SUNWAY REIT MANAGEMENT SDN BHD
Registration No. 200801005046 (806330-X)
(Manager for Sunway Real Estate Investment Trust)

ANTI-MONEY LAUNDERING POLICY

Version 3.0 (29 June 2022)

COMMITTED TO SUSTAINABLE DEVELOPMENT GOALS

Approved by Board of Directors on 13 February 2020

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).

1.2. The purpose of this AML Policy is to provide guidance to all Sunway REIT Management Sdn Bhd's (Hereinafter referred to as "SUNREIT" or "The Company") Employees concerning how to strengthen anti-money laundering governance and it reiterates SUNREIT's commitment to full compliance to the AMLATFA. This Policy complements and should be read in conjunction with our Code of Conduct and Business Ethics (CCBE) and our Whistle-blower Policy, copies of which can be obtained from our website at www.sunwayreit.com.

2. SCOPE

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

2.2. This Policy applies to all business units or entities in SUNREIT 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 SUNREIT's businesses.

3. DEFINITIONS

AML/CFT	Anti-Money Laundering and Counter Financing of Terrorism
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.

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 funds.

4.3. **The Money Laundering Offence**

Pursuant to Section 4 of the AMLAFTA, 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 and Terrorism Financing For Capital Market Intermediaries issued by the Securities Commission Malaysia-7 Dec 2016

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 AMLA 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 and Terrorism Financing For Capital Market Intermediaries issued by the Securities Commission Malaysia-7 Dec 2016

6. POLICY STATEMENT

6.1. **SUNREIT strongly objects to all practices related to money laundering, including dealing in the proceeds of criminal activities and terrorism 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 SUNREIT 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.

6.2. SUNREIT prohibits all involvement in money laundering activities and terrorism 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.

6.3. SUNREIT business units which fall under the definition of “Reporting Institutions” have to ensure full compliance with the obligations stipulated under Part IV of the AMLAFTA, which include the requirements to:

a) Implement AML/CFT 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 AML/CFT compliance programme;

e) Report suspicious transaction report (STR); and

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

The remainder of this page intentionally left blank.

7. CUSTOMER DUE DILIGENCE

7.1. As a general principle, all SUNREIT 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 or terrorism financing activities regardless of the amount transacted;

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

7.2. Each SUNREIT 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 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 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.

The remainder of this page intentionally left blank.

8. SUSPICIOUS TRANSACTION REPORTING

8.1. 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 [Compliance Officer] immediately – via an Internal Suspicion Report:-

8.2. 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.

8.3. Upon receiving the Internal Suspicion Report, the [Compliance Officer] shall evaluate the grounds for suspicion and if suspicion is confirmed he or she shall submit a suspicious transaction report to the Financial Intelligence Unit in Bank Negara Malaysia on the next working day through any of the following modes:-

No	Mode	To Whom
1	Mail	The Director, Financial Intelligence Unit 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	Online	https://bnmapp.bnm.gov.my/fins2

9. TRAINING & COMMUNICATIONS

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

9.2. In addition, SUNREIT 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 AMLATFA.

10. RECORDS KEEPING AND RETENTION OF RECORDS

10.1. SUNREIT Business Units must 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 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; and

f) Any other information as required by the authorities.

10.2. SUNREIT 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.

The remainder of this page intentionally left blank.

11. RESPONSIBILITY FOR THE POLICY

11.1. This Policy is reviewed and approved by the Board of Directors and its Audit Committee and oversight of this Policy has been delegated to the Audit Committee, which monitors the effectiveness of and compliance with this Policy.

11.2. The Board of Directors and the Management team set the tone at the top providing leadership and support for the Policy and take responsibility for its effectiveness within their business units. Management is responsible for the implementation of the Policy and all communication and training activities in relation to the Policy to ensure that those reporting to them are made aware of, and understand, this Policy.

12. EFFECTIVE DATE

12.1. The Policy is approved by the Board of Directors and effective as of 13 February 2020

The remainder of this page intentionally left blank.