ANTI-MONEY LAUNDERING POLICY

SUMISAUJANA TCM CHEMICALS SDN. BHD.
COMPANY NO: 201001023293 (907064-U)

MARCH 14, 2024

1.0 POLICY AND PROCEDURE STATEMENT

Sumisaujana TCM Chemicals Sdn. Bhd. (SSTCM) is committed to high standards of ethical behaviours, and the prevention and detection of all criminal activities, including money laundering.

This document sets out the policy and procedure to be followed if money laundering is suspected, and defines the responsibilities of the Board, management and employees of SSTCM in the process. This policy serves as preventive measures in accordance with the Anti-money Laundering, Anti-terrorism Financing and Proceeds of Unlawful Activities Act 2001 and the latest Guidelines on Anti-Money Laundering, Countering Financing of Terrorism and Targeted Financial Sanctions for the Designated Non-Financial Businesses and Professions (DNFBPs) & Non-Bank Financial Institutions (NBFIs) issued by the Bank Negara Malaysia on 31 December 2019 ("BNM Guidelines"). The Company understands the dangers and impact of these financial crimes and the deleterious socio-economic effects on the nation.

2.0 PURPOSE AND SCOPE

This Anti-Money Laundering Policy applies to all members of SSTCM, namely:

- Board of Directors
- Management and employees of SSTCM

This policy covers the activities undertaken in Malaysia or overseas, in relation to the direct and indirect activities of SSTCM. Potentially any of the members of SSTCM could be committing an offence under the money laundering laws, if they suspect money laundering or if they become involved in some way and do nothing about it.

This policy outlines SSTCM's arrangements to comply with the requirements of the money laundering regulations which are:

To obtain satisfactory evidence of the identity of each customer dealt with and/or has a business relationship. This evidence of a customer's identity and the details of transactions must be retained for at least seven (7) years from the date the account is closed or the business relationship, transaction or activity is completed or terminated.

To require all the members of SSTCM to prevent, detect and report any suspicious transactions that have been or are about to be used for money laundering, terrorist financing and other illegal activities.

To report suspicion of money laundering, if deemed appropriate, by the Board of SSTCM to the appropriate authorities in Malaysia, namely the Financial Intelligence Unit ("FIU"), established within the Financial Intelligence and Enforcement Department in Bank Negara Malaysia. The FIU will manage and provide comprehensive analysis on the financial intelligence received relating to money laundering and terrorism financing.

WHAT ARE MONEY LAUNDERING AND TERRORIST FINANCING?

Money laundering is a process of converting cash or property derived from criminal activities to give it a legitimate appearance. It is a process to clean 'dirty' money in order to disguise its criminal origin.

Terrorism financing is the act of providing financial support, funded from either legitimate or illegitimate sources, to terrorists or terrorist organisations to enable them to carry out terrorist acts or to benefit any terrorist or terrorist organisation.

While most of the funds originate from criminal activities, they may also be derived from legitimate sources; for example, through salaries, revenues generated from a legitimate business or the use of non-profit organisations to raise funds through donations.

3.0 PROCEDURES

The Directors, Senior Managers and Finance personnel are responsible for implementing and maintaining anti-money laundering procedures and responding to reports of suspected money laundering activities.

The Directors, Senior Managers and Finance personnel are responsible for:

- Receiving reports of suspicious activities and maintaining a Register of all suspected money laundering reports received;
- Considering all reports and evaluating whether there is - or seems to be - any evidence of money laundering or terrorist financing;
- Reporting any suspicious activity or transactions to the FIU if the Governance Body of SSTCM failed to take actions or investigate the reported transactions;

All members of SSTCM shall discharge their duties in accordance with this policy, as follows;

- To avoid handling any money, goods or other items known or suspected to be associated with the proceeds of crime, or becoming involved with any services known or suspected to be associated with the proceeds of crime;
- To remain vigilant and report concerns related to suspected money laundering activities;
- To co-operate fully with any investigations into reported concerns;

The members shall use their best endeavours to meet the requirements imposed and all applicable laws to commensurate with the nature of the SSTCM's businesses and activities. The Risk Management functions shall form as part of its business operations of the following:

- Risk assessment policies and procedures
- Know Your Customer (KYC) Due Diligence policies and procedures
- Supplier evaluation policies and procedures
- Ongoing monitoring processes of customers and suppliers
- Record keeping of transactions (sales and purchases)
- Suspicious transaction reporting procedures
- Monitoring system of compliance with the internal control policies, procedures and systems
- Awareness training for employees in respect to the internal control policies, procedures and systems including Standard Operating Procedures
- Internal audit functions

4.0 REPORTING

All the members of SSTCM may report any suspicious transactions that have been or are about to be used for money laundering, terrorist financing and other illegal activities to the Directors, Senior Managers and Finance personnel.

5.0 DISCIPLINARY PROCEDURES

SSTCM may follow disciplinary procedures against any employee who has committed a money laundering offence, which could result in dismissal.

6.0 MONITORING AND REVIEW

This policy shall be reviewed and updated by the Board at least once every three years, or when necessary. Any incidents of money laundering reported to, and recorded will be incorporated into that review.

7.0 EXAMPLES OF "RED FLAGS"

The examples below are not intended to be exhaustive but provide a general indication of the range of matters covered by this Policy.

- Payment by a person or company of any substantial sum in cash, particularly if they fail to provide proper evidence to confirm their identity and address.
- A person or company doing business which lacks proper paperwork, e.g. invoices, failure to quote an SST number or invoices issued by a company that lacks the company's registered office/address and number.
- A person or company attempts to engage in circular transactions, where payment is followed by an attempt to obtain a refund from 's bank accounts.
- Unusual or unexpected large payments are made into the 's bank accounts.
- A secretive person or business e.g. that refuses to provide the requested information without a reasonable explanation.
- Absence of any legitimate source for funds received.
- Overpayments for no apparent reasons.
- Involvement of an unconnected third party without a logical reason or explanation.
- Significant changes in the size, nature, frequency of transactions with a customer that is without reasonable explanation.
- Requests for payments or refunds after funds have been paid into the 's bank account by a third party, particularly if there is a request to return money to a different account or individual to the payer.
- Cancellation, reversal or requests for refunds of earlier transactions.
- Funding is received from an organisation/NGO or entities in which all/part of the fund is then used to pay services provided by the organisation/NGO or entities directly related to the funding organisation/NGO.