



# **Anti – Money Laundering Policy & Combating Terrorist Financing**

**(2023)**

## 1. GENERAL DEFINITIONS

For the purposes of this Manual, unless the context shall prescribe otherwise:

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. This manual is formulated in accordance with 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.

We (“The Company”) follow the standard Guidelines on Anti-Money Laundering and Counter Financing of Terrorism (AML/CFT) issued on 4 January 2007; and The Anti-Money Laundering and Counter Financing of Terrorism (AML/CFT) Sectoral Guidelines 1 for Offshore Financial Institutions Licensed and Registered Under Offshore Financial Services Act 1990 issued on 4 January 2007.

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); 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 Fax: +6087-411496 E-mail: [aml@labuanfsa.gov.my](mailto:aml@labuanfsa.gov.my)

Where applicable and upon the advice of the Financial Intelligence and Enforcement Department, 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>

“**Beneficial Owner**”, when used in this Manual, shall mean, unless the context requires otherwise, the natural person or natural persons, who ultimately owns or controls the Customer and/or the natural person on whose behalf a transaction or activity is being conducted; the Beneficial Owner shall in any event include:

In the case of corporate entities: the natural person or natural persons, who ultimately own(s) or control(s) a legal entity through direct or indirect ownership or control of a sufficient percentage of the shares or voting rights in that legal entity, a percentage of 10% plus one share be deemed sufficient to meet this criterion; The natural person or natural persons, who otherwise exercise control over the management of a legal entity.

**"Business Relationship"**, when used in this Manual, shall mean, unless the context requires otherwise, a business, professional or commercial relationship which is connected with the professional activities of the Company;

**"Customer"**, when used in this Manual, shall mean, unless the context requires otherwise, any legal or physical person aiming to open a trading account and conclude a Business Relationship with the Company;

**"Company"**, when used in this Manual, shall mean, unless the context requires otherwise, RIVER PRIME LTD. is operating under the FSA Labuan Financial Services and Securities Act 2010 (the "Act 704") and to carry on money broking business pursuant to Sections 90 and 92 of Labuan Financial Services and Securities Act 2010 (the "FSA") and holds Money broking Licence number MB/19/0039 (the "Licence"); having its registered office 2, Kim Business Center 2, Unit F28, 1<sup>st</sup> floor, Paragon Labuan, Jalan Tun Mustapha, Federal Territory of Labuan, 87000, Malaysia;

**"Act"**, when used in this Manual, shall mean, unless the context requires otherwise, the Proceeds of Criminal Conduct Act, 2010 with amendments;

**"Directive(s)"**, when used in this Manual, shall mean, unless the context requires otherwise, the directive or directives issued in respect of the prevention of money laundering and terrorist financing by the Labuan Financial Service Authority (the "LFSA", or the "Agency"), the Central Bank of Malaysia (the "Bank") and/or the Labuan Financial Services Authority (the "FSA", or the "Commission");

**"Manual"**, when used in this Manual, shall mean, unless the context requires otherwise, the Company's Prevention of Money Laundering & Terrorist Financing Manual (this Manual);

**"Politically Exposed Persons (PEPs)"**, when used in this Manual, shall mean, unless the context requires otherwise, the natural persons who are or have been entrusted with prominent public functions and their immediate family members or persons known to be close associates of such persons;

**"FSA"**, when used in this Manual, shall mean, unless the context requires otherwise, Labuan Financial service authority;

**"Regulated Market"**, when used in this Manual, shall mean, unless the context requires otherwise, the multilateral system managed or operated by a market operator and which brings together or facilitates the bringing together of multiple third-party buying or/and selling interests in trading instruments - in the system and in accordance with its non-discretionary rules - in a way that results in a contract, in respect of the trading instruments admitted to trading under its rules or/and systems, and which is authorized and functions regularly in accordance with the provisions of the Securities and Investment Business Act, 2010 (the "Act") and the Securities

Regulations, 2008, or similar legislation of other countries, which are considered by the FATF adequately to apply the FATF 40+9 Recommendations;

“**Shell Bank**”, when used in this Manual, shall mean, unless the context requires otherwise, a credit institution or an institution engaged in equivalent activities incorporated in a jurisdiction which it has no physical presence, involving meaningful mind and management, and which is unaffiliated with a regulated financial group.

## 2. INTRODUCTION

The purpose of the Manual is to lay down the Company's internal practice, measures, procedures and controls relevant to the prevention of money laundering and terrorist financing.

The Manual is developed and periodically updated by the Money Laundering Compliance Officer (hereinafter the “MLCO”), based on the general principles set up by the Company's Board of Directors (hereinafter the “BOD”) in relation to the prevention of money laundering and terrorist financing.

All amendments and/or changes of the Manual must be approved by the Board of Directors of the Company.

The Manual shall be communicated by the MLCO to all the employees of the Company that manage, monitor or control in any way the Customers' transactions and have the responsibility for the application of the practices, measures, procedures and controls that have been determined herein.

The Manual has been prepared to comply with the provisions of the Act and the Directives.

## 3. THE RESPONSIBILITIES OF THE BOARD OF DIRECTORS

The responsibilities of the BOD in relation to the prevention of money laundering and terrorist financing include the following:

- a) to determine, record and approve the general policy principles of the Company in relation to the prevention of money laundering and terrorist financing, consistent with the requirements of the Code, the Regulations and related enactments, and communicate them to the MLCO;
- b) to appoint the MLCO in accordance with section 13 of the Regulations and, where is necessary, assistant MLCOs and determine their duties and responsibilities, which are recorded in this Manual;
- c) to approve the Manual;

- d) to ensure that all requirements of the Act and of the Directives are applied, and ensure that appropriate, effective and sufficient systems and controls are introduced for achieving the abovementioned requirements;
- e) to ensure that the MLCO and his assistants, if any, and any other person who has been assigned with the duty of implementing the procedures for the prevention of money laundering and terrorist financing, have complete and timely access to all data and information concerning Customers' identity, transactions documents and other relevant files and information maintained by the Company so as to be fully facilitated in the effective execution of their duties, as set forth herein;
- f) to ensure that all employees are aware of the person who has been assigned the duties of the MLCO, as well as his assistants (if any), to whom they report any information concerning transactions and activities for which they have knowledge or suspicion that might be related to money laundering and terrorist financing;
- g) to establish a clear, quick and efficient reporting chain based on which information regarding suspicious transactions is passed without delay to the MLCO, either directly or through his assistants, if any, and notifies accordingly the MLCO for its explicit prescription in the Manual;
- h) to ensure that the MLCO has sufficient resources, including competent staff, financial resources and technological equipment, for the effective discharge of his duties;
- i) to assess and approve the MLCO's Annual Report and take all action as deemed appropriate under the circumstances to remedy any weaknesses and/or deficiencies identified in the abovementioned report;
- j) to meet and decide upon the necessary measures that need to be taken to ensure the rectification of any weaknesses and/or deficiencies which have been detected in the MLCO's Annual Report;
- k) to notify the Agency, or the Commission in writing within 14 (fourteen) days of its MLCO ceasing to act as such and promptly act to appoint another person to replace him in accordance with the provisions of the Regulations.

#### **4. MONEY LAUNDERING COMPLIANCE OFFICER**

##### **4.1. GENERAL**

The MLCO shall be part of the management of the Company so as to command the necessary authority. Furthermore, the MLCO shall lead the Company's Money Laundering Compliance procedures and processes and report to the Board of Directors of the Company. The MLCO shall

also have access to all relevant information necessary to perform his duties. The level of remuneration of the MLCO shall not compromise his objectivity.

#### 4.2. DUTIES OF THE MLCO

During the execution of his duties and the control of the compliance of the Company with the Act and the Directives, the MLCO shall obtain and utilize data, information and reports issued by international organizations, as these are mentioned in the Manual.

**The duties of the MLCO shall include, inter alia, the following:**

- to design, based on the general policy principles of the Company, the internal practices, measures, procedures and controls relevant to the prevention of money laundering and terrorist financing, and describe and explicitly allocate the appropriateness and the limits of responsibility of each department that is involved in the abovementioned. It is provided that, the above measures and procedures for the prevention of the abuse of new technologies and systems providing financial services, for the purpose of money laundering and terrorist financing is appropriately considered and managed in the course of daily activities of the Company with regard to the development of new products and possible changes in the Company's economic profile (e.g., penetration into new markets);
- to develop and establish the Customer Acceptance Policy and submit it to the BOD for consideration and approval;
- to review and update the Manual as may be required from time to time, and for such updates to be communicated to the BOD for their approval;
- to monitor and assess the correct and effective implementation of the policies, practices, measures, procedures and controls referred to above, and in general the implementation of the Manual; in this respect, the MLCO shall apply appropriate monitoring mechanisms (e.g., on-site visits to different departments of the Company) which will provide him with all the necessary information for assessing the level of compliance of all departments and employees of the Company with the procedures and controls which are in force; in the event that the MLCO identifies shortcomings and/or weaknesses in the application of the required practices, measures, procedures and controls, the MLCO shall give appropriate guidance for corrective measures and, where deemed necessary, shall inform the BOD;
- to review and evaluate, at least on an annual basis, the appropriateness, effectiveness and adequacy of the policies, practices, measures, procedures and control mechanisms applied for the prevention of money laundering and terrorist financing mentioned in the Manual;
- to receive information from the Company's employees, which is considered to be knowledge or suspicion of money laundering or terrorist financing activities or which might be related with such activities; the information is received in a written report form (hereinafter the "Internal Suspicion Report");

- to evaluate and examine the information received as per point “f.” above, by reference to other relevant information and discuss the circumstances of the case with the informer and where appropriate, with the informer’s superiors; the evaluation of the information of point (f) above shall be included in a report (hereinafter the “Internal Evaluation Report”); if following the evaluation described in point “f.” above, the MLCO decides to notify the LFSA, then he should complete a written report and submit it to the LFSA the soonest possible; following the submission of the MLCO Report to the LFSA, the accounts involved and any other connected accounts, will be closely monitored by the MLCO and following any directions from the LFSA, the MLCO will thoroughly investigate and examine all the transactions of the accounts; if following the evaluation described above, the MLCO decides that the information received as per point “f.” above does not substantiate a suspicion of money laundering or terrorist financing, the MLCO will as soon as possible disclose that decision in writing to the Agency, as well as fully explain the reasons for such a decision on the MLCO’s Internal Evaluation Report;
- to act as a first point of contact with the Agency, upon commencement of and during an investigation as a result of filing a report to the LFSA pursuant to above;
- to ensure the preparation and maintenance of the lists of Customers categorized following a risk-based approach, which contains, among others, the names of Customers, their account number and the dates of the commencement of the business relationship; moreover, the MLCO will ensure the updating of the said list with all new or existing Customers, in the light of any additional information obtained;
- to detect, record, and evaluate, at least on an annual basis, all risks arising from existing and new Customers, new financial instruments and services and update and amend the systems and procedures applied by the Company for the effective management of the aforesaid risks;
- to evaluate the systems and procedures applied by any third parties, if any, on whom the Company relies for Customer identification and due diligence purposes and to approve the cooperation with such third parties;
- to ensure that all branches and subsidiaries of the Company, if any, which operate in countries outside the FSA, have taken all necessary measures for achieving full compliance with the provisions of the Manual, in relation to Customer identification, due diligence and record keeping procedures;
- to provide advice and guidance to the employees of the Company on subjects related to money laundering and terrorist financing;
- to acquire the knowledge and skills required for the improvement of the appropriate procedures for recognizing, preventing and obstructing any transactions and activities that are suspected to be associated with money laundering or terrorist financing;
- to determine whether the Company’s departments and employees need further training and education for the purpose of preventing money laundering and terrorist financing and to organize appropriate training sessions/seminars; in this respect, the MLCO prepares and applies an Annual Staff Training Program; also, the MLCO assesses the adequacy of any such education and training provided;
- to prepare the Annual Report referred to in the Manual;

- to respond to all requests and queries from the LFSA, the Central Bank of Malaysia and the FSA; provide all requested information to, and fully cooperate with the same;
- to maintain a registry which includes the reports referred to in points “e.”, “f.” and “g.” above, and any other relevant statistical information (e.g., the department that submitted the internal report, date of submission to the MLCO, date of assessment and/or, as the case may be, date of reporting to the LFSA), the evaluation reports referred to in point “d.” above and all the documents that confirm the accomplishment of his duties.

## 5. ANNUAL REPORT OF THE MLCO

The Annual Report of the MLCO is a significant tool for assessing the Company's level of compliance with its obligation laid down in the Act and the Directives.

The MLCO's Annual Report shall be prepared and submitted to the Board of Directors for approval within two (2) months of the end of each calendar year (i.e., at latest, by the end of February of each year).

The Annual Report deals with issues relating to money laundering and terrorist financing during the year under review and shall include, inter alia, the following:

- information for measures taken and/or procedures introduced for compliance with any amendments and/or new provisions of the Act and the Directives which took place during the year under review;
- information on the inspections and reviews performed by the MLCO, reporting the material deficiencies and weaknesses identified in the policies, practices, measures, procedures and controls, which the Company applies for the prevention of money laundering and terrorist financing; in this respect, the report shall outline the seriousness of the deficiencies and weaknesses, the risk implications and the actions taken and/or recommendations made for rectifying the situation;
- information on the appropriateness, effectiveness and adequacy of the policies, practices, measures, procedures and control mechanisms applied for the prevention of money laundering and terrorist financing mentioned in the Manual;
- the number of Internal Suspicion Reports submitted by Company personnel to the MLCO and any possible comments/observations in that regard;
- the number of reports submitted by the MLCO to LFSA, with information/details on the main reasons for suspicion and highlights of any particular trends;
- information, details or observations regarding the communication with the employees on money laundering and terrorist financing preventive issues;
- information on the policies, measures, practices, procedures and controls applied by the Company in relation to high-risk Customers as well as the number and country of origin of high-risk Customers with whom a Business Relationship is established or an Occasional Transaction has been executed;



- information on the systems and procedures applied by the Company for the ongoing monitoring of Customer accounts and transactions;
- information on the measures taken for the compliance of branches and subsidiaries of the Company, if any, that operate in countries outside the FSA, with the requirements of the Act and the Directives in relation to Customer identification, due diligence and record keeping procedures and comments/information on the level of their compliance with the said requirements;
- information on the training courses/seminars attended by the MLCO and any other educational material received;
- information on training/education and any educational material provided to staff during the year, reporting, the number of courses/seminars organized, their duration, the number and the position of the employees attending, the names and qualifications of the instructors, and specifying whether the courses/seminars were developed in-house or by an external organization or consultants;
- results of the assessment of the adequacy and effectiveness of the above-mentioned staff training;
- information on the recommended training program for the following year;
- information on the structure and staffing of the department of the MLCO as well as recommendations and timeframe for their implementation, for any additional staff and technical resources which may be needed for reinforcing the measures and procedures against money laundering and terrorist financing.
- 

## **6. RISK-BASED APPROACH**

### **6.1. GENERAL POLICY**

The Company shall apply appropriate measures and procedures, by adopting a risk-based approach, so as to focus its effort in those areas where the risk of money laundering and terrorist financing appears to be comparatively higher.

The risk-based approach to be followed by the Company, as described in the Manual, shall have the following general characteristics:

- recognizes that the money laundering or terrorist financing threat varies across Customers, countries, services and financial instruments;
- allows the BOD to differentiate between Customers of the Company in a way that matches the risk of the Company's particular business;
- allows the BOD to apply its own approach in the formulation of policies, procedures and controls in response to the Company's particular circumstances and characteristics;
- helps to produce a more cost-effective system;
- Promotes the prioritization of effort and actions of the Company in response to the likelihood of money laundering or terrorist financing occurring through the use of services provided by the Company.

The risk-based approach adopted by the Company, as described in the Manual, shall involve specific measures and procedures in assessing the most cost effective and appropriate way to identify and manage the money laundering and terrorist financing risks faced by the Company.

**Such measures shall include:**

- identifying and assessing the money laundering and terrorist financing risks emanating from particular Customers, services, and geographical areas of operation of the Company and its Customers;
- managing and mitigating the assessed risks by the application of appropriate and effective measures, procedures and controls;
- continuous monitoring and improvements in the effective operation of the policies, procedures and controls.

The application of appropriate measures and the nature and extent of the procedures on a risk- based approach will depend on different indicators.

**Such indicators will include the following:**

- the scale and complexity of the services offered by the Company;
- geographical spread of the services offered and the location of the Company's Customers;
- the nature (e.g., non-face-to-face) and economic profile of the Company's Customers as well as of services offered by the Company;
- the distribution channels and practices of providing services by the Company;
- the volume and size of the transactions entered into by the Company;
- the degree of risk associated with each area of services;
- the country of origin and destination of Customers' funds;
- deviations from the anticipated level of transactions.

## **6.2. IDENTIFICATION OF RISKS**

The risk-based approach adopted by the Company shall involve the identification, recording and evaluation of the risks that have to be managed.

The Company shall assess and evaluate the risks it faces, in light of the possible utilization of the services it provides for the purposes of money laundering or terrorist financing; the particular circumstances of the Company determine suitable procedures and measures that need to be applied to counter and manage risk; in those instances where the services and the financial instruments provided by the Company are relatively simple, involving relatively few Customers or Customers with similar characteristics, the Company shall apply procedures that focus on those Customers who fall outside the “norm”.

The Company shall be, at all times, in a position to demonstrate to the LFSA, the Central Bank of Malaysia and/or the FSA that the extent of measures and control procedures that applies are proportionate to the risk it faces for the use of services provided, for the purpose of money laundering and terrorist financing.

The following are, inter alia, sources of risks which the Company faces with respect to money laundering and terrorist financing:

**6.2.1. Risks based on the Customer's nature:**

- i. complexity of ownership structure of legal entities;
- ii. companies incorporated in offshore centers;
- iii. Politically Exposed Persons (PEPs);
- iv. Customers engaged in transactions with significant volume;
- v. Customers from high-risk countries or countries known for high level of corruption or organized crime or drug trafficking;
- vi. Unwillingness of Customers to provide required information.

**6.2.2. Risks based on the Customer's behaviour:**

- i. Customer transactions where there is no apparent legal financial/commercial rationale
- ii. situations where the origin of wealth and/or source of funds cannot be easily verified;
- iii. Unwillingness of Customers to provide required information.

**6.2.3. Risks based on the Customer's initial communication with the Company:**

- i. non-face-to-face Customers;
- ii. Customers introduced by a third party.

**6.2.4. Risks based on the Company's services:**

- i. services that allow payments to third parties;
- ii. large cash deposits or withdrawals\*;
- iii. Products or transactions which may favor anonymity.

\* RIVER PRIME LTD Doesn't accept cash payments

These procedures to insure that include:

- Establishing clear guidelines and policies for financial transactions, including the approval process and documentation requirements.
- Ensuring that all financial transactions are processed through our centralized finance department and are subject to rigorous review and monitoring.

- Conducting regular audits to ensure that all financial activities are in compliance with regulatory requirements and our internal policies.

### **6.3. DESIGN AND IMPLEMENTATION OF MEASURES AND PROCEDURES TO MANAGE AND MITIGATE THE RISKS**

Taking into consideration the assessed risks, the Company shall determine the type and extent of measures it will adopt in order to manage and mitigate the identified risks in a cost-effective manner.

**These measures and procedures shall include:**

- a) adaption of the Company's Due Diligence Procedures in respect of Customers in line with their assessed money laundering and terrorist financing risk;
- b) requiring the quality and extent of required identification data for each type of Customer to be of a certain standard (e.g., documents from independent and reliable sources, third party information, documentary evidence);
- c) obtaining additional data and information from the Company's Customers, where this is appropriate for the proper and complete understanding of their activities and source of funds and for the effective management of any increased risk emanating from the particular Business Relationship;
- d) Ongoing monitoring of high-risk Customers, transactions and activities.

### **6.4. DYNAMIC RISK MANAGEMENT**

Risk management is a continuous process, carried out on a dynamic basis. Risk assessment is not an isolated event of a limited duration; Customers' activities change, and the services provided by the Company may change or evolve, as well; the same may happen to the transactions used for money laundering or terrorist financing.

## **7. CUSTOMER ACCEPTANCE POLICY**

The Company's Customer Acceptance Policy (hereinafter the "CAP"), in accordance with the principles and guidelines described in this Manual, defines the criteria for accepting new Customers and stipulates the Customer categorization criteria which shall be adhered to by the Company and especially by the employees who are involved in the Customer Account Opening process.

### **7.1. GENERAL PRINCIPLES OF THE CAP**

The General Principles of the CAP are the following:

- a) the Company shall classify Customers into various risk categories and based on the risk perception decide on the acceptance criteria for each category of Customer;
- b) where the Customer is a prospective Customer, an account must be opened only after the relevant pre-account opening due diligence and identification measures and procedures have been conducted, according to the principles and procedures set forth in the Manual;
- c) all documents and data required to be obtained pursuant to the Company's Customer Acceptance Policy must be collected before accepting a new Customer;
- d) no Customer shall be accepted in anonymous or fictitious names(s);

## **7.2. CRITERIA FOR ACCEPTING NEW CUSTOMERS (BASED ON RISK)**

This Section describes the criteria for accepting new Customers based on their risk categorization.

### **7.2.1 Low Risk Customers**

The Company shall accept Customers who are categorized as low risk Customers as long as the general principles set forth in in this Section 8 are adhered to.

Moreover, the Company shall follow the Simplified Customer Identification and Due Diligence Procedures for low-risk Customers set forth hereinafter.

### **7.2.2. Normal Risk Customers**

The Company shall accept Customers who are categorized as normal risk Customers as long as the general principles set forth in this Section 3 are adhered to.

### **7.2.3. High Risk Customers**

The Company shall not accept Customers who are categorized as high-risk Customers.

Moreover, in case accepted, the Company shall apply the Enhanced Customer Identification and Due Diligence measures for High-Risk Customers, set forth hereinafter, and shall, as well, apply the due diligence and identification procedures for the specific types of high-risk Customers set forth hereinafter, as applicable.

Some examples of high-risk industries include:

1. Money services businesses (MSBs)
2. Casinos and online gaming

3. Cryptocurrency exchanges
4. Precious metals and stones dealers
5. Real estate developers and brokers
6. Dealers in high-value items such as art and antiques
7. Non-profit organizations
8. Lawyers, accountants, and other professional service providers

#### **7.2.4. Unacceptable Customers**

The following list predetermines the types of Customers who are not acceptable for establishing a Business Relationship with the Company:

- a) Customers who fail or refuse to submit, the requisite data and information for the verification of their identity and the creation of their economic profile, without adequate justification;
- b) Shell Banks.

#### **7.3. CUSTOMER CATEGORISATION CRITERIA**

This Section defines the criteria for the categorization of Customers based on their risk:

##### **7.3.1. Low Risk Customers**

The following types of Customers can be classified as low risk Customers with respect to the money laundering and terrorist financing risks, which the Company may face:

- i. Financial institutions covered by the FSA Financing and Money Services Act, 2010;
- ii. credit or financial institutions carrying out one or more of the financial business activities, as these are defined by the FSA Financing and Money Services Act, 2010, situated in a country outside the FSA that is considered by the FATF adequately to apply the FATF 40+9 Recommendations, which:
  1. are subject to requirements and/or regulations equivalent to those laid down by the FSA Financing and Money Services Act, 2010; and
  2. are under supervision by a regulatory authority that is equivalent to the Central Bank of Malaysia for compliance with those requirements;
- iii. regulated companies and/or investment firms carrying out one or more of the financial business activities, as these are defined by the FSA Financing and Money Services Act, 2010 and/or the FSA Investment

Business Act, 2010, situated in a country outside the FSA that is considered by the FATF adequately to apply the FATF 40+9 Recommendations, which:

1. are subject to requirements and/or regulations equivalent to those laid down by the FSA Financing and Money Services Act, 2010
  2. are under supervision by a regulatory authority that is equivalent to the Labuan FSA for compliance with those requirements;
- iv. listed companies whose securities are admitted to trading on a Regulated Market in the FSA or in a third country outside the FSA that is considered by the FATF adequately to apply the FATF 40+9 Recommendations, which are subject to disclosure requirements equivalent to those applicable in the FSA;
- v. domestic public authorities of the FSA or public authorities of third countries outside the FSA that are considered by the FATF adequately to apply the FATF 40+9 Recommendations.

In each of the instances mentioned above, the Company must gather sufficient information to establish if the Customer qualifies as a low-risk Customer.

### **7.3.2. Normal Risk Customers**

The following types of Customers can be classified as normal risk Customers with respect to the money laundering and terrorist financing risks, which the Company may face:

Any Customer who does not fall under the “low risk Customers” or “high risk Customers” categories set forth in this Section 7.2.

### **7.3.3. High Risk Customers**

The following types of Customers can be classified as high-risk Customers with respect to the money laundering and terrorist financing risks, which the Company may face:

- a) Customers who are not physically present for identification purposes (non-face-to-face Customers);
- b) Politically Exposed Persons (PEPs) accounts;
- c) Customers from countries that is considered by the FATF inadequately to apply the FATF 40+9 Recommendations.
- d) any other Customers that their nature entail a higher risk of money laundering or terrorist financing;
- e) any other Customer determined by the Company itself to be classified as such.

## **8. CUSTOMER DUE DILIGENCE AND IDENTIFICATION PROCEDURES**

### **8.1. APPLICATION OF CUSTOMER DUE DILIGENCE AND IDENTIFICATION PROCEDURES**

The Company shall duly apply Customer identification procedures and Customer due diligence measures in the following instances:

- a) when establishing a Business Relationship;
- b) when there is a suspicion of money laundering or terrorist financing, regardless of the amount of the transaction;
- c) when there are doubts about the veracity or adequacy of previously Customer identification data.

### **8.2. DEVELOPMENT OF AN ECONOMIC PROFILE AND GENERAL CUSTOMER IDENTIFICATION AND DUE DILIGENCE PRINCIPLES**

The development of the Customer's economic profile needs to include/comply with the following principles:

- a) the Company shall be satisfied that it is dealing with a real person and, for this reason, the Company shall obtain sufficient evidence of identity to verify that the person is who he claims to be. Furthermore, the Company shall verify the identity of the Beneficial Owners of the Customers' accounts. In the cases of legal entities, the Company shall obtain adequate data and information so as to understand the ownership and control structure of the Customer. Irrespective of the Customer's type (e.g., natural or legal entity, sole trader or partnership), the Company shall request and obtain sufficient data and information regarding the Customer's business activities and the expected pattern and level of transactions. However, it is noted that no single form of identification can be fully guaranteed as genuine or representing correct identity and, consequently, the identification process will generally need to be cumulative;
- b) the verification of the Customers' identification shall be based on reliable data and information issued or obtained from independent and reliable sources, meaning those data, and information that are the most difficult to be amended or obtained illicitly;
- c) the data and information that are collected before the establishment of the Business Relationship, with the aim of constructing the Customer's economic profile and, as a minimum, may include the following:
  - the purpose and the reason for requesting the establishment of a Business Relationship;
  - the anticipated account turnover, the nature of the transactions, the expected origin of incoming funds to be credited in the account and the expected destination of outgoing transfers/payments;
  - the Customer's level of wealth and annual income and the clear description of the main business/professional activities/operations;



- d) the data and information that are used for the construction of the Customer-legal entity's economic profile shall include, inter alia, the following:
- the name of the company;
  - the country of its incorporation;
  - the head offices address;
  - the names and the identification information of the Beneficial Owners;
  - the names and the identification information of the directors;
  - the names and the identification information of the authorized signatories;
  - financial information;
- e) the said data and information are recorded in a separate form designed for this purpose which is retained in the Customer's file along with all other documents as well as all internal records of meetings with the respective Customer. The said form is updated regularly or whenever new information emerges that needs to be added to the economic profile of the Customer or alters existing information that makes up the economic profile of the Customer;
- f) identical data and information with the abovementioned shall be obtained in the case of a Customer-natural person, and in general, the same procedures with the abovementioned shall be followed;
- g) transactions executed for the Customer shall be compared and evaluated against the anticipated account's turnover, the usual turnover of the activities/operations of the Customer and the data and information kept for the Customer's economic profile; significant deviations shall be investigated and the findings shall be recorded in the respective Customer's file; transactions that are not justified by the available information on the Customer, shall be thoroughly examined, so as to determine whether suspicions over money laundering or terrorist financing arise for the purposes of submitting an internal report.

The Company shall apply each of the Customer due diligence measures and identification procedures set forth herein, but may determine the extent of such measures on a risk-sensitive basis depending on the type of Customer or services offered; when so requested, the Company shall be able to demonstrate to the LFSA, the Central Bank of Malaysia and/or the FSA that the

extent of the measures is appropriate in view of the risks of the use of its services for the purposes of money laundering and terrorist financing.

For the purposes of the provisions relating to identification procedures and Customer due diligence requirements, proof of identity shall be deemed to be satisfactory if:

- i. it is reasonable possible to establish that the Customer is the person he claims to be; and,
- ii. The person who examines the evidence is satisfied, in accordance with the appropriate procedures that the Customer is actually the person he claims to be.

**9. FURTHER OBLIGATIONS FOR CUSTOMER IDENTIFICATIONS AND DUE DILIGENCE PROCEDURES**

In addition to the principles described hereinabove, the Company shall:

- ensure that the Customer identification records remain completely updated with all relevant identification data and information throughout the Business Relationship;
- examine and check, on a regular basis, the validity and adequacy of the Customer identification data and information it maintains, especially those concerning high risk Customers.

The procedures and controls described hereinabove also determine the timeframe during which the regular review, examination and update of the Customer identification shall be conducted; the outcome of the said review shall be recorded in a separate note/form which shall be kept in the respective Customer file.

Despite the obligations described above and while taking into consideration the level of risk, if at any time during the Business Relationship, the Company becomes aware that reliable or adequate data and information are missing from the identity and the economic profile of the Customer, then the Company shall take all necessary action, by applying the Customer identification and due diligence procedures, in accordance with the Manual, to collect the missing data and information, the soonest possible, so as to identify the Customer and update and complete the Customer's economic profile.

If, during the Business Relationship, a Customer fails or refuses to submit, within a reasonable timeframe provided to him by the Company, the required verification data and information, the Company reserves the right to terminate the Business Relationship and close all the accounts of the Customer in question, while at the same time it shall examine whether it is justified under the circumstances to submit a report to the LFSA.

In addition to the obligations set forth in this policy, the Company shall check the adequacy of the data and information of the Customer's identity and economic profile, whenever one of the following events or incidents occurs:

- an important transaction takes place which appears to be unusual and/or significant compared to the normal pattern of transactions and the economic profile of the Customer;
- a material change in the Customer's legal status and situation occurs, such as:
  - i. change of directors/secretary;
  - ii. change of registered shareholders and/or Beneficial Owners;
  - iii. change of registered office;
  - iv. change of corporate name and/or trading name;
  - v. change of the principal trading partners and/or undertaking of major new business activities.

- a material change occurs in the way and the rules the Customer's account operates, such:
  - i. a change in the persons that are authorized to operate the account;
  - ii. application for the provision of new services.

## **10. SIMPLIFIED CUSTOMER IDENTIFICATION AND DUE DILIGENCE PROCEDURES**

With respect to the provisions of the Act and the Directives for simplified Customer Identification and Due Diligence Procedures, the following shall apply:

The Company shall be allowed not to apply the normal Customer due diligence measures and identification procedures set forth hereinabove in those instances where the Customer is categorized as a low-risk Customer according to the criteria set forth in the Manual.

In each of the instances mentioned above, the Company shall collect sufficient information, so as to decide whether the Customer can be exempted according to the provisions of Section 6 above; when assessing the above-mentioned circumstances, the Company shall pay special attention to any activity of those Customers or to any type of transactions which may be regarded as particularly likely, by its nature, to be used or abused for money laundering or terrorist financing purposes.

The Company shall not consider that Customers or transactions referred to in Section 6.1 above represent a low risk of money laundering or terrorist financing if there is information available to suggest that the risk of money laundering or terrorist financing may not be unlikely.

With respect to public authorities or public bodies for which the normal Customer due diligence measures and identification procedures set forth hereinabove may not be applied, they must fulfil all the following criteria:

- a) the Customer has been entrusted with public functions pursuant to applicable law and/or secondary legislation;
- b) the Customer's identity is publicly available, transparent and certain;
- c) the activities of the Customer, as well as its accounting practices, are transparent;
- d) the Customer is either accountable to public authorities or public bodies that have been entrusted with public functions pursuant to applicable law and/or secondary legislation, or appropriate check and balance procedures exist that are ensuring control of the Customer's activity.

## **11. ENHANCED CUSTOMER IDENTIFICATION AND DUE DILIGENCE (HIGH RISK CUSTOMERS)**

### **11.1. GENERAL PROVISIONS**

The Company shall apply enhanced due diligence measures, in addition to the normal Customer due diligence measures and identification procedures set forth hereinabove, with respect to the Customers categorized as “high risk” Customers according to the criteria set forth hereinabove.

11.1.1. Where the Customer has not been physically present for identification purposes, the Company shall apply one or more of the following measures:

- i. obtain additional documents, data or information for verifying the Customer's identity;
- ii. take supplementary measures to verify or certify the documents supplied, or requiring confirmatory certification by a credit or financial institution;

11.1.2. In respect of transactions or Business Relationships with Politically Exposed Persons (PEPs), the Company shall:

- i. have appropriate risk-based procedures to determine whether the Customer is a PEP;
- ii. have Board of Directors approval for establishing Business Relationships with such Customers;
- iii. take adequate measures to establish the source of wealth and source of funds that are involved in the Business Relationship or transaction, which include obtained SOF/SOW documents for single trade threshold for Cash transactions above RM20,000, in addition to the scenarios by the law.
- iv. conduct enhanced ongoing monitoring of the Business Relationship.

### **11.2. HIGH RISK CUSTOMERS**

Due diligence and identification procedures with respect to high-risk Customers are described below.

#### **a) Non-face-to-face Customers**

The Company shall apply the following with respect to non-face-to-face Customers:

- In situations where a customer requests the establishment of a Business Relationship through mail, telephone, or the internet without presenting himself for a personal interview, the Company must follow the established Customer identification and due diligence procedures, as applied for Customers with whom it comes in direct and personal contact and obtain exactly the same identification information and documents;
- However, due to the difficulty in matching the Customer with the collected identification data, the Company shall apply enhanced Customer identification and due diligence measures, in line with the provisions regarding “high risk” Customers set forth hereinabove, so as to effectively mitigate the risks associated with such Business Relationship.

Practical procedures that can be applied as implementation of the due diligence and identification procedures with respect to high-risk Customers, with respect to non-face-to-face Customers of the Company, are the following:

- telephone contact with the Customer at his residence or office, before the establishment of a Business Relationship, on a telephone number which has been verified from a reliable and independent source;

The enhanced due diligence and identification procedures with respect to high-risk Customers are also to be applied to companies or other legal entities requesting the establishment of a Business Relationship through mail, telephone or internet; the Company shall take additional measures for ensuring that the companies or other legal entities operate from the address of their main offices and carry out legitimate business activities.

**b) "Politically Exposed Persons" accounts**

The Company shall apply the following with respect to the accounts of "Politically Exposed Persons (PEPs)":

- the establishment of a Business Relationship with persons holding important public positions and with natural persons closely related to them, may expose the Company to enhanced risks, especially if the potential Customer seeking to establish a Business Relationship is a Politically Exposed Person (PEP), a member of his immediate family or a close associate that is known to be associated with a Politically Exposed Person (PEP);
- the Company shall pay more attention when the said persons originate from a country which is widely known to face problems of bribery, corruption and financial irregularity and whose anti-money laundering laws and regulations are not equivalent with international standards, such as countries, which are considered by the FATF not adequately to apply the FATF 40+9 Recommendations;
- in order to effectively manage such risks, the Company shall assess the countries of origin of its Customers in order to identify the ones that are more vulnerable to corruption or maintain laws and regulations that do not meet the 40+9 requirements of the FATF;
- with regard to the issue of corruption, one useful source of information is the Transparency International Corruption Perceptions Index which can be found on the website of Transparency International at [www.transparency.org](http://www.transparency.org);
- with regard to detect PEP/sanction lists RIVER PRIME LTD can detect and linked with PEPs list from various countries (individual and organization) and other relevant sanction lists such as "World check" or "Accuity check".
- with regard to the issue of adequacy of application of the 40+9 recommendations of the FATF, the Company shall retrieve information from the country assessment reports prepared by the FATF or other regional bodies operating in accordance with FATF's principles (e.g., Money-Val Committee of the Council of Europe) or the International Monetary Fund.

For the purposes hereof, unless the context requires otherwise, the term “Politically Exposed Persons (PEPs)” shall be deemed to include the following natural persons who are or have been entrusted with prominent public functions in a foreign country:

- heads of State, heads of government, ministers and deputy or assistant ministers;
- members of parliament;
- members of supreme courts, of constitutional courts or of other high-level judicial bodies whose decisions are not subject to further appeal, except in out-of-line circumstances;
- members of courts of auditors or of the Board of Directors of central banks;
- ambassadors, “Chargé d'affaires” and high-ranking officers in the armed forces;
- members of the administrative, management or supervisory bodies of State-owned enterprises.

Without prejudice to the application, on a risk-sensitive basis, of enhanced Customer due diligence measures referred to hereinabove, where a person has ceased to be entrusted with a prominent public function within the meaning of set forth in this policy for a period of at least one year, the Company shall no longer be obliged to consider such a person as a “Politically Exposed Person (PEP)”.

None of the provisions and descriptions set forth in this policy shall be understood as covering middle ranking or more junior officials.

For the purposes hereof, unless the context requires otherwise, the term “immediate family members” shall be deemed to include the following:

- the spouse or the person with which a person cohabits for not less than one year;
- the children and their spouses or the persons with which a person cohabits for not less than one year;
- the parents.

For the purposes hereof, unless the context requires otherwise, the term “persons known to be close associates” shall be to include the following:

- any natural person who is known to have joint Beneficial Ownership of legal entities or legal arrangements, or any other close business relations, with any PEPs persons set forth in this policy;
- any natural person who has sole Beneficial Ownership of a legal entity or legal arrangement which is known to have been set up for the benefit de facto with any PEPs persons set forth in this policy;
- Without prejudice to any of the foregoing, the Company shall adopt the following additional due diligence measures when it establishes a Business Relationship with a Politically Exposed Person (PEP):
- the Company shall put in place appropriate risk management procedures to enable it to determine whether a prospective Customer is a Politically Exposed Person (PEP); such procedures may include, depending on the degree of risk, the acquisition and installation of a reliable commercial electronic database for Politically

Exposed Persons (PEPs), seeking and obtaining information from the Customer himself or from publicly available information; in the case of legal entities and arrangements, the procedures will aim at verifying whether the Beneficial Owners, authorized signatories and persons authorized to act on behalf of the legal entities and arrangements constitute Politically Exposed Persons (PEPs); in the event that one of the above is identified as a Politically Exposed Person (PEP), then automatically the account of the legal entity or arrangement should be subject to the relevant procedures specified in this Section of the Manual;

- before establishing a Business Relationship with a Politically Exposed Person (PEP), the Company shall obtain adequate documentation to ascertain not only the identity of the said person, but also additional information allowing it to assess the business reputation of the Politically Exposed Person (PEP) (e.g., reference letters from third parties);
- in addition, the Company shall compose the economic profile of the Politically Exposed Person (PEP) by obtaining the information specified hereinabove; the details of the expected business and nature of activities of the Customer shall form the basis for the future monitoring of the account of the Politically Exposed Person (PEP); the profile shall be regularly reviewed and updated with new data and information; the Company shall be particularly cautious and most vigilant where its Customers are involved in businesses, which appear to be most vulnerable to corruption such as trading in oil, arms, cigarettes and alcoholic drinks;
- the account shall be subject to annual review in order to determine whether to allow its continuance of operation; a short report shall be prepared summarizing the results of the review by the person who is in charge of monitoring the account; the report in question shall be submitted for consideration and approval to the Board of Directors and shall be filed in the Customer's personal file.

**c) Customers from countries, which are considered by the FATF not adequately to apply the FATF40+9 Recommendations**

The FATF 40+9 Recommendations constitute the primary internationally recognized standards for the prevention and detection of money laundering and terrorist financing.

The Company shall apply the following with respect to Customers from countries, which are considered by the FATF not adequately to apply the FATF 40+9 Recommendations:

- exercise additional monitoring procedures and pay special attention to Business Relationships and transactions with persons, including companies and financial institutions, from countries which do not apply or apply inadequately the aforesaid recommendations;
- transactions with persons from the said countries, for which there is no apparent economic or visible lawful purpose, shall be further examined for the purpose of establishing their economic, business or investment background and purpose;
- with the aim of implementing the above, the Company shall regularly consult the country assessment reports prepared by the FATF (<http://www.fatf-gafi.org>). the other regional bodies that have been established and work in accordance with the principles of FATF, such as the CFATF (<https://www.cfatf->

[gafic.org](http://gafic.org)). “Money-Val Committee” of the Council of Europe ([www.coe.int/moneyval](http://www.coe.int/moneyval)) and the International Monetary Fund ([www.imf.org](http://www.imf.org)): based on the said reports, the Company shall assess the risk of entering into transactions and Business Relationships with persons from various countries and, in particular, the risk of entering into transactions and/or Business Relationships with persons of the countries that inadequately apply the FATF's recommendations; depending on the outcome of the assessment, the Company shall apply, when deemed necessary, enhanced due diligence measures for identifying and monitoring transactions of persons originating from countries with significant shortcomings in their legal and administrative systems for the prevention of money laundering and terrorist financing.

## 12. CUSTOMER IDENTIFICATION AND DUE DILIGENCE PROCEDURES (SPECIFIC CASES)

The Company shall ensure that the appropriate documents and information with respect to the following cases shall be duly obtained, as applicable and appropriate:

### 12.1. ACCOUNTS OF NATURAL PERSONS

The Company shall obtain the following information to ascertain the true identity of the natural persons willing to be a Customer:

- a) true name and/or names used as these are stated on the official identity card or passport;
- b) full permanent address, including postal code;
- c) telephone (home and mobile), if any;
- d) e-mail address;
- e) date of birth;
- f) billing address;
- g) other data, as may be deemed necessary by the Company.
- h) POA dated no more 3 months.

In addition to the information collected in accordance with Section 7.2 above, without prejudice to the application on a risk-sensitive basis, the Company shall require and receive information on public positions which the prospective Customer holds or held in the last twelve (12) months, as well as whether the prospective Customer is a close relative or associate of such individual, in order to verify if the Customer is a Politically Exposed Person (PEP).

Furthermore, official national identification documents issued by the competent authorities of their country of origin shall be obtained; certified true copies of the pages containing the relevant information from the said documents shall also be obtained and kept in the Customer's files.



In addition, if in doubt for the genuineness of any identification document, the Company shall seek verification of identity with an Embassy or the Consulate of the issuing country or a reputable credit or financial institution situated in the Customer's country of residence.

In addition to the aim of preventing money laundering and terrorist financing, the abovementioned information is also essential for implementing the financial sanctions imposed against various persons by the United Nations; for this purpose, we reserve the right to require passport copies or relevant national identification so that the Company is in the position to verify precisely whether a Customer is included in the relevant list of persons subject to financial sanctions which are issued by the United Nations, based on a United Nations Security Council' Resolution and Regulation.

## **12.2. ACCOUNTS OF LEGAL ENTITIES**

For Customers that are legal entities, the Company shall establish that the natural person appearing to act on their behalf, are appropriately authorized to do so and that their identity is satisfactorily established and verified in accordance with the procedures set forth hereinabove.

The Company shall take all necessary measures for the full ascertainment of the legal entity's control and ownership structure, as well as for the verification of the identity of the natural persons who are the Beneficial Owners and exercise control over the legal entity, all in accordance with the procedures set forth hereinabove.

The verification of the identification of a legal entity that requests the establishment of a Business Relationship, comprises the ascertainment of the following:

- a) the registered number;
- b) the registered corporate name;
- c) the full address of the head office;
- d) the telephone numbers, fax numbers and e-mail address(es);
- e) the members of the Board of Directors;
- f) POA dated no more 3 months.
- g) the individuals that are duly authorized to operate the account and to act on behalf of the legal entity;
- h) the Beneficial Owners of private companies and public companies that are not listed in a Regulated Market of a country, which is considered by the FATF adequately to apply the FATF 40+9 Recommendations, or in a country with equivalent disclosure and transparency requirements;
- i) the registered shareholders that act as nominees of the Beneficial Owners.

For the verification of the identity of the legal entity, the Company shall request and obtain, among others, certified true copies of the following documents:

1. certificate of incorporation and certificate of good standing (where available) of the legal entity;

2. certificate of registered office;
3. certificate of directors and secretary;
4. certificate of registered shareholders in the case of private companies and public companies that are not listed on a Regulated Market of a country, which is considered by the FATF adequately to apply the FATF 40+9 Recommendations, or a third country with equivalent disclosure and transparency requirements;
5. memorandum and articles of association of the legal entity;
6. documents and data for the verification, in accordance with the procedures set forth hereinabove, of the identity of the Directors and persons that are authorized by the legal entity to operate the account.

Where deemed necessary for a better understanding of the activities, sources and uses of funds/assets of a legal entity, the Company shall obtain copies of its latest audited financial statements (if available), and/or copies of its latest management accounts.

As an additional due diligence measure, on a risk-sensitive basis, the Company shall carry out (when deemed necessary) a search and obtain information from the records of the Registrar of Companies or a corresponding authority in the company's (legal entity's) country of incorporation and/or request information from other sources in order to establish that the applicant company (legal entity) is not, nor is in the process of, being dissolved or liquidated or struck off from the registry of the Registrar of Companies or a corresponding authority and that it continues to be registered as an operating company.

It is pointed out that, if at any later stage any changes occur in the structure or the ownership status or to any details of the legal entity, or any suspicions arise emanating from changes in the nature of the transactions performed by the legal entity via its account, then it is imperative that further enquiries be made for ascertaining the consequences of these changes on the documentation and information held by the Company for the legal entity and that all additional documentation and information for updating the economic profile of the legal entity is collected.

### **12. 3. INVESTMENT FUNDS, MUTUAL FUNDS AND FIRMS PROVIDING FINANCIAL OR INVESTMENT SERVICES**

The Company shall be entitled to establish and maintain Business Relationships with persons or legal entities who carry out the above services and activities, which are incorporated and/or operating in countries, which are considered by the FATF adequately to apply the FATF 40+9 Recommendations or which, in accordance with a relevant decision of the Advisory Authority, have been determined to apply procedures and measures for preventing money laundering and terrorist financing equivalent to the requirements of the FATF 40+9 Recommendations, provided that the said persons or entities:

- a) possess the necessary license or authorization from a competent supervisory/regulatory authority of the country of their incorporation and operation to provide the said services; and

- b) are subject to supervision by a competent supervisory/regulatory authority of the country of their incorporation and operation for the prevention of money laundering and terrorist financing purposes.

In the event of the establishment of a Business Relationship with persons who carry out the above services and activities and which are incorporated and/or operating in third countries other than those mentioned in Section 16, the Company shall request and obtain, in addition to the information and documentation mentioned above, all information and documentation required by the Manual for the identification and verification of legal entities and their Beneficial Owners, including, without limitation, the following:

- a) a copy of the license or authorization granted to the said person from a competent supervisory/regulatory authority of its country of incorporation and operation, whose authenticity should be verified either directly with the relevant supervisory/regulatory authority or from other independent and reliable sources; and
- b) adequate documentation and sufficient information in order to fully understand the control structure and management of the business activities, as well as the nature of the services and activities provided by the Customer.

In the case of investment funds and mutual funds, the Company, apart from identifying the Beneficial Owners, shall obtain information regarding the objectives and control structure of such investment funds and mutual funds, including documentation and information for the verification of the identity of investment managers, investment advisors, administrators and custodians.

### **13. ON-GOING MONITORING PROCESS**

#### **13.1. GENERAL**

The constant monitoring of the Customers' accounts and transactions is an imperative element in the effective controlling of the risk of money laundering and terrorist financing.

#### **13.2. PROCEDURES**

The procedures and intensity of monitoring Customers' accounts and examining transactions in light of the Customer's level of risk shall include the following:

- a) the identification of:
  - i. transactions which, as a result of their nature, may be associated with money laundering or terrorist financing;

- ii. unusual or suspicious transactions that are inconsistent with the economic profile of the Customer for the purposes of further investigation;
- b) the investigation of unusual or suspicious transactions; the results of the investigations shall be recorded in a separate memo and shall be kept in the file of the Customers concerned;
- c) the use of appropriate IT systems.

## **14. RECORD-KEEPING PROCEDURES**

### **14.1. GENERAL**

The Company shall maintain records of:

- a) the Customer identification documents obtained during the Customer identification and due diligence procedures, as applicable;
- b) the details of all relevant records with respect to the provision of Forex and CFD trading services to Customers.

The documents/data of mentioned above shall be kept for a period of at least six (6) years, which shall be deemed to commence after the execution of the relevant transaction(s) or the termination of the Business Relationship.

### **14.2. FORMAT OF RECORDS**

The Company shall retain the documents/data mentioned in Section 9.1 of the Manual in electronic format, provided, however, that the Company must be able to retrieve the relevant documents/data without undue delay and present them at any time, to the LFSA, the Central Bank of Malaysia and/or the FSA, after a relevant request.

## **15. EMPLOYEES' OBLIGATIONS**

The Company's employees shall be personally liable for failure to report information or suspicion, regarding money laundering or terrorist financing.

The employees must cooperate and report, without delay, in accordance with the provisions of Section 4.2, anything that comes to their attention in relation to transactions for which there is the slightest suspicion that they may be related to money laundering and/or terrorist financing.

The Company's employees shall fulfil their legal obligation to report their suspicions regarding money laundering and terrorist financing.

## 16. Current FATF list

### 16.1. FATF Statement on High-Risk Jurisdictions subject to a Call for Action:

Following FATF's statement of 24 February 2023, on the list of "High Risk Jurisdictions subject to a Call for Action – 24 February 2023", through which it urges all jurisdictions to apply enhanced due diligence, and, in the most serious cases, countries are called upon to apply counter-measures to protect the international financial systems from the money laundering, terrorist financing, and proliferation financing (the "ML/TF/PF") risks emanating from the country. In particular, the FATF's call for action on the following high-risk jurisdictions remain in effect:

<https://www.fatf-gafi.org/content/fatf-gafi/en/publications/High-risk-and-other-monitored-jurisdictions/Call-for-action-February-2023.html>

### 16.2. FATF Statement on Jurisdictions under Increased Monitoring:

On the 24 February 2023, the FATF issued a Publication in relation to the results of the progress review to identify new countries with strategic AML/CFT deficiencies, despite the challenged posed by Covid-19, based on which:

Jurisdictions no longer subject to increased monitoring: CAMBODIA, MOROCCO.

- Albania
- Barbados
- Burkina Faso
- The Cayman Islands
- Democratic Republic of the Congo
- Gibraltar
- Haiti
- Jamaica
- Jordan
- Mali
- Mozambique
- Nigeria
- Panama
- Philippines
- Senegal
- South Africa

- South Soudan
- Syria
- Tanzania
- Turkey
- Uganda
- United Arab Emirates
- Yemen

## **17. TARGETED FINANCIAL SANCTIONS ON TERRORISM FINANCING AND UNDER OTHER UN-SANCTIONS REGIME**

RIVER PRIME LTD must ensure that the information contained in the sanctions database is updated and effected without delay. What is the definition of “without delay”? “Without delay”, in respect of maintenance of sanctions list and freezing, blocking, and rejecting is ideally within a matter of hours of designation by the United Nations Security Council (UNSC) or its relevant Sanctions Committee. The aim is to prevent the flight or dissipation of funds or other assets which are linked to terrorists, terrorist activities, financing of terrorism or financing of proliferation of weapons of mass destruction. The PREVENTION OF MONEY LAUNDERING & TERRORIST FINANCING MANUAL is expected to be updated on any changes in the UNSC or its relevant Sanctions Committee sanctions list and are accountable to ensure their sanction database is up-to-date and comprehensive.

For customers that are legal persons, RIVER PRIME LTD required to screen every director, shareholder, nominee and also company name against the United Nations Security Council Resolutions (UNSCR) Lists. RIVER PRIME LTD is required to conduct sanctions screening on existing, potential or new customers against the UNSCR Lists and Domestic List which state the names and particulars of specified / designated entities as declared by the UNSC or Minister of Home Affairs, as part of the customer due diligence process and on-going due diligence. For customers which are legal persons, RIVER PRIME LTD is required to screen the name of the customer, i.e., among others but not limited to, companies, bodies corporate, foundations, partnerships, or associations and other similar entities, as well as the beneficial owners, i.e., directors, shareholders including nominees, against the sanctions lists.

## **18. REPORTING OF SUSPICIOUS TRANSACTION**

The transactions as per the specified criterion shall be reported to AMLC – LFSa in the format prescribed by FIU. Once the AML – LFSa identify a transaction as suspicious, we have to prepare a Suspicious Transaction Report (FIU format) and provide the same to FIU, Malaysia.

The Compliance Manager is responsible for channeling all internal suspicious transaction reports received from the employees. Upon receiving any internal suspicious transaction, the Compliance Manager must evaluate the grounds of suspicion, once it is confirmed, the Compliance Manager must submit the STR. In case, there is no reasonable grounds, Compliance Manager must document and file the decision, supported by relevant documents.

The Compliance Manager must submit the suspicious transaction report in the specified STR form through the following modes:

Mail: Director Financial Intelligence & Enforcement Department

Bank Negara Malaysia, Jalan Dato'on 50480 Kuala Lumpur

(To be opened by addresses only)

Fax: +603 2693 3625

Email: str@bnm.gov.my

AND

Mail: Director Supervision and Enforcement Department Labuan Financial Services Authority

To: Anti Money Laundering Compliance Unit

(To be opened by addresses only)

Fax: +6087-411496

Email: aml@labuanfsa.gov.my

Where applicable and upon the advice of the Financial Intelligence and Enforcement Department, Bank Negara Malaysia and/or AML Compliance Unit Labuan FSA, the Compliance Manager of River Prime Ltd must submit its suspicious transaction reports on-line Website: <https://bnmapp.bnm.gov.my/fins2>

The Compliance Manager must ensure the suspicious transaction report is submitted within the next working day; from the date the Compliance Manager establishes the suspicion.

The compliance Manager must ensure that the suspicious transaction reporting mechanism is operated in secured environment to maintain confidentiality and preserve secrecy.