ANTI-MONEY LAUNDERING POLICY

SUMISAUJANA GROUP BERHAD
COMPANY NO: 202101023259 (1423559-T)

12 FEBRUARY 2025

Table of Contents **Pages**

ANTI-MONEY LAUNDERING POLICY

1.0 INTRODUCTION

SumiSaujana Group Berhad (the "Company") and its subsidiaries ("SumiSaujana" or the "Group") are committed to maintaining high ethical standards while preventing and detecting all criminal activities, including money laundering.

This document outlines the policy and procedure to follow in the event of suspected money laundering and defines the responsibilities of the Board of Directors ("Board"), Key Senior Management ("KSM") and employees of SumiSaujana throughout the process.

This Anti-Money Laundering Policy ("Policy") is a preventive measure in accordance with the Anti-Money Laundering, Anti-Terrorism Financing, and Proceeds of Unlawful Activities Act 2001, as well as the latest Guidelines on Anti-Money Laundering, Countering Financing of Terrorism, and Targeted Financial Sanctions for Designated Non-Financial Businesses and Professions (DNFBPs) and Non-Bank Financial Institutions (NBFIs), issued by Bank Negara Malaysia on 31 December 2019 ("BNM Guidelines"). The Group recognises the dangers and impact of these financial crimes, along with their harmful socio-economic effects on the nation.

2.0 POLICY STATEMENT

SumiSaujana strongly opposes all practices related to money laundering, including dealings in the proceeds of criminal activities, terrorism financing and proliferation financing. A reasonable degree of due diligence must be conducted to understand the business and background of any prospective customer, vendor, third party or business partner that intends to do business with SumiSaujana to determine the origin and destination of money or assets involved.

3.0 SCOPE

This Policy applies to all members of the Group, including the Board, Key Senior Management, and employees. It covers activities undertaken both in Malaysia and internationally, in relation to the direct and indirect operations of the Group.

Any member of the Group could potentially be committing an offence under money laundering laws if they suspect money laundering or become involved in such activities and fail to take appropriate action.

4.0 PURPOSE

This Policy outlines the Group's measures to comply with the requirements of the money laundering regulations, which include:

- **Customer Verification:** Obtaining satisfactory evidence of the identity of each customer with whom the Group has a business relationship. This evidence, along with transaction details, must be retained for a minimum of seven (7) years from the date the account is closed or the business relationship ends.

- **Suspicious Transaction Reporting:** Requiring all members of the Group to prevent, detect and report any suspicious transactions related to money laundering, terrorist financing, or other illegal activities.

- **Regulatory Compliance:** Ensuring that any suspicion of money laundering is appropriately reported to the relevant authorities, particularly the Financial Intelligence Unit ("FIU") within the Financial Intelligence and Enforcement Department of Bank Negara Malaysia. The FIU is responsible for managing and conducting comprehensive analysis of financial intelligence related to money laundering and terrorism financing.

5.0 DEFINITION OF MONEY LAUNDERING AND TERRORIST FINANCING

- **Money laundering** refers to the process of converting cash or property derived from criminal activities to give it a legitimate appearance. It involves 'cleaning dirty money' to disguise its criminal origin.

- **Terrorism financing** refers to providing financial support to terrorists or terrorist organisations, whether funded from legitimate or illegitimate sources.

While most funds originate from criminal activities, they may also be derived from legitimate sources, such as salaries, revenues generated from legitimate businesses, or the use of non-profit organisations to raise funds through donations.

6.0 PROCEDURES

6.1 Responsibilities of the Directors, Key Senior Management and Finance Personnel

The Board, Key Senior Management and Finance personnel are responsible for:

- Receiving reports of suspicious activities and maintaining a register of all reports received.

- Evaluating reports to determine whether there is evidence of money laundering or terrorist financing.

- Reporting any suspicious activity or transactions to the FIU if the matter is not addressed internally.

6.2 Responsibilities of All Employees of SumiSaujana

All employees of SumiSaujana are required to:

- Avoid handling money, goods, or other items associated with criminal activities.
- Remain vigilant and report concerns related to suspected money laundering activities.
- Fully cooperate with any investigations into reported concerns.

6.3 Risk Management Procedures

The Group integrates risk management into its business operations, including:

- Risk assessment procedures;
- Know Your Customer (KYC) due diligence;
- Supplier evaluation procedures;
- Ongoing monitoring customers and suppliers;
- Recordkeeping of transactions (sales and purchases);
- Reporting of suspicious transactions;
- Training and awareness for employees regarding internal control systems; and
- Internal audit functions.

6.4 Anti-Money Laundering Due Diligence Procedures

The Procurement Department, assisted by Finance Department, is responsible for conducting Anti-Money Laundering due diligence when onboarding potential suppliers, vendors, and business partners. This includes:

- **Risk Assessment:** Evaluating the business background, ownership structure, and any previous involvement in illicit activities.
- **KYC Procedures:** Ensuring proper KYC checks are performed to verify the identities of suppliers and partners.
- **Ongoing Monitoring:** Monitoring the business relationship for suspicious activities.

- **Suspicious Transaction Reporting:** Reporting any suspicious activities to relevant authorities.

7.0 REPORTING

All members of SumiSaujana are required to report any suspicious transactions that have been, or are about to be, used for money laundering, terrorist financing, or other illegal activities to:

- **Email:**
  - Finance Department: finance@sumisaujanagroup.com; or
  - Chairman of the Audit and Risk Management Committee ("ARMC"): armcchairman@sumisaujanagroup.com

- **Post:**
  Finance Department / Chairman of ARMC,
  No. 57, Jalan TIAJ 2/1,
  Taman Industri Alam Jaya,
  42300 Puncak Alam, Selangor.

- **Phone:** +603 – 6039 7768

8.0 DISCIPLINARY PROCEDURES

SumiSaujana will initiate disciplinary procedures against any employee found to have committed a money laundering offence, which could result in dismissal.

9.0 REVIEW

The ARMC will review and/or update this Policy at least once every three (3) years or when there are amendments to the AMLR or any other applicable laws and regulations. This is to ensure the Policy remains relevant, appropriate and consistent with the Group's practices, AMLR, and other regulatory requirements. Any revisions recommended by the ARMC will be submitted to the Board for consideration and approval.

This Policy was reviewed, approved and adopted by the Board on 12 February 2025.

APPENDIX 1: EXAMPLES OF "RED FLAGS"

The examples below are not exhaustive but provide a general indication of the types of matters covered by this policy.

- Payment by an individual or company of any substantial sum in cash, especially if they fail to provide proper evidence to confirm their identity and address.
- A person or company conducting business without proper documentation, e.g. missing invoices, failure to provide an SST number, or invoices issued by a company that lacks the company lacking a registered address or company number.
- A person or company attempting to engage in circular transactions, where payment is followed by an attempt to obtain a refund from company's bank accounts.
- Unusual or unexpected large payments made into the company's bank accounts.
- A secretive person or business that refuses to provide the requested information without a reasonable explanation.
- Absence of any legitimate source for funds received.
- Overpayments with no apparent reason.
- Involvement of an unconnected third party without a logical reason or explanation.
- Significant, unexplained changes in the size, nature, or frequency of transactions with a customer.
- Requests for payments or refunds after funds have been paid into the company's bank account by a third party, particularly if there is a request to return money to a different account or individual than the payer.
- Cancellation, reversal, or requests for refunds of previous transactions.
- Funding is received from entities such as Non-Governmental Organisations ("NGOs"), and all or part of the funds are used to pay for services provided by the NGO or by entities that are directly connected to the NGO.
- Payments made in currencies that differ from those on the invoices.
- Attempts to make payments in cash or cash equivalents (out of normal business practice).
- Payments to or from accounts of third parties who are not parties to the contract.

- Repayment of loan instalments through multiple cash transactions or multiple cash repayments structured below the reporting threshold to avoid detection.