KJ Advanced Investment Bank

ANTI-MONEY LAUNDERING, COUNTERING FINANCING OF TERRORISM AND TARGETED FINANCIAL SANCTIONS POLICY (AML/CFT AND TFS POLICY)

TABLE OF CONTENTS

1.0 INTRODUCTION

Money laundering and terrorism financing (ML/TF) remain as threats that can undermine the credibility of international financial systems. Failure to effectively manage the ML/TF risk may result in adverse consequences for the financial institution's customers, shareholders, officers and the financial institution itself. The Anti-Money Laundering, Countering Financing Terrorism and Targeted Financial Sanctions Policy ("the Guidelines") has been establish by KAIB to act as a guideline in managing the ML/TF risk.

2.0 APPLICABILITY

The guidelines apply to all staff (including Board of Directors and Senior Management) of KJ ADVANCED INVESTMENT BANK LIMITED (hereinafter referred to as "KAIB").

3.0 APPLICATION OF RISK-BASED APPROACH

KAIB have adopted the risk-based approach methodology and implemented the Risk Assessment as below:

3.1 Business-based Risk Assessment

To identify the overall ML/TF risks arising from its business activities which include the following risk factors:

- Customer risk (e.g., resident or non-resident, type of customers, occasional or one-off, legal person structure, types of politically exposed persons (PEPs), types of occupation);
- Country or geographic risk (e.g., location of business, origin of customers);
- Products, services, transactions or delivery channels (e.g., cash-based, face-to-face or non-face-to-face, cross-border); and
- Any other information suggesting that the customer is a high-risk customer.

3.2 Relationship-based Risk Assessment

To identify the risk associated with third parties having the relationship with particularly its customers. The risk assessment is required to be done for the purpose of customer's profiling.

Appendix I and II shows the methodology used by KAIB to conduct the above risk assessments.

4.0 EMPLOYEE TRAINING AND AWARENESS PROGRAMMES

KAIB shall conduct an awareness and training programmers on AML/CFT to all the employees. Such training and awareness will be conducted regularly. The employees shall be made aware that they may be held personally liable for any failure to observe the AML/CFT requirements.

KAIB shall make available all its AML/CFT policies and procedures for all its employees and its documented AML/CFT measures shall contain, at least the following:

- the relevant documents on AML/CFT issued by competent authority or relevant supervisory authorities; and
- its internal AML/CFT policies and procedures.

The training conducted shall be appropriate depending on the employees' level of responsibilities in detecting ML/TF activities and the risks of ML / TF identified. Employees who deal directly with customers of KAIB shall be trained on AML/CFT practices and measures prior to them dealing with the customers.

KAIB shall document the provision of training (including details on the date and nature of the training given).

The scope of training shall include, at least:

- ML/TF risks;
- CDD, enhanced CDD and on-going due diligence;
- TFS screening;
- risk profiling and risk assessment;
- suspicious transaction reporting mechanism and red flags; and
- record keeping,

5.0 CUSTOMER DUE DILIGENCE ("CDD")

5.1 KAIB will conduct CDD on customers and persons conducting the transaction when:

- Establishing business relations;
- Providing wire transfer services;
- Providing electronic-money (e-money);
- It has any suspicion of money laundering or terrorism financing, regardless of the amount; or
- It has any doubt about the veracity or adequacy of previously obtained information.

5.2 When conducting CDD, KAIB will:

- identify the customer and verify the identity using reliable, independent source documents, data or information;
- identify and verify the identity of the authorised person whom acting on behalf of the customer;
- 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,
- understand, and where relevant, obtain information on the purpose and intended nature of the business relationship.

5.3 KAIB strictly does not do business with, either directly or indirectly, including facilitating transactions for or on behalf of the following sanctions target listed adopted by KAIB:

- Targeted Financial Sanctions on Terrorism Financing by Ministry of Home Affairs ("MOHA") Malaysia (known as Domestic List)
- Targeted Financial Sanctions on Proliferation Financing by and United Nations Security Council ("UNSC");
- Targeted Financial Sanctions - Other UNSC Sanctions Program
- Entities that are known or suspected to be involved in terrorism activity or its funding; or a criminal organization or members of such or persons associated with such in any capacity.
- Entities which fail to provide evidence of their identity or give rise to suspicion that the information provided is false / entities attempting to open anonymous accounts or accounts in fictitious names.

Employees are prohibited from onboarding any new customer, or continuing to deal with any existing customer, unless the requirements set out in this Manual and the relevant Regulation on AML/CFT and TFS have been met.

KAIB defines Compliance Risk based on Labuan FSA Guidelines, "Compliance Risk refers to the risk of financial losses due to legal or regulatory sanctions, or reputational loss due to its non-compliance to the applicable requirements of the laws, regulation, or code of conduct related to the Labuan Licensed Entity (LE)'s activities."

6.0 CUSTOMER VERIFICATION

KAIB shall verify and be satisfied with the identity of the customers or beneficial owner through reliable and independent documentation, electronic data or any other measures that deems necessary.

Appendix III shows Customer Identification and Verification Matrix for the mandatory information to be obtained and the supporting documents required for verification.

7.0 STANDARD CDD

7.1 Individual Customer and Beneficial Owner

In conducting CDD, KAIB shall identify an individual customer and beneficial owner, by obtaining at least the following information:

- full name;
- National Registration Identity Card (NRIC) number or passport number or reference number of any other official documents of the customer or beneficial owner;
- residential and mailing address;
- date of birth;
- nationality;
- occupation type;
- name of employer or nature of self-employment or nature of business;
- contact number and/or any contact details including email address; and

- purpose of transaction.

KAIB shall identify and verify the identity of the customer and the beneficial owner based on the guidance provided in Appendix IV herein.

7.2 Legal Persons

For a customer that is a legal person, KAIB shall identify the customer and verify its identity through the following information:

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

KAIB shall identify and verify the person authorised to represent the company including business or activities either by means of a letter of authority or directors' resolution when dealing with such person.

KAIB shall identify and take reasonable measures to verify the identity of beneficial owners according to the following sequence:

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

Where there is doubt in identifying a Legal Person and the authorized representatives, KAIB shall:

- Conduct a basic search or enquiry on the background to ensure that the person:
  - ✓ is not in the process of being dissolved or liquidated;
  - ✓ has not been dissolved or liquidated; or
  - ✓ is not a bankrupt; and
  - ✓ verify the authenticity of the information provided by the said person with the Registrar of Companies of Labuan FSA or any other relevant authorities.

For references relating to customers exempted from the above verification process, refer to Section 10.26 of the Guidelines for Labuan KRI.

7.3 Legal Arrangement

For Legal Arrangement, KAIB shall identify the customer and verify its identity through the following information:

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

KAIB shall identify and take reasonable measures to verify the identity of beneficial owners through the following information:

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

7.4 Club, Societies and Charities

For customers that are clubs, societies or charities, KAIB shall conduct CDD and require them to furnish the relevant identification documents including Certificate of Registration and other constituent documents. In addition, to identify and verify the office-bearer or any person authorised to represent the club, society or charity, as the case may be.

KAIB is also required to take reasonable measures to identify and verify the beneficial owners of the clubs, societies or charities.

Where there are doubts on the identity of persons referred at the above, KAIB shall verify the authenticity of the information provided by such person with the relevant authority1.

8.0 OTHER TYPES OF CDD

8.1 Simplified CDD

KAIB shall conduct simplified CDD for its low-risk customers. It involves obtaining basic information about the customer's identity and assessing the risk level of their activities to determine if they pose a low risk of money laundering or other illegal activities. This shall include obtaining the following information from its customer and its beneficial owner:

- full name;
- NRIC number or passport number or reference number of any other official documents of the customer or beneficial owner;
- residential and/or mailing address;
- date of birth;

[1] In relation to Malaysia, relevant authorities include the Companies Commission of Malaysia, Registrar of Societies and Legal Affairs Division under the Prime Minister's Department.

- nationality; and
- contact number and/or any other contact details including email address.

KAIB shall identify and verify the identity of the customer and the beneficial owner based on the guidance provided in Appendix IV herein.

8.2 Delayed Verification

When a customer applies to open an account or use a financial service, their identity and other information should be verified as soon as possible. However, in certain circumstance, and only where the ML/TF risks are assessed as low and verification is not possible at the point of establishing the business relationship. For example, if the customer is not physically present, or if their identity documents are not readily available.

When delayed verification applies, the following conditions must be satisfied:

- this occurs as soon as reasonably practicable (shall not exceed 10 working days);
- the delay is essential so as not to interrupt the KAIB normal conduct of business;
- the ML/TF risks are effectively managed; and
- there is no suspicion of ML/TF.

KAIB adopts risk management procedures to mitigate or address the risk of delayed verification when it allows the customer to utilise the business relationship prior to undertake verification which may include limiting the number, types and/or amounts of transactions that can be performed pending the verification.

8.3 Enhanced CDD

For higher-risk customers, such as those with political connections or in certain professions, Enhanced CDD must be conducted. This involves more extensive measures to assess the customer's background and risk profile.

In addition to all the information required to be collected required for Standard CDD above, KAIB shall also collect additional information on the customer and beneficial owner(s) as follows:

- the owner’s source of wealth and background, material ownership changes in the past 1 year, volume of assets (e.g., from public databases);
- Inquiring on the source of wealth or source of funds. In the case of PEP, both sources must be verified by obtaining the documents and certified true; and
- Obtaining approval from Senior Management before establishing (or continuing, for existing customer) such business relationship with the customer. In the case of PEPs, Senior Management refers to Senior Management of the KAIB HQ.

8.4 In relation to Politically Exposed Persons (PEPs)

Where the beneficial owner are PEPs and assessed as higher risk at the latest time of payout, the procedures is as follows:

- inform the Senior Management before the payout of the policy/certificate proceeds;

- conduct enhanced scrutiny on the whole business relationship with the policyholder; and
- consider lodging a suspicious transaction report.

8.5 Ongoing Due Diligence

In order to ensure transactions with existing customers are conducted consistent with KAIB's knowledge about the customer and their risk profile, as well as to keep the data collected up-to-date, an ongoing due diligence may be conducted taking into consideration the economic background and purpose of any transaction or business relationship which:

- appears unusual;
- is inconsistent with the expected type of activity and business model when compared to the volume of transaction;
- does not have any apparent economic purpose; or
- casts doubt on the legality of such transactions, especially with regard to complex and large transactions or involving higher risk customers.

8.6 Non-Face-to-Face Verification

"Non-face-to-face" means no meeting with the individual customer or meeting with the qualified representative of the non-individual customer. Qualified representatives of a non-individual customer include Directors, management personnel, authorised persons or employees holding a valid authorisation letter.

Where there is no face-to-face contact, to apply additional verification measures to mitigate the risk of impersonation fraud. The additional measures include but are not limited to the following:

- Conducting a video call with the customer via the official company email address prior to establishing relationship, for the purpose of comparing the physical identity of a customer with copies of original documents and to verify additional aspects of identity information collected during the identification stage;
- Obtaining copies of original documents certified by authorised persons. The documents must be signed off and date-stamped appropriately by the authorised persons with their name and designation indicated. The list of authorised persons include:
  - ✓ Solicitors;
  - ✓ Police;
  - ✓ Court officials;
  - ✓ Medical doctor;
  - ✓ Commissioner of oath; or
  - ✓ Notary public, Embassy, Consulate or High Commission of the country issuing the documentary evidence.

- Corroborating copies of original documents with independent and credible sources such as the National Registration Department database, the Immigration Department

of Malaysia databases, telecommunication companies, sanctions lists issued by credible domestic or international sources etc.

- Obtaining evidence of payment made from an account in the name of the end user with a bank incorporated and registered in Malaysia.

9.0 ELECTRONIC KNOW-YOUR-CUSTOMER ("E-KYC")

9.1 Implementation of e-KYC

KAIB may implement e-KYC subject to the approval of its Board of Directors and in accordance with the Guidelines for Labuan KRIs. The e-KYC used by KAIB includes the following elements:

- identify and verify customers information securely and effectively;
- implement the authentication factors when verifying customers identity through e-KYC (copy of personal identification, PIN number, etc);
- verify against a government issued ID by using biometric technology, fraud detection mechanism;
- ensure that the customer is a live subject and not an impersonator;
- use artificial intelligence, machine learning or other forms of predictive algorithm; and
- rely on human representative to conduct verification process in tandem with machine capabilities.

KAIB continuously address any potential vulnerabilities in the e-KYC solution by having a periodic review (at least every 1 year) with the technology providers with the aim to improve its effectiveness.

9.2 Reporting requirements of e-KYC

In monitoring the effectiveness and accuracy of e-KYC solutions utilising artificial intelligence, machine learning or other forms of predictive algorithms, KAIB shall maintain a record of the performance of the e-KYC solution segregated on a monthly basis.

KAIB shall submit the annual report to Labuan FSA by 15 January of the following year as prescribed under the Guidelines for Labuan KRIs.

10.0 TRANSACTION MONITORING

The purpose of transaction monitoring is to evaluate whether the transactions fit the profile of KAIB's customers by scrutinising the alerted transactions. This also ensures the transactions being conducted are consistent with KAIB's knowledge of the customer, their business and risk profile.

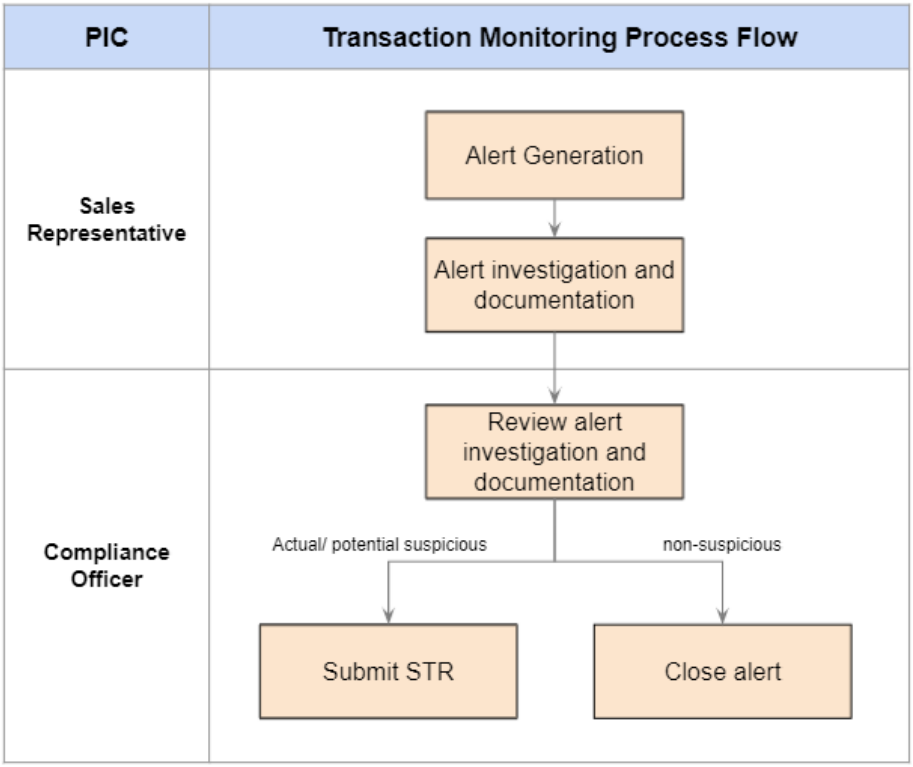
10.1 Parameters/Rules

KAIB adopts the following parameters to identify irregular transactions:

- Existence of any suspicions or any reasonable grounds of suspicions during the inception of new transactions.
- Excess repayment more than 3x of the customer's monthly instalment amount.
- Early settlement within 6 months from the loan commencement date.

The parameters are set based on the existing profile of the products offered by KAIB. The parameters and thresholds will be reassessed from time to time as KAIB acquires more customers and data in the future, or, at a minimum, on an annual basis.

Diagram below illustrates the process flow for transaction monitoring:



10.2 Alert Generated

On a monthly basis (not more than 5 working days from the end of the previous month), a report listing all the transactions for the previous month which meet the parameters/rules set will be generated. Each of the transactions will be regarded as an "alert" for further investigation.

10.3 Investigation

The process of alert investigation shall involve a minimum of 2 personnel:

- Maker – person-in-charge (i.e., the sales representative) to gather information on the transaction and also to make recommendations on whether to close the alert as non-suspicious or to escalate for further reporting based on the analysis of the information gathered. The basis for recommendation is required to be documented.
- Checker – person-in-charge (i.e., the Compliance Officer) for reviewing and making a decision on whether to close the alert as non-suspicious or to file a suspicious

transaction report ("STR") to AML Policy Unit, Policy and Digital Technology Department, LFSA and Financial Intelligence and Enforcement Department ("FIED"), BNM using the specified template in Appendix VII. All decisions by the checker are required to be documented with proper justification.

As part of the alert investigation, KAIB may approach the customers to conduct appropriate enquiry and/or to request for supporting documents, if necessary, to address the following concerns:

- Who - Who is the customer (i.e., the profile of the customer) and/ or third party involved?
- What - What is the alert (excess repayment or early settlement) or ground for suspicion and what is the amount involved?
- When - When did the transaction take place?
- Where - Where did the money come from (i.e., source of funds)?
- Why - Why is the customer conducting the transaction (making excess payment or early settlement)?

KAIB shall assess whether the information gathered commensurate with the customer profile and be vigilant in identifying red flags (Refer to Appendix 1 for a list of red flag examples) which may indicate that a particular transaction meets the following criteria for the filing of STR to FIED, BNM:

- Appears unusual;
- Has no clear economic purpose;
- Appears illegal;
- Involves proceeds from an unlawful activity or instrumentalities of an offence; or
- Indicates that the customer is involved in ML/TF.

KAIB applies a prudent basis of escalating the alerts for reporting when it fails to obtain sufficient information to satisfy that a particular transaction is non-suspicious.

The alert investigation shall be completed by the 15th day of each month. Approval from the Senior Management/Managing Director shall be sought for any extension of time required, with proper justification.

10.4 Documentation

The justification and conclusion for each alert should be documented. Clear and concise basis of conclusion for closing an alert as non-suspicious or for the filing of STR should be documented, including key information addressing the WHO, WHAT, WHEN, WHERE and WHY.

In the event that an STR is recommended to be filed, the maker should fill in the information in the specified reporting form.

11.0 REPORTING PROCESS

The Compliance Officer (i.e., the checker) is responsible for reviewing all alerts and evaluating the grounds for suspicion and subsequently, making a decision on whether a particular alert warrants the submission of STR to LFSA and BNM. To assist the Compliance Officer to determine whether a STR should be filed, the Compliance Officer is required to have access to the relevant records for that particular customer and staff should be co-operative in any request for access to records or other assistance in the review process.

The STR must be submitted to FIED, BNM within the next working day from the date the Compliance Officer establishes the suspicion. All STRs shall be submitted in the specified reporting form through the following mode:

- By accessing the Financial Intelligence System (FINS) through the following website: https://bnmapp.bnm.gov.my/fins2 ;or
- In case the Compliance Officer have yet to obtain the access to FINS, the STR may be submitted using the template form to:

Director Financial Intelligence and Enforcement Department Bank Negara Malaysia Jalan Dato' Onn 50480 Kuala Lumpur (To be opened by addressee only) Fax: +603-2691 6108 E-mail: str@bnm.gov.my	Head AML Policy Unit Policy and Digital Technology Department Labuan Financial Services Authority Level 17, Main Office Tower Financial Park Complex 87000, Jalan Merdeka (To be opened by addressee only) E-mail: aml@labuanfsa.gov.my

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

The Compliance Officer is also required to provide additional information and documentation as may be requested by LFSA BNM and to respond promptly to any further enquiries with regards to any report received under Section 14 of AMLATFPUAA. All STRs lodged and its relevant supporting documents must be kept securely and only accessible by authorised personnel.

12.0 CONFIDENTIALITY

Utmost care must be undertaken to ensure that the STRs are treated with the highest level of confidentiality. The STR reporting process should be operated in a secured environment to maintain confidentiality and preserve secrecy. Except for the purposes permitted in section 79 of the AMLATFPUAA, the disclosure of any information or matter which has been obtained by any person, in the performance of his duties or exercise of his functions is an offence under the AMLATFPUAA.

13.0 POST STR REPORTING

In the event an STR has been lodged on a customer, his/her risk rating should be elevated to "High risk" and an Enhanced CDD should be conducted to determine the next course of action. KAIB may consider exiting the business relationship with the customer should there be any heightened ML/TF risks identified, beyond the risk appetite of KAIB. Please refer to Customer Due Diligence (CDD) on the Enhanced CDD for further guidance on conducting Enhanced CDD.

14.0 RECORD KEEPING

KAIB shall maintain all records and documents of transactions, in particular, those obtained during CDD procedures, for at least six (6) years after the transaction has been completed or after the business relations with the customer have ended. This is to enable it to comply swiftly with information requests from LFSA or BNM or any law enforcement authorities for investigative purposes and to create an audit trail on individual transactions that are traceable by LFSA or BNM, the relevant supervisory and/or law enforcement agencies.

The record-keeping (in either hard and/ or soft copy) should be easily accessible and readily available and enable the Company to establish the history, circumstances and reconstruction of each transaction.

15.0 TARGETED FINANCIAL SANCTIONS ON TERRORISM FINANCING, PROLIFERATION FINANCING AND UNDER OTHER UN-SANCTIONS REGIMES

15.1 General

KAIB shall keep abreast of the relevant United Nations Security Council resolutions (UNSCR) list relating to combating the financing of terrorism, which includes:

- UNSCR 1267(1999), 1373(2001), 1988(2011), 1989(2011) and 2253(2015) which require sanctions against individuals and entities belonging or related to Taliban, ISIL (Da'esh) and Al-Qaida; and
- new UNSCR list which is published by the UNSC or its relevant Sanctions Committee as published in the United Nations (UN) website.

KAIB shall keep updated with the list of countries and persons designated as restricted end-users and prohibited end-users under the Strategic Trade Act 2010 (STA), in accordance with the relevant UNSCR relating to prevention of proliferation of weapons of

mass destruction (WMD) as published in the UN website, as and when there are new decisions by the UNSC or its relevant Sanctions Committee as listed in Appendix XI.

KAIB shall keep updated with the list of designated countries and persons under the CBA Regulations, in accordance with the relevant UNSCR relating to upholding of peace and security, through prevention of armed conflicts and human rights violations, as published in the UN website, as and when there are new decisions by the UNSC or its relevant Sanctions Committee as listed in Appendix XII.

15.2 Maintenance of Sanctions List

A Labuan KRI is required to maintain a sanctions database which comprised, at the minimum, the following:

- UNSCR list; and
- Domestic List.

16.0 REVIEW OF THE POLICY

The Policy will be reviewed annually or as and when necessary to ensure that it remains relevant and applicable.

APPENDIX I

1.0 RISK ASSESSMENT

Business-Based Risk Assessment Methodology

KAIB considers the following factors in the Business-based risk assessment to identify the risk factors that affects its business and how it addresses the impact of its overall ML/TF risk:

i. Customer Risks

Customer risks refer to the ML/TF risks arising from the profile and status of the customer, its Director(s), shareholder(s) and beneficial owner(s). The key considerations in determining the customer risks include the following:

- PEP/ RCA status
  If a customer or its Director(s), shareholder(s) and beneficial owner(s) is identified as a PEP or RCA, the customer will be classified as High risk by default as they generally present a higher risk for potential involvement in bribery and corruption by virtue of their position and the influence that they may hold.
- Form of incorporation
  An entity or legal arrangement, including trust, club, society, organisation etc. which is set up for political, religious, charity and philanthropic purposes will be automatically classified as a high-risk customer as the source of funds is generally unclear or unknown and the use of funds is more difficult to justify due to lack of commercial purpose.
- Structure of ownership
  Entities or legal arrangements with complex ownership structure which results in difficulty in identifying the beneficial owner will be considered as one of the high-risk factors.
- Adverse news
  Entities or legal arrangements with any identified adverse news relating to ML/TF or predicate offences will be considered a high-risk factor for risk profiling, if the adverse news is deemed relevant, significant and material. Guidance on assessing the relevance, significance and materiality of the adverse news is as below:

Criteria	Factors to consider
Relevance	● Time elapsed (i.e., within 7 years from assessment date) ● Credibility of the information source ● Number and frequency of events ● Scope and severity ● Relevance of the adverse news to the relationship with KAIB.
Significance	● Is there a wide-coverage of such news by the local and overseas media. ● Will establish a relationship with the KAIB to regulatory risk and reputation risk.

Materiality	● Is the news relating to any serious ML/TF crimes and/ or predicate offense under Second Schedule of AMLA ● Does the crime/ offence result in significant financial losses, multiple victims or cross jurisdictional fraud and sanctions.

ii. Geographical and Countries Risks

Geographical risks refer to the ML/TF risks of the country in which the business is incorporated, or the country in which the business is operated. Some of the considerations of classifying a country as high risk are as below:

- Countries subject to sanctions, embargoes or similar measures imposed by the OFAC, United Nations etc.;
- Countries identified as lacking appropriate AML/CFT laws, regulations, enforcement and other measures by the Financial Action Task Force ("FATF"); and
- Countries identified as non-cooperative jurisdictions for tax purposes by the European Union ("EU").

Countries which meet the criteria above will be considered as high-risk countries for the purpose of assessing the risk profile of the customers.

Customers which are incorporated or are operating in countries which meet the following criteria will be classified as High risk by default:

- Countries subject to the UNSCR or UNSC sanctions such as Iran, North Korea.

iii. Transaction and Distribution Channel risks

Channel risks refer to the ML/TF risks arising from the channels from which the customers are onboarded and the channels available for customers to perform transactions. Relationships established via non-face-to-face channels are subject to higher ML/TF risks as it is generally harder to verify the identity of the customers.

iv. Products and Services

Refers to products and services that potential risks of ML/FT associated with the products and services offered by KAIB. Some of the examples to take into account are as follows:

Nature of the products i.e., Transferability/liquidity of the products;

- Level of complexity of the products and services;
- Bearer instruments;
- Electronic money and services e.g., e-money, e-wallet etc.;
- Domestic and international private banking facilities and/or trust and asset management products/services;
- E-banking or mobile banking products and services;
- Volume of stored value cards offered with no restrictions;
- Products that return a significant portion of premiums paid as surrender value in the event of surrender or early termination;
- Products with a short maturity period;
- Payment instruments with funds transfer /cross border facility; and

- Payment instruments with cash withdrawal facility.

v. KAIB's Structure

Refers to the ML/TF risks identified from the structure of KAIB, i.e., its size, structure and nature of business. In this regard the following may be taken into account:

- Number of branches, subsidiaries and/or agents;
- Size of the Labuan KRI relative to industry/sector;
- Number and profile of employees;
- Degree of dependency on technology;
- Number of foreign correspondent financial institution accounts with inadequate AML/CFT controls, policies and procedures;
- Number of foreign correspondent financial institutions accounts located in higher risk jurisdictions;
- Level of staff turnover, especially in key personnel positions.

vi. Findings of the National Risk Assessment (NRA) or any other risk assessments issued by relevant authorities

Under the NRA, a Labuan KRI is expected to take into account the following:

- Sectors identified as highly vulnerable to ML/TF risks and the KAIB exposure to such sectors in relation to customer segments served;
- Crimes identified as high risk or susceptible to ML/TF and the adequacy of the KAIB's mitigating measures to detect and deter such illegal proceeds or in preventing dealings with customers involved in such illicit activities;
- Terrorism Financing and/or Proliferation Financing risks faced by the industry.

vii. Other risks

In addition to the risk factors above, we will also take into consideration other factors which may indicate higher ML/TF risks of the customers, for example:

- Current trends and typologies for the sector in relation to ML/TF and other crimes;
- The Labuan KRI's internal audit and regulatory findings;
- Current trends and typologies for other sectors with similar business model or product/service offerings in relation to ML/TF and other crimes;
- The number of suspicious transaction reports it has filed with the FIED, BNM and Labuan FSA; and
- Whether the Labuan KRI has been subjected to service any freeze or seize order by any law enforcement agencies pursuant to the AMLA, Dangerous Drugs (Forfeiture of Property) Act 1988, Malaysian Anti-Corruption Commission Act 2009, etc

The customer risk profiling methodology will be reviewed and updated on a periodic basis (at least annually). In addition, KAIB may also review and update the methodology on an ad-hoc basis, e.g., upon any regulatory changes or a change in KAIB's risk appetite or business model.

Relationship-Based Risk Assessment Methodology

This is the risk parameter used by KAIB to identify the risk associated to its customers for the purpose of risk profiling. KAIB may adopt the factors for Business-based risk in order to conduct the risk profiling of its customers, i.e., to consider the customer risk, geographical and countries risk, products and services, and others.

Customer Risk Profiling – for the purpose of profiling, KAIB applies 3 tier of risk level on its customers profile based on the abovementioned factors, i.e., Low, Medium and High Risk.

Based on the result of the risk profiling, the type of CDD to be conducted will be determined i.e., to use simplified CDD, standard CDD or enhanced DD.

See Appendix II (2) for sample of the Risk Assessment Template for Customer Profiling.

APPENDIX II

CUSTOMER RISK PROFILING SAMPLE

No	Key risk factors	Questions	Yes/ No
Section A: Default high risk factors			
1	Customer	Is the customer, Director(s), shareholder(s) or beneficial owner(s) identified as a PEP?	
2	Customer	Is the entity a non-profit organisation, trust or foundation (for charitable, political, religious, philanthropic purposes)?	
3	Geographical	Is the entity incorporated or operating in a country/ region subject to UNSCR or UNSC sanctions?	
4	Others	Has any STR been filed on the customer? *Note: Only applicable for existing customers.*	
Section B: Other risk factors			
5	Geographical	Is the entity incorporated or operating in a high-risk country?	
6	Channel	Is the customer onboarded via a non-face-to-face channel?	
7	Customer	Does the entity have a complex structure which leads to difficulty in identifying the beneficial owners?	
8	Customer	Is there any relevant, material and significant adverse news identified from name screening or other sources?	
9	Others	Are there any other high-risk factors observed? E.g. ● Challenges in verifying the identity of the customer, Director, shareholder or beneficial owner/ non-cooperative ● Unilateral termination of business relationship by other financial institutions ● Third party representation which appears unrelated to the customer ● Others (Please specify):_____	

Customer risk rating (based on Section A and Section B):		
High risk □	**Medium risk** □	**Low risk** □
Final customer risk rating (manual adjustment, if applicable):		
High risk □	**Medium risk** □	**Low risk** □
Reasons for manual adjustment:		

Notes:

1. If the answer for any of the questions under *Section A: Default high risk factors* is a "Yes", the customer will be automatically classified as High risk.
2. If none of the answers for *Section A: Default high risk factors* is "Yes", the risk rating of the customer will be subject to the responses under *Section B: Other risk factors* as below:

Customer risk rating	**No. of "Yes"**
High risk	2 or more
Medium risk	1
Low risk	0

3. The customer risk rating derived from Section A and Section B may be manually adjusted **higher** (e.g., from Low risk to Medium or High risk; or from medium risk to High risk), if there are reasons to believe that the customer is of higher ML/TF risks. Manual adjustment to a lower risk rating is not permissible.

Approval Item	**Customer risk rating**	**Recommendation by Compliance[N1] required?**	**Minimum approving authority**
Establishment of business relationship	Low	No	Managing Director
	Medium	No	Managing Director
	High	Yes	Managing Director
Delayed verification	Low	Yes	Managing Director
	Medium	- N/A -	- N/A -
	High	- N/A -	- N/A -
Periodic review	Low	- N/A -	- N/A -
	Medium	No	Managing Director
	High	Yes	Managing Director
Trigger event review	Low	Yes	Managing Director
	Medium	Yes	Managing Director
	High	Yes	Managing Director

APPENDIX III

CUSTOMER IDENTIFICATION AND VERIFICATION MATRIX

Role	*CDD information to be identified*	*Verification*	*Documents for verification*
Customer ● Sole proprietorship ● Partnership ● Private limited company (Sdn Bhd) ● Public limited company (Bhd) ● Government-linked companies ● Unincorporated Joint Venture (JV) ● Trust ● Club/ Society/ Charity/ Foundation/ Cooperative/ Non-government organisation/ Non-profit organisation	1) Full name, including alias and former name 2) Legal form/ entity type classification 3) Registered address 4) Business/ Operating address 5) Business registration number 6) Date of registration 7) Nature of business 8) Power that regulate and bind the customer such as Directors' resolution, as well as the names of relevant persons having a Senior Management position 9) Ownership and control structure 10) Contact number 11) Country of business activity 12) Purpose of relationship/ transactions	Items 1-9	1) Company constitutional documents (e.g., certificate of incorporation, registration deed, partnership deed, enabling registration such as statutory bodies under certain Act); 2) Company search, including searches perform via reliable 3rd party vendor (e.g., SSM, Ramci, SME Credit Bureau, Bureau Van Dijk, etc.); and 3) Audited annual report *Note: In the event that the above-mentioned documents are unavailable, customer's declaration signed off by a Director or a reliable independent person is acceptable.*
Beneficial Owner[N3] a) Natural person with ≥25% effective shareholding	1) Full name, including alias and former name 2) Identification number 3) Date of birth 4) Nationality 5) Residential and mailing address 6) Occupation type	Items 1- 4	1) Malaysian – National Registration Identity Card; Non-Malaysian - Government issued valid passport; 2) Company constitutional documents (e.g., Form 24, Form 32A, Superform, annual return, etc.);

b) Natural person who exercises ultimate effective control over the entity	7) Employer name 8) Occupation sector 9) Contact number *Note: In the event where beneficial owner (a) has been identified, the required CDD information to be identified for Senior Management are limited to items 1-5 only.*		3) Company search, including searches perform via reliable 3rd party vendor (e.g., SSM, Ramci, SME Credit Bureau, Bureau Van Dijk, etc.); or 4) Audited annual report *Note: In the event that the above-mentioned documents are unavailable, customer's declaration signed off by a Director or a reliable independent person is acceptable.*
Person conducting transaction on behalf of customer, whichever is applicable and with equivalent roles: ● Mandate ● Power of Attorney ● Liquidator ● Authorised signatory **Other related parties (natural persons)** such as: ● Directors ● Guarantors	1) Full name, including alias and former name 2) Identification number 3) Date of birth 4) Nationality 5) Residential and mailing address 6) Occupation type 7) Employer name 8) Occupation sector 9) Contact number	Items 1- 4	1) Malaysian – National Registration Identity Card; Non-Malaysian - Government issued valid passport; 2) Company constitutional documents (e.g., Form 24, Form 32A, Superform, annual return, etc.); 3) Company search, including searches perform via reliable 3rd party vendor (e.g., SSM, Ramci, SME Credit Bureau, Bureau Van Dijk, etc.); or 4) Audited annual report *Note: In the event that the above-mentioned documents are unavailable, customer's declaration signed off by a Director or a reliable independent person is acceptable.*
Other related parties (legal persons) such as: ● Guarantors	1) Full name, including alias and former name 2) Legal form/ entity type classification 3) Registered address	Items 1- 7	1) Company constitutional documents (e.g., certificate of incorporation, registration deed, partnership deed, enabling registration such

	4) Business/ Operating address 5) Business registration number 6) Date of registration 7) Nature of business 8) Contact number		as statutory bodies under certain Act); 2) Company search, including searches perform via reliable 3rd party vendor (e.g., SSM, Ramci, SME Credit Bureau, Bureau Van Dijk, etc.); and 3) Audited annual report. *Note: In the event that the above-mentioned documents are unavailable, customer's declaration signed off by a Director or a reliable independent person is acceptable.*
Immediate and intermediate corporate shareholder	1) Full name, including alias and former name	N/A	N/A

APPENDIX IV

1.0 IDENTIFICATION AND VERIFICATION OF BENEFICIAL OWNERSHIP

Method to identify the BO:

Entity type	Examples of individual(s) to be identified as BO
Partnership	● With partnership deed/ agreement: Partner with 25% or more shareholdings ● Without partnership deed/ agreement: All partners
Private Limited/ Sdn Bhd	● Shareholder (direct/ indirect) with 25% or more effective shareholdings
Limited Company/ Bhd (publicly listed)	● Senior Management (e.g., Chairman/ Managing Director / CFO, etc.)
Limited Company/ Bhd (none publicly listed)	● Senior Management (e.g., Chairman / CEO / CFO, etc.) ● Shareholder (direct/ indirect) with 25% or more effective shareholdings
Unincorporated Joint Ventures	● Senior Management (e.g., Board of representatives, etc.) ● Shareholder (direct / indirect) with 25% or more effective shareholdings
Trust	● Settlor ● Trustee ● Protector ● Beneficiaries
Club/ Society/ Charity/ Foundation/ Cooperative/ Non-government organisation/ Non-profit organisation	● Officer bearers (e.g., Chairman/ President, secretary, treasurer, and their vice/ deputy/ assistant etc.) ● Individual who will receive the assets/ funds upon dissolution of the entity (if this is specified in any of the entity's official document ● Donor/ Founder (if applicable)
Government-linked entities	● Senior Management (e.g., Managing Director, CEO, CFO, authorised representatives, etc.)

Method to Verify the BO information:

Individual	Legal Person/Legal Arrangement
To verify and be satisfied with the identity of the beneficial owner through reliable and independent documentation, electronic data or any other measures that the reporting institution deem necessary, for example: • Identity Card issued by Malaysian government • Employee Identity Card issued by ministries and statutory bodies • Foreign passport or identity card issued by the United Nations • Documents issued by Malaysian government • Biometric identification • Organisation that maintains reliable and independent electronic data to verify customer's identity	To verify the identity of directors/shareholders with equity interest of more than 25% / Partners through the following documents, for example: • Sections 58 and 78 Forms as prescribed by the Companies Commission of Malaysia or equivalent documents for Labuan companies or foreign incorporations • Other equivalent documents for other types of legal person • Authorisation for any person to represent the company • Letter of authority or directors' resolution.

Notes: Subject to exemption provided under the Guidelines for Labuan KRIs.