AIFC TECHNOLOGY LTD
(LL17076)
Unit 14D, Main Office Tower , Financial Park Complex Labuan, Jalan Merdeka 87000 Wp Labuan.
Tel: 1700 827 827 | Email: info@aifctechnology.com

ANTI-MONEY LAUNDERING AND COUNTER FINANCING OF TERRORISM POLICY AND PROCEDURES

1. INTRODUCTION

1.1. AIFC Technology Limited ("**AIFC**") demonstrates its full commitment to high standards of compliance with the Anti-Money Laundering and Counter Financing of Terrorism ("**AML/CFT**") requirements by establishing this comprehensive policy and procedures (the "**Policy**") for the prevention and detection of money laundering and terrorist financing activities.

1.2. This Policy is issued pursuant to Paragraph 8.8 of the Guidelines on Money Broking Business in Labuan IBFC and is subject to periodic reviews to ensure that it remains robust and complies with the requirements of the Anti-Money Laundering and Anti-Terrorism Financing Act 2001 ("**AMLATFA 2001**"), the Guidelines on AML/CFT – Banking Sector ("**AML/CFT Guidelines"**) and the Financial Action Task Force ("**FATF**") Recommendations as well as other applicable domestic and international practices.

2. DEFINITION

The terms and expression used in this Policy shall have the same meanings assigned to it in the AMLATFA, LFSSA and the Guidelines as the case may be, unless otherwise defined in this Policy. For the purpose of this Policy the following definitions shall apply:

Term	Definition
AIFC	Means AIFC Technology Limited (LL17076).
AML/CFT	Means anti-money laundering and counter financing of terrorism.
AML/CFT Guidelines	Means the Guidelines on Anti-Money Laundering and Counter Financing of Terrorism – Banking Sector issued by the Labuan FSA.
AMLATFA	Means the Anti-Money Laundering and Anti-Terrorism Financing Act 2001.
Board of Directors	Refers to the board of directors of AIFC from time to time;

Customer(s)	Refers to the person(s) (whether a natural person, legal person or legal arrangement):- a) with whom AIFC establishes or intends to establish business relations; or b) for whom AIFC undertakes or intends to undertake any transaction without an account being opened.
Customer Due Diligence	Refers to the identification and verification procedures undertaken by AIFC applicable to its Customers pursuant to Paragraph 7.2.
Compliance Officer	Refers to the compliance officer appointed by the Senior Management of AIFC whose duties and responsibilities are set out in Paragraph 12.
Employee(s)	Refers to the employee(s) of AIFC.
Higher Risk Countries	Refers to the countries set out in Paragraph 8.4 with either on-going or substanstial ML/TF risks or strategic AML/CFT deficiencies.
Labuan FSA	Refers to Labuan Financial Services Authority.
Money-Broking Services	Refers to the business of arranging transactions between buyers and sellers in the money or foreign exchange markets as an intermediary in consideration of brokerage fees paid or to be paid, but does not include the buying or selling of ringgit or foreign currencies as a principal in such markets;
Senior Management	Refers to the any person(s) having authority and responsibility for planning, directing or controlling the activities including the management and administration of AIFC.

3. KEY CONCEPTS

3.1. Money Laundering

3.1.1. Money laundering encompasses all activities, procedures or processes aimed to legitimise funds obtained through illegal or criminal actitivites. The money brokerage services industry may serve as an avenue to launder money and this threatens the intergrity, trust and confidence of the public in the industry itself.

3.1.2. Generally, the process of money laundering comprises three stages, namely: placement, layering and integration. They may occur in sequence, but may often overlap.

(a) Placement

In the intitial stage, the criminal introduces his illegal profits and gains into the financial system. This is the physical disposal of criminal proceeds. In the case of many serious crimes (not only drug trafficking) the proceeds take the form of cash which the criminal wishes to place in the financial system. Placement may be achieved by a wide variety of means according to the opportunity afforded to and the ingenuity of the criminal, his advisers and their network. Typically, it may include:

- placing cash on deposit at a bank (ofter intermingled with legitimate credit to obscure the audit trail), thus converting cash into a readily recoverable debt.
- physically moving cash between jurisdictions;
- making loans in cash to businesses which appear to be legitimate or are connected with legitimate businesses, thereby converting cash into debt;
- purchasing the services of high-value professionals or firms;
- purchasing the services of high-value professionals or firms;
- purchasing negotiable assets in one-off Transactions; or
- placing cash in the client account of a professional intermediary.

(b) Layering

After the funds have entered the financial system, the criminal proceeds are separated from their source by the creation of layers of transactions designed to disguise the audit trail and provide the appearance of legitimacy. Again, this may be achieved by a wide variety of means according to the opportunity afforded to, and the ingenuity of, the criminal, his advisers and their network. Typically, it may include:

- rapid switches of funds between bank and/or jurisdictions;
- use of cash deposit as collateral secutity in support of legitimate transactions;
- switching cash through a network of legitimate businesses and "shell" companies across several jurisdictions; or
- resale of goods/assets.

(c) Integration

When the layering succeeds, the criminal proceeds have been successfully laundered, i.e. 'cleaned' and are regarded for all intent and purposes as legitimate funds. The criminal proceeds are then reintroduced, i.e. intergrated back into the financial system through investments in businesses or purchase of assets.

3.2. Terrorist Financing

3.2.1. Terrorism seeks to influence, compel or intimidate governments or the general public through threats or violence, causing of damage to property or danger to life, creating of serious risks to public health or safety, or disrupting of important public services or infrastructure.

3.2.2. Terrorists require funds to carry out acts of terrorism and terrorist financing provides the funds needed. Sources of terrorist financing may be legitimate or illegitimate. It may be derived from criminal activities such as kidnapping, extortion, fraud or drug trafficking. It may also be derived from legitimate income such as membership dues, sale of publications, donations from persons or entities sympathetic to their cause, and sometimes income from legitimate business operations belonging to terrorist organisations.

3.2.3. Terrorist financing involces amounts that are not always large and the associated transactions may not necessarily be complex given that some sources of terrorist funds may be legitimate.

3.2.4. However, the methods used by terrorist organisations to move, collect, hide or make available funds for their activities remain similar to those used by criminal organisations to launder their funds. This is especially so when the funds are derived from illegitimate sources, in which case, the terrorist organisation would have similar concerns to a typical criminal organisation in laundering the funds. Where the funds are derived from legitimate sources, terrorist organisations would usually still need to employ the same laundering techniques to obscure or disguise the links between the organisation and the funds.

4. SUMMARY OF BUSINESS AND RISK ASSOCIATED WITH THE BUSINESS

4.1. AIFC is licensed by the Labuan FSA under the Labuan Financial Services and Securities Act 2010 to carry on Money-Broking Business in Labuan. It has been identified by the Labuan FSA that the products and services provided by AIFC may be abused for ML/FT purposes as criminals are seeking new corporate vehicles or trusts as a means of disguising or hiding assets or transactions, as a conduit for proceeds obtained through illegal acts or for creating layers of "smoke and mirrors" to prevent identification of ultimate controllers or owners of assets.

5. UNDERLYING PRINCIPLES

5.1. This Policy is based on the following principles:

(a) AIFC shall exercise due diligence when dealing with its Customers, natural persons appointed to act on the Customer's behalf, connected parties of the Customer and beneficial owners of the Customers.

(b) AIFC shall conduct its business in conformity with high ethical standards, and guard against establishing any business relations or undertaking any transaction that facilitates or may facilitate ML/TF.

(c) AIFC shall, to the fullest extent possible, assist and cooperate with the relavant law enforcement authorities in Malaysia to prevent ML/TF.

6. AML/CFT COMPLIANCE FRAMEWORK

6.1. In compliance with the AML/CFT Guidelines by Labuan FSA, AIFC shall implement and maintain the following AML/CFT procedure:

(a) identifications and verification procedures (including but not limited to, Customer due diligence (simplified and enhanced) and on-going monitoring);

(b) record keeping procedures;

(c) employee screening procedures and training programmes;

(d) internal reporting procedures;

(e) external reporting procedures;

(f) other internal controls and communication procedures for the purpose of preventing ML/TF.

7. RISK PROFILING & CUSTOMER DUE DILIGENCE

7.1. Risk Profiling

7.1.1. On or before establishing business relations with a Customer, AIFC shall conduct risk profiling on such Customer for the purposes of managing and mitigating any ML/TF risks identified.

7.1.2. 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.

7.1.3. The risk profile of a particular Customer or type of Customer will dictate the level and degree of Customer due diligence that must be conducted by AIFC.

7.1.4. Upon the initial acceptance of the Customer, AIFC shall regularly review and update the Customer's risk profile based on their level of ML/TF risks.

7.2. Customer Due Diligence ('CDD')

7.2.1. The purpose of identification and verification process is to establish that the Money-Broking Business provided by AIFC is a genuine transaction and this can be achieved by conducting CDD on the Customer and the person conducting the transaction.

7.2.2. AIFC shall 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.

7.2.3. The CDD measures undertaken by AFIC comprises the following:

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

(b) to identify the Customer and verify the Customer's identify using reliable, independent source documents, data or information;

(c) to verify that any person purporting to act on behalf of the Customer is so authorized, and identify and verify the identity of that person;

(d) to 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

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

7.2.4. The specific CDD measures on individual customer/beneficial owner and legal persons are set out in **Appendix I** of this Policy.

7.2.5. 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, AIFC may, in its absolute discretion, complete verification after the establishment of the business relationship to allow some flexibilities for its Customer and/or beneficial owner to furnish the relevant documents.

7.2.6. The delayed verification under Paragraph 7.3 shall only apply if AIFC are satisfied that the following conditions are met:

(a) the delay occurs as soon as reasonably practicable and shall not be later than ten (10) working days or any other period as may be specified by Labuan FSA;

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

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

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

7.2.7. AIFC will 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 AIFC is in the view that it is unable to comply with any of the CDD requirements and may consider lodging a suspicious transaction report under Paragraph 16.

8. ENHANCED CUSTOMER DUE DILIGENCE

8.1. Upon determination of a Customer's risk profile pursuant to Paragraph 7.1, AIFC shall perform enhanced CDD where the Customer's risk profile are assessed as having higher ML/TF risks.

8.2. Factors which present a high risk of ML/TF includes, but not limited to:

8.2.1. Customer risk factors

(a) the business relationship is conducted in unusual circumstances (e.g. significant unexplained geographic distance between the reporting institution and the customer);

(b) non-resident customer;

(c) legal persons or arrangements that are personal asset-holding vehicles;

(d) companies that have nominee shareholders or shares in bearer form;

(e) business that are cash-intensive;

(f) the ownership structure of the company appears unusual or excessively complex given the nature of the company's business;

(g) high net worth individuals;

(h) persons from locations known for their high rates of crime (e.g. drug producing, trafficking, smuggling);

(i) businesses or activities identified by the FATF as having higher risk for ML/TF;

(j) legal arrangements that are complex (e.g. trust, nominee); and

(k) persons who match the red flags criteria of AIFC.

8.2.2. Country or geographic risk factors

(a) countries having inadequate AML/CFT systems;

(b) countries subject to sanctions, embargos or similar measures issued by, for example, the United Nations;

(c) countries having significant levels of corruption or other criminal activity; and

(d) countries or geographic areas identified as providing funding or support for terrorist activities, or that have designated terrorist organisations operating within their country.

8.2.3. Product, service, transaction or delivery channel risk factors

(a) anonymous transactions (which may include cash);

(b) non face-to-face business relationships or transactions;

(c) payment received from multiple persons and/or countries that do not fit into the person's nature of business and risk profile; and

(d) payment received from unknown or un-associated third parties.

8.3. An enchanced CDD shall include the following:

(a) obtaining CDD information under Paragraph 7.2;

(b) obtaining additional information on the Customer and beneficial owner (e.g. volume of assets and 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 before establishing (or continuing, for existing Customer) such business relationship with the Customer.

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

(f) updating more regularly the identification data of Customer and beneficial owner;

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

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

8.4. <u>Politically Exposed Persons ('PEPs')</u>

8.4.1 AIFC shall determine whether a Customer or a beneficial owner is a foreign or domestic PEP by conducting a risk profling in accordance to Paragraph 7.1.

8.4.2 Upon determination by AIFC that a Customer is a foreign PEPs, the requirements of enhanced CDD set out under Paragraph 8.2 shall be conducted on the PEPs.

8.4.3 Upon determination by AIFC that a Customer is a domestic PEP and that AIFC is satisfied that the domestic PEPs is assessed as higher risk, the requirements of enhanced CDD as set out under Pargraph 8.2 must be conducted. If however, AIFC is satisfied that the domestic PEPs are not assessed as higher risk, AIFC may;

in its absolute discretion, apply CDD measures similar to other low risks customers.

8.5. Higher Risk Countries

8.5.1 AIFC shall conduct enhanced CDD for business relationships and transactions with any person from countries identified by the FATF or the Government of Malaysia as having having strategic AML/CFT deficiencies and have not made sufficient progress in addressing those deficiencies.

8.5.2 In addition to the enhanced CDD requirement under Paragraph 8.4.1, AIFC shall also 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.

9. RECORD KEEPING

9.1. All relevant records, including but not limited to, any accounts, files and business correspondence and documents relating to transactions, in particular, those obtained during the CDD process (which includes documetns used to verify the identity of Customer and beneficial owners, and results of any analaysis undertaken) shall be kept

for at least six (6) years (subject to Paragraph 9.2. below) following the completion of the transaction, the termination of business relationship or after the date of occasional transaction.

9.2. 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 AIFC are informed by the relevant law enforcement agency that such records are no longer required.

10. RESPONSIBILITIES OF THE BOARD OF DIRECTORS

10.1. The roles and responsibilities of the Board of Directors in relation to the prevention of ML/TF include the following: -

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

(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 Policy are periodically reviewed ans assessed in line with changes and developments in AIFC'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 AIFC;

(e) define the lines of authority and responsibility for implementing the AML/CFT measures and ensure that there is 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 senior management and Audit Committee (as defined below); and

(h) establish a management information system (MIS) that is reflective of the nature of AIFC's operations, size of business, complexity of business operations and

structure, risk profiles of produucts and services offered and geographical coverage.

11. RESPONSIBILITIES OF THE SENIOR MANAGEMENT

11.1. The roles and responsibilities of Senior Management in relation to the prevention of ML/TF include the following: -

(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 and procedures to ensure that they are in line with the risks profiles, nature of business, complexity, volume of the transactions undertaken by AIFC and its geographical coverage;

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

(d) undertake review and propose to the Board of Directors 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 of Directors 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 AIFC;

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

(g) appoint a Compliance Officer at management level at Head Office;

(h) provide appropriate levels of AML/CFT training for its Employeess 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.

12. APPOINTMENT OF COMPLIANCE OFFICER

12.1. The Compliance Officer is a person appointed by the Senior Management to act as the reference point for AML/CFT matters within AIFC.

12.2. It is the Compliance Officer's duty and responsibilities to ensure the following: -

(a) AIFC'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 Compliance Officer is secured and that information is kept confidential;

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

(g) awareness of any lastest information or announcement in relation to AML Compliance on Labuan FSA website on frequent basis;

(h) all suspicious transaction reports to be submitted to the Financial Intelligence and Enforcement Department, Bank Negara Malaysia and AML Compliance Unit of Labuan FSA; and

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

12.3. The Compliance Officer shall ensure and check any latest information or announcement in relation to AML Compliance on Labuan FSA website on frequent basis. It is also responsible to take necessary action (if any) in relation to the prevention of ML/TF within reasonable time.

13. EMPLOYEE SCREENING PROCEDURES

13.1. The employee screening procedure implemented by AIFC shall take place before the commencement of employement and throughout the course of employment of an Employee.

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

14. EMPLOYEE TRAINING AND AWARENESS PROGRAMMES

14.1. The effectiveness of the AML/CFT measures implemented by AIFC depends on the extent to which the Employees of AIFC comprehend the issues surrounding ML/TF and their respective obligations under this AML/CFT Policy, as well as their obligations to comply with any AML/CFT Regulations.

14.2. All Employees shall participate in the awareness and training programmes on AML/CFT practices and measures conducted by AIFC. The training conducted for each Employee will be appropriate to their level of responsibilities in detecting ML/TF activities and the risks of ML/TF faced by AIFC. Apart from the initial training, refresher training at regular intervals will also be conducted to ensure that the Employees are reminded of their responsibilities and are kept informed of developments.

14.3. The objective of the awareness and training programmes is to 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.

14.4. The internal AML/CFT Policy of AIFC and the relevant documents on AML/CFT issued by Labuan FSA or relevant supervisory authorities shall be made available for all Employees.

14.5. Additional training is required for specific categories of Employees:

14.5.1. 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 and understand the 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 enchanced CDD is required.

14.5.2. Employees that Establish Business Relationships

The training provided for Employees who establish business relationship shall focus on Customer identification, verification and CDD procedures, including when to conduct enchanced CDD and circumstances where there is a need to defer establishing business relationship with a new Customer until CDD is completed satisfactorily.

14.5.3. Supervisors and Managers

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

14.6. AIFC Employees must be aware that they may be held personally liable for any failure to observe the AML/CFT requirements provided in this Policy.

15. INDEPENDENT AUDIT FUNCTIONS

15.1. AIFC is required to submit an annual Independent Audit Report on AML/CFT to the Supervision and Enforcement Department of Labuan FSA. 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 any of its supplementary issued by Labuan FSA.

15.2. The requirement for the independent audit functions is to determine the effectiveness and compliance of AIFC's internal AML/CFT measures with AMLATFA 2001, 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.

15.3. 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.

15.4. 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 AIFC'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.

16. SUSPICIOUS TRANSACTION REPORT

16.1. Suspicious Transaction

A suspicious transaction will often be one which is inconsistent with a Customer's known activities. Examples of transactions that may constitute triggers for the purpose of reporting suspicious transactions are set out in **Appendix II** to this Policy.

16.2. Internal Reporting

All internal suspicious transaction reports made by the Employees shall be channelled directly to the Compliance Officer. Upon receiving any internal suspicious transaction report, 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 accordance to Paragraph 16.3 below. 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.

16.3. External Reporting

AIFC shall 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 Compliance Officer suspects 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.

16.4. Tipping Off

In cases where an Employee forms a suspicion of ML/TF and reasonably believes that performing the CDD process would tip off the Customer, the Employee handling the transaction is permitted not to pursue the CDD process. In such circumstances, the Employee shall proceed with such transactions and immediately file a suspicious transaction report to the Compliance Officer.

[THE REMAINDER OF THIS PAGE HAS BEEN INTENTIONALLY LEFT BLANK]

APPENDIX I

SPECIFIC CDD MEASURES

This appendix sets out the required information and documentation that must be obtained during the course of conducting CDD on individual customer/beneficial owner and legal persons.

1. Individual Customers and Beneficial Owner

1.1. The individual customer and beneficial owner shall provide AFIC with the following information:

(a) full legal name (including former names, other current names and aliases used);

(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).

1.2. AFIC may accept any other official documents bearing the photograph of the customer and beneficial owner under Paragraph 1.1(b) of this Appendix I provided that AFIC can be satisfied with the authenticity of the documents which contain the necessary required information.

1.3. The customer or beneficial owner shall furnish the original and make a copy of the said document to verify the documents referred to in Paragraph 1.1(b) of this Appendix I. However, where biometric identification method is used, verification is deemed to be satisfied.

1.4. Where there is any doubt, the customer and beneficial owner shall 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.

2. **Legal Persons**

2.1. For customers that are legal persons, they shall provide AFIC with the following information:

(a) nature of business, its ownership and control structure;

(b) 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;

(c) 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

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

(e) 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.

2.2. Where there is any doubt as to the identity of persons referred to under Paragraphs 2.1(b) and (e) of this Appendix I, AFIC 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.

[END OF APPENDIX I]

Appendix II

EXAMPLES OF TRANSACTIONS 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.

(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.

[END OF APPENDIX II]