SUNWAY®

SUNWAY BERHAD

ANTI-MONEY LAUNDERING, COUNTERING FINANCING OF TERRORISM AND COUNTERING PROLIFERATION FINANCING POLICY

(AML/CFT/CPF POLICY)

Edition 3.0 (October 2024)

Process Owner: Group Risk & Compliance

Intended Users: Sunway Group – All Users

COMMITTED TO SUSTAINABLE DEVELOPMENT GOALS

Approved by Board of Directors on 26 November 2024

CONTENTS

1. INTRODUCTION AND PURPOSE

1.1. **Money laundering is the process of introducing money, property or other assets derived from illegal and criminal activities into the legal financial and business cycle to give it a legitimate appearance. It is a process to clean 'dirty' money in order to disguise its criminal origin.** Money Laundering is an offence under the Anti-Money Laundering, Anti-Terrorism Financing and Proceeds of Unlawful Activities Act 2001 ("the **AMLATFA**") and the Guidelines on Prevention of Money Laundering, Countering Financing of Terrorism, Countering Proliferation Financing and Targeted Financial Sanctions for Reporting Institutions in the Capital Market, issued by the Securities Commission Malaysia ("**SC**"), as amended from time to time ("**AML/CFT/CPF Guidelines**").

1.2. The purpose of this Anti-Money Laundering, Counter Financing of Terrorism and Countering Proliferation Financing (''**AML/CFT/CPF**'') Policy is to provide guidance to all SUNWAY employees concerning how to strengthen anti-money laundering governance and it reiterates SUNWAY's commitment to full compliance to the AMLATFA and AML/CFT/CPF Guidelines. This Policy complements and should be read in conjunction with our Code of Conduct and Business Ethics (CCBE) and our Whistleblowing Policy, copies of which can be obtained from our website at www.sunway.com.my.

2. SCOPE

2.1. This Policy establishes the general framework to manage and prevent the risks of SUNWAY's businesses from being used as a conduit for money laundering, terrorism financing or proliferation financing activities. All Sunway employees are required to adhere to the requirements of this Policy when carrying out their daily responsibilities.

2.2. This Policy applies to all Sunway business units or entities especially those which fall under the definition of "Reporting Institutions" as described in the First Schedule of the AMLAFTA.

The standards set out in this policy are the minimum requirements for all SUNWAY's businesses. Detailed policies on AML/CFT/CPF for the Group's businesses in money services, leasing, money lending and factoring are maintained by Sunway Money Sdn Bhd, Sunway Leasing Sdn Bhd and Sunway Credit Sdn Bhd respectively.

2.3 In addition, we shall comply with all applicable laws and regulations regarding to anti-money laundering, counter-terrorism financing and proliferation financing in all jurisdictions where we operate.

3. DEFINITIONS

AML/CFT/CPF	Anti-Money Laundering, Counter Financing of Terrorism and Counter Proliferation Financing
TFS-PF	Targeted Financial Sanctions relating to Proliferation Financing
UNSCR	United Nations Security Council Resolution
Employees	All employees including directors of the company and its subsidiaries.
Family Members	Includes your spouse(s), children (including step-children and adopted children), parents, step-parents, siblings, step-siblings, grandparents, grandchildren, in-laws, uncles, aunts, nieces, nephews, and first cousins, as well as other persons who are members of your household.
Designated Person	means a person who has been designated under the Second Schedule of the Strategic Trade (Restricted End-Users and Prohibited End-Users) Order 2010 (P.U. (A) 484/2010).
Senior Management	refers to any person having authority and responsibility for planning, directing or controlling the activities of a reporting institution or a legal person or legal arrangement including the management and administration of a reporting institution, legal person or legal arrangement.

The remainder of this page intentionally left blank.

4. GENERAL DESCRIPTION OF MONEY LAUNDERING[1]

4.1. In principle, money laundering generally involves proceeds of unlawful activities that are related directly or indirectly, to any serious offence, that is processed through transactions, concealments, or other similar means, so that they appear to have originated from a legitimate source.

4.2. The process of money laundering comprises three stages, during which there may be numerous transactions that could alert a business unit (especially a reporting institution) to the money laundering activities. These stages are:

a) **Placement:** The physical disposal of proceeds / benefits of unlawful activities by introducing illegal funds (generally in the form of cash) into the financial system;

b) **Layering:** The separation of the illicit proceeds/ benefits of unlawful activities from their source by creating layers of financial transactions designed to disguise the audit trail; and

c) **Integration:** Placement of laundered funds back into the economy so that they re-enter the financial system appearing to be legitimate business funds.

4.3. **The Money Laundering Offence**

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.

4.4. **Penalty for Money Laundering Offence**

The penalty for a money laundering offence is, upon conviction, imprisonment for a term not exceeding fifteen (15) years and 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 five (5) million ringgit, whichever is the higher.

[1] *Adapted from Guidelines on Prevention of Money Laundering, Countering Financing of Terrorism, Countering Proliferation Financing and Targeted Financial Sanctions for Reporting Institutions in the Capital Market issued by the Securities Commission Malaysia-13 June 2024*

5. GENERAL DESCRIPTION OF TERRORISM FINANCING[2]

5.1. Financing of terrorism generally refers to carrying out transactions involving funds or property, whether from a legitimate or illegitimate source, that may or may not be owned by terrorists, or those have been, or are intended to be used to assist the commission of terrorist acts, and/or the financing of terrorists and terrorist organisations.

5.2. Section 3(1) of the AMLATFA defines a "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.

The remainder of this page intentionally left blank.

[2] *Adapted from Guidelines on Prevention of Money Laundering, Countering Financing of Terrorism, Countering Proliferation Financing and Targeted Financial Sanctions for Reporting Institutions in the Capital Market issued by the Securities Commission Malaysia-13 June 2024*

6. GENERAL DESCRIPTION OF PROLIFERATION FINANCING[3]

6.1 In response to growing concerns over the proliferation of nuclear, biological and chemical weapons and their means of delivery which continue to pose a significant threat to international peace and security, the United Nations Security Council ("**UNSC**") has intensified efforts to strengthen its global sanctions regime in order to prevent, suppress and disrupt proliferation of weapons of mass destruction and its financing.

6.2 As is the case with other UNSC sanctions programmes, targeted financial sanctions on countries and specifically identified individuals and entities (i.e. designated persons) is the primary aspect of its overall sanctions regime to effectively disrupt financial flows across known proliferation networks.

6.3 Recommendation 7 of the Financial Action Task Force Standards requires countries to implement TFS-PF made under UNSCRs. Under this standard, countries are required to implement targeted financial sanctions without delay to comply with UNSCRs relating to the prevention, suppression and disruption of the proliferation of weapons of mass destruction and its financing.

6.4 Proliferation financing refers to the act of raising, moving, or making available funds, other assets or other economic resources, or financing, in whole or in part, to persons or entities for purposes of weapons of mass destruction proliferation, including the proliferation of their means of delivery or related materials (including both dual-use technologies and dual-use goods for non-legitimate purposes).

6.5 TFS-PF are applicable to persons designated by the UNSC or the relevant committees set up by the UNSC. Designation or listing criteria are:

a) Person engaging in or providing support for, including through illicit means, proliferation-sensitive activities and programmes;

b) Acting on behalf of or at the direction of designated person;

c) Owned or controlled by designated person; and

d) Person assisting designated person in evading sanctions, or violating UNSCR provisions.

[3] *Adapted from Guidelines on Prevention of Money Laundering, Countering Financing of Terrorism, Countering Proliferation Financing and Targeted Financial Sanctions for Reporting Institutions in the Capital Market issued by the Securities Commission Malaysia-13 June 2024*

7. POLICY STATEMENT

7.1. **SUNWAY strongly objects to all practices related to money laundering, including dealing in the proceeds of criminal activities, terrorism financing and proliferation financing.** 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 SUNWAY to determine the origin and destination of money or assets involved. Any suspected activities relating to money laundering or terrorism financing should be reported immediately to Bank Negara Malaysia and relevant authorities.

7.2. SUNWAY prohibits all involvement in money laundering activities, terrorism financing and proliferation financing either directly or indirectly. The activities may 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.

7.3. SUNWAY Business Units which fall under the definition of "Reporting Institutions" must ensure full compliance with the obligations stipulated under Part IV of the AMLATFA, which include the requirements to:

a) Implement AML/CFT/CPF risk management that commensurate with the level of money laundering, terrorism financing and proliferation financing risks;

b) Conduct customer due diligence;

c) Keep proper record on the customer and transactions;

d) Implement AML/CFT/CPF compliance programme;

e) Report suspicious transaction report (STR); and

f) Report cash threshold report (CTR) for cash transaction exceeding the amount specified, where applicable.

Detailed policies on AML/CFT/CPF for the Group's businesses in money services, leasing, money lending and factoring are maintained by Sunway Money Sdn Bhd, Sunway Leasing Sdn Bhd and Sunway Credit Sdn Bhd respectively.

8. RISK-BASED APPROACH APPLICATION

8.1 SUNWAY Business Units must take appropriate steps to identify, assess and understand its Money Laundering, Terrorism Financing and Proliferation Financing ("**ML/TF/PF**") risks, in relation to its customers, countries or geographical areas and products, services, transactions or delivery channels, and other relevant risk factors.

8.2 The risk assessment processes must incorporate the following:

a) Documenting the risk assessments and findings;

b) Considering all the relevant risk factors before determining the level of overall risk and the appropriate level and type of mitigation to be applied;

c) Keeping the reporting institution's risk assessment up-to-date, considering changes in surrounding circumstances affecting the reporting institution;

d) Having a scheduled periodic assessment or as and when specified by the SC; and

e) Having appropriate mechanisms to provide risk assessment information to the SC.

8.3 SUNWAY Business Units are required to–

a) have policies, procedures and controls, which are approved by the board of directors, to enable it to manage and mitigate effectively the ML/TF/PF risks that have been identified and assessed;

b) monitor the implementation of those policies, procedures and controls and to enhance them if necessary; and

c) take enhanced measures to manage and mitigate the risks where higher risks are identified

8.4 The risk control and mitigation measures implemented must commensurate with the risk profile of the particular customer or type of customer.

8.5 SUNWAY Business Units must implement and maintain appropriate policies and procedures to conduct risk profiling of its customer.

9. CUSTOMER DUE DILIGENCE

9.1. As a general principle, all SUNWAY Business Units are required to perform customer due diligence ("**CDD**") procedures when:

a) at the start of a new business relationship;

b) it has any suspicion of money laundering, terrorism financing or proliferation financing activities regardless of the amount transacted;

c) it has any doubt about the adequacy or authenticity of previously obtained information.

9.2. Each SUNWAY Business Unit management is responsible to implement the appropriate CDD procedures relevant to the nature of their business transactions. Business Unit management should adopt a risk-based approach when deciding on the degree of CDD to apply. Risks are assessed at the outset of a business relationship and updated regularly.

The CDD procedures should minimally include:-

a) identifying the customer (including foreign body corporate) and verifying 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) In the case of a customer who is a trust, to ensure that trustees or persons holding equivalent positions in similar legal arrangements disclose their status or function in the legal arrangement when establishing business relations.

e) understand and, where relevant, obtain information on the purpose of opening an account and the intended nature of the business relationship; and

f) maintain an updated and current database of designated persons and entities listed in global and local sanctions lists to enable it to detect suspected financing of terrorism and proliferators, including but not limited to:

(i) The UN Consolidated List.

(ii) Malaysia's Ministry of Home Affairs List (and equivalent lists specific to relevant jurisdictions).

(iii) Other applicable sanctions lists, such as:

- The Office of Foreign Assets Control (OFAC) List (United States).
- The European Union Sanctions List.
- The UK Sanctions List (administered by the Office of Financial Sanctions Implementation).
- Relevant regional or national sanctions lists in jurisdictions where the organisation operates.

g) 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 above.

9.3. If there is any name match, reasonable and appropriate measures must be taken to verify and confirm the identity of its customer. Upon such confirmation, the following steps must be taken immediately–

a) freeze without delay the customer's fund or block the transaction, if it is an existing customer;

b) reject the customer, if the transaction has not commenced;

c) lodge a Suspicious Transaction Reporting with the Financial Intelligence and Enforcement Department ("**FIED**"); and

d) notify the SC.

10. SUSPICIOUS TRANSACTION REPORTING

10.1. If any suspicious money laundering or financing of terrorism activities are detected or any attempted transaction fits the list of "Red Flags" as in the table below, these transactions must be reported to the AML/CFT/CPF Compliance Officer immediately – via an Internal Suspicion Report:

10.2. Examples of "Red Flags" – Possible Suspicious Transactions

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.

g) Multiple cash repayments that were structured below the reporting requirements to avoid detection.

10.3. Upon receiving the Internal Suspicion Report, the AML/CFT/CPF Compliance Officer shall evaluate the grounds for suspicion within 5 working days and if suspicion is confirmed, the officer shall submit a suspicious transaction report to the Financial Intelligence and Enforcement Department in Bank Negara Malaysia and notify the SC within the next working day through any of the following modes: -

No	Mode	To Whom
1	Mail	The physical forms should be placed in a sealed envelope and addressed to the following: The Director, Financial Intelligence and Enforcement Department (FIED) Bank Negara Malaysia Jalan Dato' Onn 50480 Kuala Lumpur (To be opened by addressee only)
2	Fax	+603-2693 3625

3	E-mail	str@bnm.gov.my
4	Others (where and if available)	FIED's Financial Intelligence System (FINS 2.0) (https://fins.bnm.gov.my)

Contact point	
Securities Commission Malaysia Executive Director Surveillance, Authorisation and Supervision Securities Commission Malaysia, 3 Persiaran Bukit Kiara, Bukit Kiara, 50490 Kuala Lumpur Tel: 03-6204 8000 Website: www.sc.com.my	***(For reporting of Target Financial Sanction in relation to Proliferation Financing)*** **Strategic Trade Controller** Strategic Trade Secretariat, Ministry of International Trade and Industry, Level 4, MITI Tower, No. 7, Jalan Sultan Haji Ahmad Shah, 50622 Kuala Lumpur Tel: 03-8000 8000 E-mail: admin.sts@miti.gov.my Website: http://www.miti.gov.my/index.php/pages/view/sta2010

11. TRAINING & COMMUNICATIONS

11.1. Further information on AML/CFT/CPF can be obtained from Bank Negara Malaysia's website at http://amlcft.bnm.gov.my/index.html.

11.2. In addition, SUNWAY Business Units which fall under the definition of reporting institutions are responsible to provide adequate training to its employees to ensure compliance to the requirements of the **AMLATFA** and **AML/CFT/CPF Guidelines**.

12. RECORDS KEEPING AND RETENTION OF RECORDS

12.1. SUNWAY Business Units must keep record of all transactions and ensure that 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 in whose name the account is opened or transaction is executed;

b) The identification of the beneficial owner or the person on whose behalf the account is opened or transaction is 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.

12.2. SUNWAY Business Units are 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.

13. RESPONSIBILITY FOR THE POLICY

13.1. This Policy is reviewed and approved by the Board of Directors and its Audit Committee and accountability and oversight for establishing this Policy has been delegated to the Audit Committee, which monitors the effectiveness of implementation of this Policy.

13.2. The Board of Directors set the tone at the top providing leadership and support for the Policy and take ultimate responsibility for proper supervision, reporting and compliance pursuant to AMLATFA and AML/CFT/CPF Guidelines.

13.3. The board shall ensure regular independent audit function to check on the compliance and effectiveness of the AML/CFT/CPF framework in relation to the AMLATFA and provisions of AML/CFT/CPF Guidelines. Any audit findings and any necessary corrective measures to be undertaken must be tabled to the board of directors.

13.4. The senior management are responsible for effective implementation of AML/CFT/CPF internal programmes, policies and procedures that can manage the ML/TF/PF risks identified.

13.5. Senior Management shall include, but not limited to the following roles and responsibilities:-

a) must be aware of and understand the ML/TF/PF risks associated with among others its business activities or strategies, delivery channels and geographical coverage of its business products and services offered and to be offered including new business activities or strategies, new products, new delivery channels and new geographical coverage;

b) is responsible for effective implementation of AML/CFT/CPF internal programmes, policies and procedures, communication and training activities in relation to the Policy to ensure that those reporting to them are made aware of, and understand, this Policy.

13.6. The AML/CFT/CPF Compliance Officer(s) must have necessary knowledge, expertise and the required authority to discharge his/her responsibilities effectively, including knowledge on the relevant laws and regulations and the latest AML/CFT/CPF developments.

13.7. SUNWAY Business Units are to nominate and appoint AML/CFT/CPF Compliance Officer who will be responsible for compliance of the AML/CFT/CPF internal programmes, policies and procedures.

14. EFFECTIVE / REVIEW DATE

14.1. The Policy is renamed and revised from Anti-Money Laundering ("AML") Policy to AML/CFT/CPF Policy and approved by the Board of Directors with effect from **26 November 2024.**

14.2. The Board will review this policy periodically or as changes arise to ensure that it remains relevant.

The remainder of this page intentionally left blank.