Diligence

20.1 Reporting institutions may rely on third parties to conduct CDD or to introduce business.

20.2 The ultimate responsibility and accountability of CDD measures shall remain with the reporting institution relying on the third parties.

20.3 Reporting institutions shall have in place internal policies and procedures to mitigate the risks when relying on third parties, including those from foreign jurisdictions that have been identified as having strategic AML/CFT deficiencies that pose a ML/TF risk to the international financial system.

20.4 Reporting institutions are prohibited from relying on third parties located in the higher risk countries that have been identified as having on-going or substantial ML/TF risks.

20.5 The relationship between reporting institutions and their third parties relied upon by the reporting institutions to conduct CDD shall be governed by an arrangement that clearly specifies the rights, responsibilities and expectations of all parties. At the minimum, reporting institutions must be satisfied that the third party:

(a) can obtain immediately the necessary information concerning CDD as required under Paragraph 13.4;

(b) has an adequate CDD process;

(c) has measures in place for record keeping requirements;

(d) can provide the CDD information and make copies of the relevant documentation immediately upon request; and

(e) is properly regulated and supervised by the respective authorities.

20.6 Reporting institutions may obtain an attestation from the third party to satisfy themselves that the requirements in Paragraph 20.5 have been met.

20.7 Reporting institutions may obtain written confirmation from the third party that they have conducted CDD on the customer or beneficial owner as the case may be, in accordance with Paragraph 13.

20.8 The requirements under Paragraphs 20.1, 20.3 and 20.5 may be fulfilled if the reporting institution relies on a third party that is part of the same financial group subject to the following conditions:

(a) the group applies CDD and record keeping requirements and AML/CFT programmes in line with the requirements in this document;

(b) the implementation of those CDD and record keeping requirements and AML/CFT programmes are supervised at a group level by a competent authority; and

(c) any higher country risk is adequately mitigated by the financial group's AML/CFT policies.

20.9 Reporting institutions are prohibited from relying on a third party located in the 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.

On-going Due Diligence

20.10 Reporting institutions shall not rely on third parties to conduct on-going due diligence of its customers.

21. Non Face-to-Face Business Relationship

21.1 Reporting institutions may establish non face-to-face business relationships with its customers.

21.2 Reporting institutions may obtain an attestation from the third party to satisfy themselves that the requirements in Paragraph 20.5 have been met.

21.3 Reporting institutions are required to be vigilant in establishing and conducting business relationships via information communication technology.

21.4 Reporting institutions are required to establish appropriate measures for identification and verification of customer's identity that shall be as effective as that for face-to-face customer and implement monitoring and reporting mechanisms to identify potential ML/TF activities.

21.5 Reporting institutions may use the following measures to verify the identity of non face-to-face customer such as:

(a) requesting additional documents to complement those which are required for face-to-face customer;

(b) developing independent contact with the customer; or

(c) verifying customer information against any database maintained by the authorities.

22. Higher Risk Countries

22.1 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 on-going or substantial ML/TF risks.

22.2 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.

22.3 In addition to the enhanced CDD requirement under Paragraph 22.1 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:

(a) limiting business relationship or financial transactions with identified countries or persons located in the country concerned;

(b) review and amend, or if necessary terminate, correspondent banking relationships with financial institutions in the country concerned;

(c) 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;

(d) submit a report with a 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 also to Supervision and Enforcement Department, Labuan FSA on an annual basis; and

(e) conduct any other measures as specified by Labuan FSA.

23. Failure to Satisfactorily Complete CDD

23.1 Reporting institutions shall not open the account, commence business relations or perform any transaction in relation to a potential customer or shall terminate business relations in the case of an existing customer, if the reporting institution is unable to comply with the CDD requirements.

23.2 In the event of failure to comply with the CDD requirements, reporting institutions must consider lodging a suspicious transaction report to under Paragraph 28.

24. Management Information System

24.1 Reporting institutions must have in place an adequate management information system (MIS), either electronically or manually, to complement its CDD process. The MIS is required to provide the reporting institution with timely information on a regular basis to enable the reporting institution to detect irregularity and/or any suspicious activity.

24.2 The MIS shall commensurate with the nature, scale and complexity of the reporting institution's activities and ML/TF risk profile.

24.3 The MIS shall include, at a minimum, information on multiple transactions over a certain period, large transactions, anomaly in transaction patterns, customer's risk profile and transactions exceeding any internally specified threshold.

24.4 The MIS shall be able to aggregate customer's transactions from multiple accounts and/or from different systems.

24.5 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.

25. Financial Group (Labuan Home Grown Entities)

25.1 A parent company incorporated in Labuan is required to implement group-wide programme against ML/TF which is required to be applicable, and appropriate to, all branches and subsidiaries of the group. These shall include the following measures:

a) framework for AML/CFT Compliance programme at the group level;

b) appoint a group compliance officer at management level;

c) policies and procedures for sharing information required for the purposes of CDD and ML/TF risk management;

d) the provision of customer, account and transaction information from branches and subsidiaries when necessary for AML/CFT purposes; and

e) safeguards on the confidentiality and use of information exchanged.

25.2 A group compliance officer is responsible for creating, coordinating and making a group-wide assessment for the implementation of a single AML/CFT strategy, including mandatory policies and procedures and the authorisation to give orders to all branches and subsidiaries.

26. Record Keeping

26.1 Reporting institutions are required to keep the relevant records including any accounts, files and business correspondence and documents relating to transactions, in particular, those obtained during the CDD process. This includes documents used to verify the

identity of customers and beneficial owners, and results of any analysis undertaken. The records maintained must remain up-to-date and relevant.

26.2 Reporting institutions are required to keep the records for at least six years following the completion of the transaction, the termination of business relationship or after the date of occasional transaction.

26.3 In situations where the records are subject to ongoing investigations or prosecution in court, they shall be retained beyond the stipulated retention period until such time reporting institutions are informed by the relevant law enforcement agency that such records are no longer required.

26.4 Reporting institutions are required to retain the relevant records in the form that is admissible in as evidence in court and make available to the supervisory authorities and law enforcement agencies in a timely manner.

27. AML/CFT Compliance Programme

27.1 Policies, Procedures and Controls

27.1.1 Reporting institutions are required to implement programmes to mitigate against ML/TF, which correspond to its ML/TF risks and the size of its business.

27.2 Board of Directors

27.2.1 *General*

(a) Members of Board of Directors (Board members) shall understand their roles and responsibilities in managing ML/TF risks faced by the reporting institution;

(b) Board members must be aware of the ML/TF risks associated with business strategies, delivery channels and geographical coverage of its business products and services; and

(c) Board members must understand the AML/CFT measures required by the laws including the AMLATFA subsidiary legislation and instruments issued under the AMLATFA, and the industry's standards and best practices as well as the importance of implementing AML/CFT measures to prevent the reporting institution from being abused by money launderers and financiers of terrorism.

27.2.2 *Roles and Responsibilities*

The Board of Directors (Board) have the following roles and responsibilities:

(a) maintain accountability and oversight for establishing AML/CFT policies and minimum standards;

(b) approve policies regarding AML/CFT measures within the reporting institution, including those required for risk assessment, mitigation and profiling, CDD, record keeping, on-going due diligence, reporting of suspicious transactions and combating the financing of terrorism;

(c) establish appropriate mechanism to ensure the AML/CFT policies are periodically reviewed and assessed in line with changes and developments in the reporting institution's products and services, technology as well as trends in ML/TF;

(d) establish an effective internal control system for AML/CFT and maintain adequate oversight of the overall AML/CFT measures undertaken by the reporting institutions;

(e) define the lines of authority and responsibility for implementing the AML/CFT measures and ensure that there is a separation of duty between those implementing the policies and procedures and those enforcing the controls;

(f) ensure effective internal audit function in assessing and evaluating the robustness and adequacy of controls implemented to prevent ML/TF;

(g) assess the implementation of the approved AML/CFT policies through regular reporting and updates by the senior management and Audit Committee; and

(h) establish MIS that is reflective of the nature of the reporting institution's operations, size of business, complexity of business operations and structure, risk profiles of products and services offered and geographical coverage.

27.3 Senior Management

27.3.1 Senior management is accountable for the implementation and management of AML/CFT compliance programmes in accordance with policies and procedures established by the Board, requirements of the law, regulations, guidelines and the industry's standards and best practices.

27.3.2 *Roles and Responsibilities*

The senior management have the following roles and responsibilities:

(a) be aware of and understand the ML/TF risks associated with business strategies, delivery channels and geographical coverage of its business products and services offered and to be offered including new products, new delivery channels and new geographical coverage;

(b) formulate AML/CFT policies to ensure that they are in line with the risks profiles, nature of business, complexity, volume of the transactions undertaken by the reporting institution and its geographical coverage;

(c) establish appropriate mechanism and formulate procedures to effectively implement AML/CFT policies and internal controls approved by the Board, including the mechanism and procedures to monitor and detect complex and unusual transactions;

(d) undertake review and propose to the Board the necessary enhancement to the AML/CFT policies to reflect changes in the reporting institution's risk profiles, institutional and group business structure, delivery channels and geographical coverage;

(e) provide timely periodic reporting to the Board on the level of ML/TF risks facing the reporting institution, strength and adequacy of risk management and internal controls implemented to manage the risks and the latest development on AML/CFT which may have an impact on the reporting institution;

(f) allocate adequate resources to effectively implement and administer AML/CFT compliance programmes that are reflective of the size and complexity of the reporting institution's operations and risk profiles;

(g) appoint a compliance officer at management level at Head Office and designate a compliance officer at management level at each branch or subsidiary;

(h) provide appropriate levels of AML/CFT training for its employees at all levels throughout the organisation;

(i) ensure that there is a proper channel of communication in place to effectively communicate the AML/CFT policies and procedures to all levels of employees;

(j) ensure that AML/CFT issues raised are addressed in a timely manner; and

(k) ensure the integrity of its employees by establishing appropriate employee assessment system.

27.4 Compliance Management Arrangements

27.4.1 The Compliance Officer acts as the reference point for AML/CFT matters within the reporting institution.

27.4.2 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.

27.4.3 The Compliance Officer is required to be "fit and proper" to carry out his AML/CFT responsibilities effectively.

27.4.4 For the purposes of Paragraph 27.4.3, "fit and proper" may include minimum criteria relating to:

(a) probity, personal integrity and reputation; and

(b) competency and capability.

27.4.5 The Compliance Officer must have the necessary knowledge and expertise to effectively discharge his roles and responsibilities, including being informed of the latest developments in ML/TF techniques and the AML/CFT measures undertaken by the industry.

27.4.6 Reporting institutions may encourage their Compliance Officer to pursue professional qualifications in AML/CFT so that they are able to carry out their obligations effectively.

27.4.7 Reporting institutions are required to ensure that the roles and responsibilities of the Compliance Officer are clearly defined and documented.

27.4.8 The Compliance Officer has a duty to ensure the following:

(a) the reporting institution's compliance with the AML/CFT requirements;

(b) proper implementation of the AML/CFT policies and procedures;

(c) the appropriate AML/CFT procedures, including, CDD, record-keeping, on-going due diligence, reporting of

suspicious transactions and combating the financing of terrorism are implemented effectively;

(d) the AML/CFT mechanism is regularly assessed to ensure that it is effective and sufficient to address any change in ML/TF trends;

(e) the channel of communication from the respective employees to the branch or subsidiary compliance officer and subsequently to the Compliance Officer is secured and that information is kept confidential;

(f) all employees are aware of the reporting institution's AML/CFT measures, including policies, control mechanism and the channel of reporting;

(g) internal generated suspicious transaction reports by the branch or subsidiary compliance officers are appropriately evaluated before submission to the Financial Intelligence and Enforcement Department, Bank Negara Malaysia and AML Compliance Unit of Labuan FSA; and

(h) the identification of ML/TF risks associated with new products or services or arising from the reporting institution's operational changes, including the introduction of new technology and processes.

27.4.9 Reporting institutions are required to inform, in writing, the Financial Intelligence and Enforcement Department, Bank Negara Malaysia and AML Compliance Unit of Labuan FSA within ten working days, on the appointment or change in the appointment of the Compliance Officer, including such details as the name, designation, office address, office telephone number, fax number, e-mail address and such other information as may be required.

27.4.10 The Compliance Officer or any designated person as Compliance Officer needs to ensure and check any latest information or announcement in relation to AML Compliance

on Labuan FSA website on frequent basis. The person also responsible to take necessary action (if any) within reasonable time.

27.5 **Employee Screening Procedures**

27.5.1 The screening procedures shall apply upon hiring the employee and throughout the course of employment.

27.5.2 Reporting institutions are required to establish an employee assessment system that is commensurate with the size of operations and risk exposure of reporting institutions to ML/TF.

27.5.3 The employee assessment system shall include an evaluation of an employee's personal information, including criminal records, employment and financial history.

27.6 **Employee Training and Awareness Programmes**

27.6.1 Reporting institutions are required to conduct awareness and training programmes on AML/CFT practices and measures for their employees. Such training must be conducted regularly and supplemented with refresher course.

27.6.2 The employees must be made aware that they may be held personally liable for any failure to observe the AML/CFT requirements.

27.6.3 The reporting institution must make available its AML/CFT policies and procedures for all employees and its documented AML/CFT measures must contain at least the following:

(a) the relevant documents on AML/CFT issued by Labuan FSA or relevant supervisory authorities; and

(b) the reporting institution's internal AML/CFT policies and procedures.

27.6.4 The training conducted for employees must be appropriate to their level of responsibilities in detecting ML/TF activities and the risks of ML/TF faced by reporting institutions.

27.6.5 Employees who deal directly with the customer shall be trained on AML/CFT prior to dealing with customers.

27.6.6 Training for all employees may provide a general background on ML/TF, the requirements and obligations to monitor and report suspicious transactions to the Compliance Officer and the importance of CDD.

27.6.7 In addition, training may be provided to specific categories of employees:

(a) **Front-Line Employees**

Front-line employees may be trained to conduct effective on-going CDD, detect suspicious transactions and on the measures that need to be taken upon determining a transaction as suspicious. Training may also be provided on factors that may give rise to suspicion, such as dealing with occasional customer transacting in large amount of transaction, PEPs, higher risk customers and the circumstances where enhanced CDD is required.

(b) **Employees that Establish Business Relationships**

The training for employees who establish business relationships may focus on customer identification, verification and CDD procedures, including when to conduct enhanced CDD and circumstances where there is a need to defer establishing business relationship with a new customer until CDD is completed satisfactorily.

(c) **Supervisors and Managers**

The training on supervisors and managers may include overall aspects of AML/CFT procedures, in particular, the risk-based approach to CDD, risk profiling of customers,

enforcement actions that can be taken for non-compliance with the relevant requirements pursuant to the relevant laws and procedures related to the financing terrorism.

27.7 **Independent Audit Functions**

27.7.1 The requirements for the independent audit functions shall be read together with the Guidelines on Minimum Audit Standards for Internal Auditors of Labuan Banks and Supplementary Guidelines to Minimum Audit Standards for Internal Auditors issued by Labuan FSA.

27.7.2 The Board is responsible to ensure regular independent audits of the internal AML/CFT measures to determine their effectiveness and compliance with the AMLATFA, its regulations, subsidiary legislations and relevant policies, circulars and directives on AML/CFT issued by the Labuan FSA as well as the requirements of the relevant laws and regulations of other supervisory authorities, where applicable.

27.7.3 The Board is required to ensure that the roles and responsibilities of the auditor are clearly defined and documented. The roles and responsibilities of the auditor shall include, at a minimum:

(a) checking and testing the compliance with, and effectiveness of the AML/CFT policies, procedures and controls; and

(b) assessing whether current measures are in line with the latest developments and changes to the relevant AML/CFT requirements.

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

(a) compliance with AMLATFA, its subsidiary institution's subsidiary legislation and instruments issued under the AMLATFA;

(b) compliance with the reporting institution's internal AML/CFT policies and procedures;

(c) adequacy and effectiveness of the AML/CFT compliance programme; and

(d) reliability, integrity and timeliness of the internal and regulatory reporting and management of information systems.

27.7.5 The auditor must submit a written audit report to the Board to highlight the assessment on the effectiveness of AML/CFT measures and any inadequacy in internal controls and procedures.

27.7.6 Reporting institutions are required to ensure that independent audits are carried out at the institution level at least on an annual basis.

27.7.7 Reporting institutions must ensure that such audit findings and the necessary corrective measures undertaken are submitted to the Supervision and Enforcement Department, Labuan FSA within three months after the completion of the internal audit and within ten working days after submission to Board.

28. Suspicious Transaction Report

28.1 General

28.1.1 Reporting institutions are required to promptly submit a suspicious transaction report to the Financial Intelligence and Enforcement Department, Bank Negara Malaysia and to Anti-

Money Laundering Compliance Unit, Labuan FSA whenever the reporting institution suspect or have reason to suspect that the transaction (including attempted or proposed), regardless of the amount:

(a) appears unusual;
(b) has no clear economic purpose;
(c) appears illegal;
(d) involves proceeds from an unlawful activity; or
(e) indicates that the customer is involved in ML/TF.

28.1.2 Reporting institutions must provide the required and relevant information that giving rise to the suspicion in the suspicious transaction report form, which includes but 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.

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

28.1.4 Reporting institutions may refer to **Appendix I** to this guidelines which provides examples of transactions that may constitute triggers for the purposes of reporting suspicious transactions.

28.2 **Reporting Mechanisms**

28.2.1 Reporting institutions are required to ensure that the designated branch or subsidiary compliance officer is responsible for channelling all internal suspicious transaction reports received from the employees of the respective branch or subsidiary to the Compliance Officer at the head office. In the case of employees at the head office, such internal suspicious transaction reports shall be channelled directly to the Compliance Officer.

28.2.2 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.

28.2.3 Upon receiving any internal suspicious transaction report whether from the head office, branch or subsidiary, the Compliance Officer must evaluate the grounds for suspicion. Once the suspicion is confirmed, the Compliance Officer must promptly submit the suspicious transaction report. In the case where the Compliance Officer decides that there are no reasonable grounds for suspicion, the Compliance Officer must document and file the decision, supported by the relevant documents.

28.2.4 The Compliance Officer must submit the suspicious transaction report in the specified suspicious transaction report form through the following modes:

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

AND

Mail : Director
Supervision and Enforcement Dept
Labuan Financial Services Authority
Level 17, Main Office Tower
Financial Park Complex
Jalan Merdeka
87000 Labuan F.T.
Attention to : Anti-Money Laundering Compliance Unit
(To be opened by addressee only.)
Fax : +6087-411496
E-mail : aml@labuanfsa.gov.my

28.2.5 Where applicable and upon the advice of the Financial Intelligence and Enforcement Department, Bank Negara Malaysia and/or Anti-Money Laundering Compliance Unit, Labuan FSA, the Compliance Officer of a reporting institution must submit its suspicious transaction reports on-line:
Website: https://bnmapp.bnm.gov.my/fins2

28.2.6 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.

28.2.7 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.

28.2.8 Reporting institutions must provide additional information and documentation as may be requested by Labuan FSA

and to respond promptly to any further enquiries with regard to any report received under Section 14 of the AMLATFA.

28.2.9 Reporting institutions must ensure that the suspicious transaction reporting mechanism is operated in a secured environment to maintain confidentiality and preservation of secrecy.

28.2.10 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.

28.3 Tipping Off

28.3.1 In cases where the reporting institution forms a suspicion of ML/TF and reasonably believes that performing the CDD process would tip off the customer, the reporting institution is permitted not to pursue the CDD process. In such circumstances, the reporting institution shall proceed with the transactions and immediately file a suspicious transaction report.

28.3.2 Tipping off in relation to suspicious transaction reports is not applicable if:

(a) the purpose of the disclosure is made to inform the ML/TF risks involved in dealing with the customer within the financial group; or

(b) such disclosure is made to a supervisory authority of the reporting institution.

28.3.3 Provisions under Paragraph 28.3.2 will not come into effect until such date as may be specified by Labuan FSA.

28.4 **Triggers for Submission of Suspicious Transaction Report**

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

28.4.2 Reporting institutions may be guided by examples of suspicious transactions provided by the Labuan FSA or other corresponding competent authorities, supervisory authorities and international organisations.

28.4.3 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".

28.5 **Internally Generated Suspicious Transaction Reports**

28.5.1 Reporting institutions must ensure that the Compliance Officer maintains a complete file on all internally generated reports and any supporting documentary evidence regardless of whether such reports have been submitted. If there is no suspicious transaction reports submitted to Financial Intelligence and Enforcement Department, Bank Negara Malaysia, and also to AML Compliance of Labuan FSA, the internally generated reports and the relevant supporting documentary evidence must be made available to the relevant supervisory authorities upon request.

29. Combating the Financing of Terrorism

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

29.2 Reporting institutions are required to keep updated with the various resolutions passed by the United Nations Security Council (UNSC) on counter terrorism measures in particular the UNSC Resolutions 1267 (1999), 1373 (2001), 1988 (2011) and 1989 (2011) which

require sanctions against individuals and entities belonging or related to the Taliban, Osama bin Laden and the Al-Qaeda organisation.

29.3 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:
http://www.un.org/sc/committees/1267/aq_sanctions_list.shtml

29.4 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 AMLATFA by the Minister of Home Affairs.

29.5 Reporting institutions shall ensure that the information contained in the database is updated and relevant, and made easily accessible to its employees at the head office, branch or subsidiary.

29.6 Reporting institutions are required to conduct regular checks on the names of new and existing customer and potential customers, against the names in the database. If there is any name match, reporting institutions are required to take reasonable and appropriate measures to verify and confirm the identity of its customer. Once confirmation has been obtained, reporting institutions must immediately:

(a) freeze without delay the customer's funds or block the transaction (where applicable), if it is an existing customer;
(b) reject the potential customer, if the transaction has not commenced;
(c) submit a suspicious transaction report; and
(d) inform the relevant supervisory authorities as the case may be.

29.7 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 sections 66B or 66C of the AMLATFA.

29.8 Reporting institutions are required to ascertain potential matches with the Consolidated List to confirm whether they are true matches to eliminate "false positives". 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.

29.9 Reporting institutions may also consolidate their database with the other recognised lists of designated persons or entities issued by other jurisdictions.

30. Non-Compliance

30.1 Enforcement actions can be taken against the reporting institutions including its Directors, Officers, and Employees for any non-compliance with provisions under:

(a) In Sections 22, 66E, 86, 87, 88, 92 and 93 of the AMLATFA; and/or

(b) Section 4B of LFSAA.

Appendix I

Examples of Transactions[3] That May Trigger Suspicion

1. Unusual amount of remittances which does not commensurate an individual or company business activities.

2. Substantial increases in cash deposits of any individual or business without apparent cause, especially if such deposits are subsequently transferred within a short period out of the account and/or to a destination not normally associated with the customer.

Accounts

3. Accounts that appear to act as pass through accounts with high volumes of credits and debits and low average monthly balances.

4. Customers who wish to maintain a number of trustee or client accounts, which do not appear consistent with the type of business, including transactions which involve nominee names.

5. Customers who have numerous accounts and pay in amounts of cash to each of them in circumstances in which the total amount of credits would be large.

6. Any individual or company whose account shows no normal personnel banking or business related activities, but is used to receive or disburse large sums which have no obvious purpose or relationship to the account holder and/or his business (e.g. a substantial increase in turnover on an account).

7. Reluctance to provide normal information when opening an account or providing information that is difficult or expensive for the reporting instruction to verify.

[3] Modified from 'A Model of Best Practices to Combat Money Laundering in the Financial Sector' by the Commonwealth Secretariat.

8. Customers who appear to have accounts with several reporting institutions within the same locality but choose to consolidate funds from such accounts on regular basis for onward transmission to a third party account.

9. Matching of payments out with credits paid-in by cash on the same or previous day.

10. Large cash withdrawals from a previously dormant/inactive account, or from an account which has just received an unexpectedly large credit from abroad.

11. Company's representatives avoiding contact with branch officers.

12. Substantial increases in deposits or negotiable instrument by a professional firm or company, using client accounts or in-house company, or trust accounts, especially if the deposits are promptly transferred between other client's company and trust accounts.

13. Customers who show an apparent disregard for accounts offering more favourable terms, e.g. avoidance of high interest rate facilities for large credit balances.

14. Customers who decline to provide information that in normal circumstances would make the customer eligible for credit or for other banking services that would be regarded as valuable.

15. Insufficient use of normal banking facilities.

16. Large number of individuals making payments into the same account without any adequate explanation.

***International Banking/Trade* Finance**

17. Customers introduced by an overseas branch, affiliate or any other bank based in countries where production of drugs or drug trafficking may be prevalent.

18. Use of Letter of Credit and other methods of trade finance to move money between countries where such trade is not consistent with the customer's usual business.

19. Customers who make regular and large payments, including wire transfers, that cannot be clearly identified as bona fide transactions, or receive regular and large payments from countries which are commonly associated with the production, processing or marketing of drugs, prescribed terrorist organizations or which are tax havens.

20. Building up of large balances, which are not consistent with the known turnover of the customer's business, and subsequent transfer to accounts held overseas.

21. Unexplained electronic fund transfers by customers on an in-and-out basis or without passing, through an account.

22. Customers who show apparent disregard for arrangements offering more favourable terms.

23. Items shipped that are inconsistent with the nature of the customer's business.

24. Customers conducting business in higher risk countries.

25. Customers shipping items through higher risk countries, including transit through non-cooperative countries.

26. Customers involved in potentially higher risk activities, including activities that may be subject to export/import restrictions (e.g. equipment for military of foreign governments, weapons, ammunition, chemical mixtures, classified defense articles and sensitive technical data).

27. Obvious over or under pricing of goods and services.

28. Obvious misrepresentation of quantity or type of goods imported or exported.

29. Transaction structure appears unnecessarily complex and designed to obscure the true nature of the transaction.

30. Customers request payment of proceeds to an unrelated third party.

31. Shipment locations or description of goods not consistent with letter of credit.

32. Significantly amended letters of credits without reasonable justification or changes to the beneficiary or location of payment.

Employees and Agents

33. Changes in employee's characteristics, e.g. lavish life styles or avoiding taking holidays.

34. Changes in employees or agent's performance, e.g. the salesman, selling products for cash, have a remarkable or unexpected increase in performance.

35. Any dealing with an agent where the identity of the ultimate beneficiary or counterpart is undisclosed, contrary to normal procedure for the type of business concerned.

36. For private banking or trust services, sudden strong performance by employees in special relationship/confidential relationship banking services

such as trust or private banking services or sudden increase in the wealth/spending of such employees.

Private Banking and Trust Services

37. The grantors of private banking trust accounts that direct loans from their accounts to other parties or business interests of account principals or beneficiaries.

Secured and Unsecured Lending

38. Customers who repay problem loans unexpectedly and with no proper explanation as to the source of funds.

39. Request to borrow against assets held by the reporting institution or a third party, where the origin of the assets is not known or the assets are inconsistent with the customer's standing.

40. Request by a customer for a reporting institution to provide or arrange financial contribution to a deal which is unclear, particularly, where property is involved.

41. A customer who unexpectedly repays in part or in full a fixed loan or other loan that is inconsistent with his/her earning capacity or asset base.

42. A customer who applies for property / vehicle loan with a very low margin of finance that is not customary for the type of property / vehicle or profile of the customer.