Paradigm REIT Management Sdn Bhd

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

Effective Date: 16 May 2025

TABLE OF CONTENTS

DEFINITION

AML/CFT/CPF	Anti-Money Laundering/ Countering Financing of Terrorism/Countering Financing Terrorism
AML Guidelines	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 Securities Commission
Beneficial Owner	Any natural person(s) who ultimately owns or controls the customer and/or the natural person(s) on whose behalf a transaction or activity is being conducted.
Board	Board of Directors of Paradigm REIT Management Sdn Bhd
BRSC	Board Risk and Sustainability Committee of Paradigm REIT Management Sdn Bhd
CEO	Chief Executive Officer
Customer	Customers encompass customers, hotel guests, and any stakeholders from whom payments are received.
Customer Due Diligence or CDD	Customer due diligence includes the identification and verification of the customer's and the other relevant parties' identity, the assessment of the purpose and intended nature of the business relationship, and the ongoing monitoring of the business relationship.
Deed	A deed of trust to be entered into between the Manager and the Trustee under which Paradigm REIT will be constituted
DIFA	Director of Investment, Finance and Accounts
Enhanced Due Diligence or EDD	Additional examination and cautionary measures aimed at identifying customers and confirming that their activities and funds are legitimate.
FIED	Financial Intelligence and Enforcement Department of Bank Negara Malaysia
HOFA	Head of Finance and Accounts
HOL	Head of Leasing
HOM	Head of Marketing
HOFM	Head of Facilities Management
HOCRS	Head of Compliance, Risk and Sustainability
Key Management	Consists of the CEO, DIFA, RD, HOFA, HOL, HOM, HOFM and HOCRS
Know-Your-Customer or KYC	The Know-Your-Customer process is intended to enable Paradigm REIT to form a reasonable belief that it knows the true identity of each customer and other relevant parties. This process is a component of the overall CDD procedures.
Manager	Paradigm REIT Management Sdn Bhd
ML	Money Laundering
MOHA List	Such orders as may be issued under sections 66B (UNSCR List) and 66C (Domestic List) of the AMLA by the Minister of Home Affairs (MOHA)

Person Acting on Behalf (or Person Purporting to Act on Behalf)	A person is acting on behalf of a customer when that person is operating or transacting on a business relationship, financial instrument, account or facility that is held by another party (i.e., the customer). This may include: a. A person with authority to sign, amend business relationship details, transfer funds and spend in the customer's name (e.g. a signatory or second cardholder on a spouse's account); b. A person granted authority because they are the legal or natural guardian of a minor or the holder of an operational power of attorney, or similar; c. An individual who is authorised to represent any legal entity appointed as a professional third party to act for the customer; d. A person who is authorised to use a password (or similar) to log in to an account or facility held by the customer (e.g. internet or mobile banking); e. An employee of the customer who undertakes daily duties for the customer; f. A third-party payer.
Paradigm REIT	A diversified REIT established in Malaysia and constituted by a deed of trust
PF	Proliferation financing
RD	Retail Director
Risk-Based Approach (RBA)	The approach whereby obliged entities identify, assess and understand the money laundering/ terrorism financing risks to which subjects of assessment are exposed and take AML/CFT/CPF mitigation measures that are proportionate to those risks.
SC	Securities Commission Malaysia
Service Provider(s)	External party(ies) with whom the Manager has, or plans to establish, some business relationship. This may include outsourcing providers, contractors, consultants, suppliers, vendors, advisors, agents, distributors and representatives.
Subject Properties	Collectively – Bukit Tinggi Shopping Centre, Paradigm Mall Petaling Jaya and Paradigm Mall Johor Bahru
Suspicious Activity	Unusual customer behavior or activity that raises a suspicion that it may be related to money laundering or financing of a terrorist activity: may also refer to a transaction that is inconsistent with a customer's known legitimate business, personal activities, or the normal level of activity for that kind of business or account
Suspicious Transaction Report or STR	A suspicious transaction/ activity, whether completed or attempted, is a transaction/ activity that raise the feeling or impression that something or someone could be related to a money laundering or terrorism financing offence. All suspicious relationships and transactions, including attempted transactions, should be reported to the local FIED, regardless of the amount of the single transaction

Transaction	A Transaction is any transmission or movement of funds regardless the connection with an ongoing relationship, as well as the designation of one or more beneficiaries specifically identified or unambiguously identifiable
UN Consolidated List	Various resolutions passed by the United Nations Security Council (UNSC) on counter terrorism measures, in particular, the UNSC Resolutions 1267 (1999), 1373 (2001), 1988 (2011), 1989 (2011), 2253 (2015) and other subsequent resolutions which require sanctions against individuals and entities associated to al-Qaida, Taliban, and the Islamic State in Iraq (Da'esh) organisations
UNSCR	United Nations Security Council Resolution

1. INTRODUCTION

This AML/CFT/CPF Policy ("Policy") sets out the framework by which the Manager manages its ML/TF/PF risks and establishes the AML/CFT/CPF minimum standards, in accordance with AML/CFT/CPF legal framework that requires the Manager to establish AML/CFT/CPF policies and procedures.

The roles and responsibilities section defines the tasks that the Board, the Key Management, the HOCRS and all employees of the Manager shall discharge within the AML/CFT/CPF control framework.

Money Laundering ("ML") 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.

Terrorism Financing ("TF") 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. can be defined as the provision or collection of funds (either legally or illegally) with the intention of being used to carry out acts of terrorism, including the financing of the proliferation of weapons of mass destruction.

Proliferation financing ("PF") 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).

2. OBJECTIVES

The Manager is fully committed to the highest standards of AML/CFT/CPF, including the prevention, suppression and disruption of proliferation of weapons of mass destruction and its financing to manage Paradigm REIT.

This Policy outlines the Manager's minimum AML/CFT/CPF standards for Paradigm REIT and seeks to:

a) Prevent Paradigm REIT from being used as a conduit for ML/TF/PF purposes, by establishing a robust framework, including the prevention from being misused for the financing of proliferation of weapons of mass destruction;

b) Protect the Manager, its Board and employees as well as Paradigm REIT against any corporate or personal liability arising under AML/CFT/CPF laws and regulations;

c) Protect the reputation and brand of Paradigm REIT by minimising ML/TF/PF risk.

3. SCOPE

This Policy applies to the Manager, as the holder of a licence under the Capital Markets and Services Act 2007 ("CMSA") carrying out the regulated activities of fund management, which falls under the definition of "Reporting Institutions" as described in the First Schedule of the Anti-Money Laundering, Anti-Terrorism Financing and Proceeds of Unlawful Activities Act 2001 ("AMLA"), as well as Property Managers appointed by the Manager to manage the properties of Paradigm REIT.

All Board members, employees and Service Providers acting on behalf of Paradigm REIT and the Manager are required to adhere to these standards to protect Paradigm REIT's reputation.

The requirements and the spirit of this policy shall always be met. There will be serious consequences for individuals / entities who attempt or actually breach the external and internal provisions related to AML/CFT/CPF depending on the severity of the breach, ranging from

consequence management actions (e.g., disciplinary letter, change of role) and withdrawal of variable compensation rights to termination of employment.

4. SCOPE OF APPLICATION

This Policy shall be read together with:

a) Sections 158(1) and 160A of the Securities Commission Malaysia Act 1993 ("SCMA");
b) Sections 66B, 66E and 83 of AMLA; and
c) SC AML Guidelines.

5. APPROVAL AND REVIEW

The Policy is approved by the Board, upon proposal by the HOCRS. It shall be promptly reviewed, and in any case once at least every three (3) years, or as and when there are developments in the regulation, legislation, market and/or best practices in relation AML/CFT/CPF activities.

The HOCRS is delegated by the Board to approve minor changes.

The HOCRS is responsible to provide guidance on common AML/CFT/CPF standards, support an effective implementation of this Policy and to keep the Board updated on the initiatives taken.

The minimum requirement for conducting periodic independent reviews of Paradigm REIT's AML/CFT/CPF program shall be ascertained and documented in the risk register (risk owner shall be the HOCRS) and the internal auditor shall assess its effectiveness and identify areas for improvement.

(The remaining section of the page has been intentionally left empty)

6. ROLES AND RESPONSIBILITIES

6.1. BOARD

The Board, in line with this Policy,

a) Maintains accountability over AML/CFT/CPF measures in place and approves the AML/CFT/CPF Policy;

b) Oversees the implementation of the Policy and respective regulations and the extent to which the AML/CFT/CPF risk to which Paradigm REIT and the Manager is exposed to;

c) Ensures that the roles and responsibilities to prevent the ML/TF/PF risks are clearly and appropriately allocated;

d) Establishes a compliance, risk and sustainability department and ensures that the department is independent and endowed with adequate quantitative and qualitative resources responsible for managing the ML/TF/PF risks faced by the Manager;

e) Verifies and ensures that the governance is effective over time with particular reference to internal control systems aimed at managing and controlling ML/TF/PF risks;

f) Ensures that adequate, complete and timely information flows are established between the compliance, risk and sustainability department and other relevant key functions;

g) Ensures that an effective independent audit function in assessing the adequacy of AML/CFT/CPF measures is in place;

h) Examines and approves AML/CFT reports and plans submitted by the HOCRS, and in particular the results of the AML/CFT risk assessments; and

i) Must keep itself updated with new or emerging trends of ML/TF/PF.

6.2. KEY MANAGEMENT

The Key Management shall:

a) Ensure that strategic decisions and the Policy adopted by the Board on ML/TF/PF risks are effectively implemented;

b) Formulate and implement internal procedures and controls aimed to identify and clarify the measures in place to mitigate the AML/CFT /CPF risks;

c) Be responsible for the adoption of all the necessary actions, in accordance with the recommendations and opinions of the HOCRS, to ensure that an effective internal control system for the mitigation of ML/TF/PF risks is maintained over time;

d) Ensure that adequate resources, including human capital, expertise, information technology and others are dedicated to managing the ML/TF/PF risks;

e) Ensure that all employees receive adequate information and training on the ML/TF/PF risks and factors;

f) Approve high-risk business relationships and transactions when necessary, in accordance with the Policy and the applicable laws and regulations.

6.3. HOCRS

The HOCRS must have the necessary qualification, knowledge, professional and personal skills to enable him/her to carry out the duties effectively.

The HOCRS shall evaluate and monitor the effectiveness of the AML/CFT/CPF work plan, which is prepared annually by the HOCRS and approved by the BRSC. The HOCRS shall perform at least the following activities with respect to the management and mitigation of AML/CFT/CPF risks and in accordance with the applicable laws and regulation:

a) Identify the AML/CFT/CPF applicable rules and evaluates their impact on the internal processes and procedures;

b) Monitor the implementation of appropriate AML/CFT/CPF policies and procedures including, but not limited to; CDD, reporting of suspicious transactions/activities, record keeping, and training programmes;

c) Cooperating with the Key Management in formulating the internal control framework and the procedures aimed at managing the ML/TF/PF risks;

d) Coordinate the AML /CFT /CPF risk assessment;

e) Provide the Board with periodic reporting on the level of ML/TF/PF risks and mitigation measures in place;

f) Submit to the Board, the AML/CFT/CPF annual report and an annual work plan;

g) Ensuring that the adoption of technology enabled tools (e.g., CDD, Suspicious Activities reporting, screening and record keeping tools) is adequate to mitigate the ML/TF/PF risks;

h) Perform testing controls, when necessary, in coordination with the internal auditors, in order to identify potential issues and critical areas;

i) Informs without delay any violation or any identified significant weakness;

j) Act as a central reference point for all AML/CFT/CPF matters, including reviewing regularly all internal reports on suspicious transactions or ad hoc reports made by employees; and lodging of STRs to the FIED;

k) Provide advice and assistance on ML/TF/PF risks;

l) Provide the Key Management with recommendations and opinions on all relevant remediation actions before they are submitted, if needed, to the Board;

m) Devise an adequate AML/CFT/CPF training plan for all employees;

n) Monitor and verify the implementation of formalised escalation processes for the assessment of high-risk business relationship and/or Transaction(s); and

o) Ensure that any STRs raised are appropriately evaluated before submission and that the channel of communication for reporting suspicious activities/transactions are secured and kept confidential for submission to FIED.

6.4. EMPLOYEES, PROPERTY MANAGER AND SERVICE PROVIDERS ACTING ON BEHALF OF PARADIGM REIT

It is the responsibility of all employees, the Property Manager and Service Providers acting on behalf of the Manager in the performance of their duties, to implement the necessary measures to prevent and mitigate the ML and TF risks and to exercise professional due diligence and good faith in the pursuit of the rigorous application of the Policy and of all relevant regulatory requirements.

It is particularly important that all employees make themselves aware of all restrictions applicable to their business and remain vigilant to the related risks applicable to their client relationships and Transactions and report any anomalous activity to the HOCRS. Any breach or attempt to circumvent or facilitate the violation of AML/CFT/CPF obligations should be reported by the employee to the HOCRS, in accordance with the relevant regulations.

7. AML/CFT RISK ASSESSMENT

The Manager shall undertake an AML/CFT/CPF risk assessment process which is appropriate with the nature, size and complexity of the business in order to identify, assess and understand its ML/TF/PF risks, taking into account relevant risk factors such as:

a) Customers/tenants/business partners of the Manager and the Subject Properties;

b) Geographic location of the Manager and the Subject Properties;

c) Transactions and distribution channels offered by the Manager and the Subject Properties;

d) Products and services of the Manager;

e) Structure of the Manager and the Subject Properties;

f) Findings of the National Risk Assessment (NRA) or any other risk assessment issued by relevant authorities; and

g) Other specific risk factors that the reporting institution may consider for the purpose of identifying its ML/TF/PF risks.

The outcome of the AML/CFT/CPF risk assessment process undertaken will determine the extent of ML/TF/PF risks that the Manager, the Property Manager and/or the Subject Properties are exposed to. This will then enable the Manager to formulate effective and appropriate risk mitigation measures which would commensurate with the ML/TF/PF risks that have been identified as well as the size, structure and complexity of the Manager's business.

The risk assessment process and findings shall be adequately documented and a periodic assessment of ML/TF/PF risks shall be conducted at least once every two (2) years, or at any time there are significant changes in the business or in the relevant regulatory framework.

8. CUSTOMER DUE DILIGENCE

Generally, CDD refers to measures undertaken to know your customer and to know whom you are dealing with and as a general rule, the Manager shall adopt CDD procedures:

a) Before accepting or establishing the relationship with a customer/tenant/business partner;

b) For as long as they remain a customer/tenant/business partner of the Manager or Paradigm REIT;

c) When there is reasonable suspicion of any ML/TF/PF activities and/or offences; and

d) When there is reasonable doubt about the veracity or adequacy of previously obtained customer/tenant/business partner identification data.

CDD includes:

a) obtaining satisfactory information to properly establish the identity and legal existence of each customer, the purpose and intended nature of the business relationship with the customer/tenant/business partner, and

b) ensuring that the information obtained and perceived ML/TF/PF risk profile are appropriate and updated throughout the business relationship.

For the purposes of conducting CDD, the Manager and Property Manager is required to:

a) identify and verify the customer/tenant/business partner's (including foreign body corporate) identity using reliable, independent source documents, data or information;

b) verify that any person purporting to act on behalf of the customer is authorised, by identifying and verifying the identity of that person;

c) identify the Beneficial Owner and take reasonable measures to verify the identity of the Beneficial Owner, using the relevant information or data obtained from a reliable source; and

d) understand, and where relevant, obtain information on the purpose and intended nature of the business relationship.

All frontline employees of the Manager and/or Property Manager are responsible for conducting CDD and therefore required to obtain the necessary documentation required to identify and verify the customer/tenant/business partner or the beneficial owner. Nonetheless, the Manager and/or Property Manager shall adopt a risk-based approach in determining the degree of CDD to apply, taking into account the customer/tenant/business partner's background and specific circumstances, among others.

In the event that the Manager is unable to verify the identity of the customer/tenant/business partner then the Manager shall not establish business relationships or permit any anonymous relationship (e.g. shell company) with the potential customer/tenant/business partner.

9. SANCTIONS SCREENING

The Manager shall maintain an updated and current database of names and particulars of designated persons in the UN Consolidated List and MOHA List (collectively referred to as "Sanctions List") to enable efficient detection of suspected TF activities and suspected proliferators.

The Manager shall also ensure that it takes appropriate steps and establishes procedures to screen its customers/tenants/business partners against the Sanctions List database as part of its CDD procedures, including performing appropriate background checks, where relevant; on the names of individuals or entities of customers/tenants to ensure that it has not entered into a business relationship or transaction with those listed on the sanctions list and in line with the requirements of Part VII and Part VIII of the AML Guidelines respectively.

The Manager will also ensure that it screens the entire customer/tenant/business partner database immediately when new names are listed in the UNSCR list.

In the event of a name match, the Manager shall take appropriate steps to verify and confirm the identity of the customer/tenant/business partner against the designated person in the UNSCR list. Upon such confirmation, the Manager shall immediately -

a) freeze without delay[1] the customer/tenant/business partner's fund or block the transaction, if it is an existing customer/tenant/business partner;

b) reject the customer/tenant/business partner, if the transaction has not commenced;

c) lodge a STR with the FIED; and

d) notify the SC.

[1] Reference made to Appendix D of SC AML Guidelines: According to the Financial Action Task Force, without delay is defined to be ideally within a matter of hours of designation by United Nations Security Council.

The Manager shall immediately report to the SC on any freezing, blocking and rejection actions undertaken towards the identified funds, properties or accounts; in accordance with Paragraph 18 of the AML Guidelines using the form prescribed under Appendix I of the AML Guidelines.

The Manager shall also observe the requirement to report periodically to the SC every six (6) months for both lists on frozen funds, properties or accounts of individuals/entities of its customers/tenants/business partners who are listed in the manner prescribed by Appendix J of the AML Guidelines and based on the intervals prescribed below:

List	UNSCR List	Domestic List
Reporting Intervals	Every 31 January and 31 July	Every 31 May and 30 November

10. DUE DILIGENCE ON THIRD PARTIES / SERVICE PROVIDERS

The Manager shall ensure there are adequate controls and due diligence performed on Service Providers, with whom it enters into business relationships with in order to mitigate the risk of entering into relationships / having transactions with individuals and/or entities which may be involved in ML/ TF/PF activities.

Prior to onboarding of these Service Providers, relevant Key Management shall be responsible to conduct due diligence with a specific focus on the country of residence, country of operation and the type of business conducted by the company.

11. INVESTIGATING AND REPORTING SUSPICIOUS TRANSACTION / ACTIVITY

The Manager shall be vigilant when performing CDD obligations and carry out sufficient monitoring activities of the Transactions and relationships to enable the detection of unusual or Suspicious Activities.

A Suspicious Transaction/Activity, whether completed or attempted, is a Transaction/Activity that raises the feeling or impression that something or someone could be related to a money laundering or terrorism financing offence.

The Manager shall develop scenarios or "red flags" as guidance in considering whether a transaction is suspicious, including but not limited to, the following:

a) The nature of, or unusual circumstances, surrounding the transaction;

b) The known business background of the person conducting the transaction;

c) The production of seemingly false identification in connection with any transaction, the use of aliases and a variety of similar but different addresses;

d) The behaviour of the person or persons conducting the transactions; and

e) The person or group of persons the Manager is dealing with.

After considering all relevant factors and there are reasonable grounds to suspect that the activity/transaction is suspicious, such transaction shall be reported immediately to the FIED through lodgement of STRs immediately. The HOCRS has the sole discretion and independence to report suspicious activity / transaction, therefore lodgement of STR shall be via the HOCRS using the prescribed STR form which can be downloaded from the Bank Negara Malaysia's website as outlined in **Appendix I**.

12. TRAINING

The Manager shall provide to its directors and employees (new and existing) periodic AML/CFT/CPF training which commensurate with their level of responsibilities, where applicable.

Employees and Service Providers acting on behalf of Paradigm REIT and the Manager shall be trained to be aware of potential scenarios by which Paradigm REIT and the Manager may be misused for ML/TF/PF activities and on how to proceed when they detect anomalous activities.

13. RECORD KEEPING

The Manager shall implement and maintain procedures that ensure the retention of records pertaining to the business relationship and/or Transactions including for the purpose of CDD, for at least seven (7) years from the termination of any business relationship and/or business transaction.

However, the Manager may retain a record beyond the retention period of seven (7) years if the record is in relation to:

a) a STR that has been lodged to FIED;

b) subject to an ongoing investigation by any law enforcement agency; or

c) subject to prosecution in court.

Data records and relevant documentation shall be stored in a format (preferably electronic) that ensures they are appropriately archived and easily retrievable, in a form that is admissible as evidence in court and are made available to the relevant law enforcement agencies and/or authorities in a timely manner.

The main custodian for KYC and CDD documents and records is the Retail Director.

14. CIRCULATION AND REVIEW

This Policy will be:

a) Circulated to all existing and new employees;

b) Updated as and when required and in any event at least once every three (3) years; and

c) Any revisions or amendments to this Policy will be submitted for approval by the Board and communicated to all employees. The revised Policy will supersede the previous version.

(end of Policy)

APPENDIX I – Submission of STR

1. A STR should be lodged with the FIED using the prescribed STR form which can be downloaded via the Bank Negara Malaysia's website.

2. The lodgement of the STR may be made by any of the following means:

   Mail:

   The physical forms should be placed in a sealed envelope and addressed to the following:

   Director
   Financial Intelligence and Enforcement Department
   Bank Negara Malaysia
   Jalan Dato' Onn
   50480 Kuala Lumpur

   Fax:
   03-2693 3625

   E-mail:
   str@bnm.gov.my