

**SPB DEVELOPMENT BERHAD**  
**ANTI-MONEY LAUNDERING POLICY**

**1. INTRODUCTION**

- 1.1 SPB Development Berhad (“**Company**”) and its subsidiaries (“**Group**”) is committed to uphold its stakeholders’ trust by adhering to the highest ethical standards of business conduct in accordance with, amongst others, the Anti-Money Laundering, Anti-Terrorism Financing and Proceeds of Unlawful Activities Act 2001 (“**AMLATFA**”).
- 1.2 The Group strongly objects to all practices related to money laundering which includes dealing in the proceeds of illegal and criminal activities and/or terrorism financing.
- 1.3 This Anti-Money Laundering Policy (“**Policy**”) provides a framework for compliance with applicable laws and regulatory guidelines in reporting of any suspicious transactions or activities within the Group.
- 1.4 This Policy should be read in conjunction with the Company’s Code of Conduct and Business Ethics and the Whistleblowing Policy which are available on the Company’s website at [www.spb-property.my](http://www.spb-property.my).

**2. OBJECTIVES**

- 2.1 The objectives of this Policy are as follows:
  - (a) to set out the responsibilities of the Group to comply with laws against money laundering;
  - (b) to establish the general framework to manage and prevent the risks of the Group’s businesses from being used as a conduit for money laundering and terrorism financing activities; and
  - (c) to provide information and guidance to those working for or dealing with the Group on how to recognise money laundering and terrorism financing issues and the procedures in dealing with such issues.

**3. SCOPE AND APPLICATION**

- 3.1 This Policy applies to all employees who are employed by or work for the Group (whether in or outside Malaysia and whether permanent, contract or temporary basis), Directors, (executive and non-executive), Company Secretaries and Board Committees’ members of the Company/Group (collectively “**Employees and Personnel**”) and all business units or entities in the Group especially those which fall under the definition of “Reporting Institutions” as described in the First Schedule of the AMLAFTA.
- 3.2 All Employees and Personnel are expected, as part of their normal duties, to do the following:
  - (a) familiarise themselves with and comply with this Policy and any policy and procedures which apply to their jobs issued and revised by the Group from time to time;
  - (b) participate in any anti-money laundering training provided by the Group; and
  - (c) immediately report any actual or suspected money laundering or allegation of money laundering which come to their attention to their head of department or superior.

3.3 This Policy is intended to supplement all applicable laws, rules and other internal policies and is not intended to supplant any local or international laws.

#### **4. MONEY LAUNDERING OFFENCE AND PENALTY UNDER THE AMLATFA**

4.1 Pursuant to Section 4 of the AMLATFA, a money laundering offence is committed when a person:

- (a) engages, directly or indirectly, in a transaction that involves proceeds of an unlawful activity or instrumentalities of an offence;
- (b) acquires, receives, possesses, disguises, transfers, converts, exchanges, carries, disposes of or uses proceeds of an unlawful activity or instrumentalities of an offence;
- (c) removes from or brings into Malaysia, proceeds of an unlawful activity or instrumentalities of an offence; or
- (d) conceals, disguises or impedes the establishment of the true nature, origin, location, movement, disposition, title of, rights with respect to, or ownership of, proceeds of an unlawful activity or instrumentalities of an offence.

4.2 Any person who commits a money laundering offence under the AMLATFA shall on conviction be liable to:

- (a) imprisonment for a term not exceeding fifteen (15) years; and
- (b) a fine of not less than five (5) times the sum or value of the proceeds of an unlawful activity or instrumentalities of an offence at the time the offence was committed or RM5 million, whichever is the higher.

#### **5. TERRORISM FINANCING OFFENCE UNDER THE AMLATFA**

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

- (a) providing or collecting property for terrorist acts;
- (b) providing services for terrorism purposes;
- (c) arranging for retention or control of terrorist property; or
- (d) dealing with terrorist property.

#### **6. ANTI-MONEY LAUNDERING AND ANTI-TERRORISM FINANCING ACTIVITIES**

6.1 Money laundering and terrorism financing activities are serious crimes and the penalties for breaching the AMLATFA are severe. Involvement in such activities damages our reputation and integrity.

6.2 As a general rule, reasonable degree of due diligence must be carried out in order to understand the business and background of any prospective customer, vendor, third party or business partner that intends to do business with the Group to determine the origin and destination of money or assets involved.

- 6.3 The Group prohibits all involvement in money laundering activities and terrorism financing either directly or indirectly. Such activities include but not limited to the following:
- (a) payments made in currencies that differ from invoices;
  - (b) attempts to make payment in cash or cash equivalent (out of normal business practice);
  - (c) payments made by third parties that are not parties to the contract; and
  - (d) payments to or from accounts of third parties that are not parties to the contract.
- 6.4 The Group shall ensure full compliance with the obligations stipulated under Part IV of the AMLATFA which include the requirements to:
- (a) implement risk management that commensurate with the level of money laundering and terrorism financing risks;
  - (b) conduct customer due diligence;
  - (c) keep proper record on the customer and transactions;
  - (d) implement anti-money laundering and terrorism financing compliance program;
  - (e) report suspicious transaction report (“**STR**”); and
  - (f) report cash threshold report (“**CTR**”) for cash transaction exceeding the amount specified, where applicable.
- 6.5 The Group shall perform customer due diligence (“**CDD**”) procedures when:
- (a) at the start of a new business relationship;
  - (b) it has any suspicion of money laundering or terrorism financing activities regardless of the amount transacted; or
  - (c) it has any doubt about the adequacy or authenticity of previously obtained information.
- 6.6 The Group shall adopt a risk-based approach when deciding the degree of CDD to apply. Risks are assessed at the outset of a business relationship and updated regularly.
- 6.7 The CDD procedures should minimally include:
- (a) identifying the customer (including foreign body corporate) and verify such customer’s identity using reliable, independent source of documents, data or information;
  - (b) verifying that any person purporting to act on behalf of the customer is authorised, and identifying and verifying the identity of that person;
  - (c) identifying and take reasonable measures to verify the identity of the beneficial owner(s), using relevant information or data obtained from reliable sources;
  - (d) understand and, where relevant, obtain information on the purpose of opening an account and the intended nature of the business relationship; and
  - (e) where necessary, performing appropriate background checks, where practical and relevant, on the names of individuals or entities of customers to ensure that transactions are not entered

with those listed on the sanction lists maintained by Ministry of Home Affairs (“MOHA”) and United Nations Security Council.

## 7. SUSPICIOUS TRANSACTION REPORTING

7.1 If any Employee and Personnel suspects or has evidence of any activity in violation of this Policy or any attempted transaction which fits the list of “Red Flags” which includes, but not limited to the following:

- (a) reluctance to provide detailed information of the source of income;
- (b) large cash transaction with no history of prior business experience;
- (c) shielding the identity of the beneficial owners;
- (d) the transaction appears illegal or is not economically justified considering the customer’s business or profession;
- (e) repayment of loan instalments with multiple cash transactions;
- (f) early settlement of loan by multiple transferring of funds from third party or foreign bank accounts; and
- (g) multiple cash repayments that were structured below the reporting requirements to avoid detection,

he or she shall immediately make a report to the following persons by post or via email as set out below:

	By Post	Via Email
If writing to the Chairman of the Board of Directors (“ <b>Board Chairman</b> ”)	Address:  No.16 & 17, Plaza Seri Kubu, Jalan Tan Chay Yan, 75300 Melaka.  Attention to: The Board Chairman	boardchairman@spb.my  Attention to: The Board Chairman
If writing to the Chairman of the Audit and Risk Management Committee (“ <b>ARMC Chairman</b> ”)	Address:  No.16 & 17, Plaza Seri Kubu, Jalan Tan Chay Yan, 75300 Melaka.  Attention to: The ARMC Chairman	armcchairman@spb.my  Attention to: The ARMC Chairman

7.2 Protection will be given in pursuant to the Whistleblower Protection Act 2010 and the Group's Whistleblowing Policy. All notifications will be treated as confidential unless otherwise required by law or the purpose of any proceedings by or against the Group.

## **8. RECORDS KEEPING AND RETENTION OF RECORDS**

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

- (a) documents relating to the identification of the customer for transaction executed;
- (b) the identification of the beneficial owner for transaction executed;
- (c) records of the relevant account pertaining to the transaction executed;
- (d) the type and details of transaction involved;
- (e) the origin and the destination of the funds, where applicable; and
- (f) any other information as required by the authorities.

8.2 The Group is required to retain for at least seven (7) years, the records of transactions, relevant customer due diligence information and other relevant records including agreements, financial accounts, business correspondences and documents relating to the transactions in a form that is admissible as evidence in court and make such documents available to authorities and law enforcement agencies in a timely manner.

## **9. REVIEW AND APPROVAL OF POLICY**

9.1 The ARMC is responsible for regular reviews of this Policy, at least once every three (3) years, and making any recommended changes to ensure that it continues to remain relevant, appropriate and consistent with the Group's practices or any other applicable regulatory requirements.

9.2 Any revisions and/or changes to the terms of this Policy as recommended by the ARMC shall be subject to the approval of the Board.

9.3 The Board should disclose the application of this Policy in the annual report and on the corporate website of the Company.

This Policy is approved and adopted by the Board on 18 July 2024.