PAVILION

REAL ESTATE INVESTMENT TRUST

Managed by
Pavilion REIT Management Sdn Bhd

ANTI-MONEY LAUNDERING AND COUNTER FINANCING OF TERRORISM (AML/CFT) POLICY

Effective Date : 1 May 2022

Contents

1 Introduction

The Anti-Money Laundering Act 2001 ("**AMLA**") was gazetted on 5th July 2001 and came into force on 15th January 2002.

AMLA was renamed the Anti-Money Laundering and Anti-Terrorism Financing Act 2001("**AMLATFA**") with effect from 6th March 2007 (Gazette Order P.U. (B) 66/2007). In addition, the act was also amended to provide for the offence of money laundering, the measures to be taken for the prevention of money laundering and terrorism financing offences and to provide for the forfeiture of terrorist property and property involved in or derived from money laundering and terrorism financing offences.

AMLATFA was subsequently amended and renamed the Anti-Money Laundering, Anti-Terrorism Financing and Proceeds of Unlawful Activities Act 2001 ("**AMLATFPUAA 2001**") in August 2014 to include provisions relating to the use of the proceeds of crime.

Capital Markets Services License ("**CMSL**") holders carrying out activities of "fund management" are classified as one of the "*Reporting Institutions*" regulated by the Securities Commission ("**SC**") on AML/CFT compliance requirements[1].

Pavilion REIT Management Sdn Bhd ("**The Manager**") is a CMSL holder and manages Pavilion Real Estate Investment Trust ("**Pavilion REIT**"). The Manager is a "*Reporting Institution*" under AMLATFPUAA 2001 and the SC's AML Guidelines.

The core activity of Pavilion REIT is investment in income producing real estate assets used solely for retail purposes (including mixed-use developments with a retail component).

SC expects *Reporting Institutions* to implement controls to mitigate the risks of money laundering and terrorism financing ("**ML/TF**"). The internal controls encompass governance and oversight, effective internal control systems to assess and address ML/TF issues, regular independent audit function to assess the compliance programmes' effectiveness, and ongoing training.

[1] Section 3(1), First Schedule of the AMLATFPUAA 2001, read together with Paragraph 2.1 of the "*Securities Commission's Guidelines on Prevention of Money Laundering and Terrorism Financing for Reporting Institutions in the Capital Market*" ("SC's AML Guidelines").

This Policy is a benchmark to assess the robustness of the Manager's compliance programme against current and changing regulatory requirements and developments, most importantly, to be in sync with the fast-moving crime landscape.

2 Scope

This Policy for Anti-Money Laundering & Counter Financing of Terrorism ("**AML/CFT Policy**") aims to establish controls to manage and prevent the risks of Pavilion REIT being used as a conduit for money laundering and terrorism financing activities. It serves as a general guide to the Manager's employees to comply with the AMLATFPUAA 2001 and the SC's AML Guidelines.

3 Objectives

The objectives of this AML/CFT Policy are:

(a) To comply with the AMLATFPUAA 2001 and the SC's AML Guidelines;

(b) To interpret the AML/CFT requirements and how they may be implemented in practice;

(c) To create awareness and communicate this policy and AML/CFT requirements to all employees;

(d) To communicate the AML/CFT procedures and measures in terms of:

- Customer Acceptance Policy;
- Customer Due Diligence;
- Enhanced Due Diligence;
- Record-keeping;
- On-Going Monitoring;
- Recognition of Suspicious Transactions;
- Reporting of Suspicious Transactions; and

(e) To ensure efficient monitoring and management of any Suspicious Transactions.

4 Definition

In principle, Money Laundering generally involves the proceeds of unlawful activities related directly or indirectly to any serious offences that proceed through transactions, concealments, or other similar means. The main objective of Money Laundering is to legitimise funds obtained through illegal or criminal activities.

The Money Laundering process may be summarised in three stages, as follows:

(a) Placement

The physical disposal of benefits of unlawful activities by introducing illegal funds (generally in the form of cash) into the financial system.

(b) Layering

In this phase, criminal engages a series of conversions or movements of the funds to distance them from their source. The illicit proceeds are separated from their source by creating complex layers of financial transactions to disguise the audit trail and provide an appearance of legitimacy as well as anonymity.

(c) Integration

When layering succeeds, the criminal proceeds have been successfully laundered, i.e. cleaned and regarded as legitimate funds for all intent and purposes. Criminals will place the laundered funds back into the economy to re-enter the financial system appearing to be legitimate business funds.

Examples would include funds reinvested into assets, real estate, stocks, business ventures etc.

5 Obligations of the Board of Directors, Senior Management and Compliance Officer

The Board of Directors has the roles and responsibilities of maintaining accountability and oversight for establishing AML/CFT policies and procedures.

The Senior Management is responsible for effective implementation of AML/CFT internal programmes, policies and procedures to manage the ML/TF risks identified.

Compliance Officer must have the necessary knowledge, expertise, and the required authority to discharge their responsibilities effectively, which includes knowledge of the relevant laws and regulations and the latest AML/CFT developments.

6 Customer Due Diligence ("CDD")

Generally, Customer Due Diligence refers to measures undertaken to know your Tenant and to know whom you are dealing with:

(a) before accepting or establishing the relationship with a Tenant;
(b) for as long as they remain a Tenant of the Manager or Pavilion REIT;
(c) when there is reasonable suspicion of the commission of any ML/TF offences; and
(d) when there is reasonable doubt about the veracity or adequacy of previously obtained Tenant identification data.

Customer Due Diligence includes:

(a) obtaining satisfactory information to properly establish the identity and legal existence of each Tenant, the purpose and intended nature of the business relationship with the Tenant, and
(b) ensuring that the information and perceived ML/TF risk profile are appropriate and updated throughout the relationship.

For the purpose of conducting CDD, employee is required to: -

(a) identify and verify the Tenant's identity using reliable, independent source documents, data or information;
(b) verify that any person purporting to act on behalf of the Tenant 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;
(d) understand, and where relevant, obtain information on the purpose and intended nature of the business relationship.

7 Suspicious Transaction Reporting

The Manager will promptly submit a Suspicious Transaction Report ("**STR**") to the FIED, BNM when any of the employees have reasonable grounds to suspect that the transaction involve proceeds an unlawful activity (including attempted or proposed), regardless of the amount.

All suspicious transaction reports would be channeled directly to the Compliance Officer to establish whether the transaction is indeed suspicious and require onward submission to FIED. The Compliance Officer will ensure that the suspicious transaction reporting mechanism is operated in a secured environment to maintain confidentiality and preserve secrecy.

The Compliance Officer will ensure that the STR is submitted to FIED in BNM within the next working day after having established that the transaction is suspicious. In the course of submitting the STR, utmost care will be taken to ensure that such reports are treated with the highest level of confidentiality. The Compliance Officer has the sole discretion and independence to report suspicious transactions.

The Compliance Officer shall submit to the FIED in BNM through *any of the following modes*:

i. Mail : Director
Financial Intelligence and Enforcement Department
Bank Negara Malaysia
Jalan Dato' Onn
50480 Kuala Lumpur
(To be opened by addressee only)

ii. Fax : +03-2693 3625

iii. E-mail : : str@bnm.gov.my

8 Training

The Manager will identify courses relevant to the training and create awareness on AML/CFT activities for their employees, both existing and new.

Employees in the category of messenger, driver, and receptionist are not required to undergo training on AML/CFT. Employees who are hired on a contract or temporary basis for less than 3 consecutive months and interns are also exempted from AML/CFT training.

Training will be conducted at least once every 2 years. Training programmes will include the latest AML/CFT developments such as industry or transactions that are susceptible to the risk of money laundering and remind employees of their responsibilities under the AML/CFT programmes.

The Manager shall ensure that employees receive comprehensive training in:

i. the relevant laws.
ii. the Manager's AML policy and procedures.
iii. the obligation to monitor and report suspicious transactions.
iv. the personal obligation as an employee under the relevant laws.

9 Record-Keeping

The Manager shall maintain all records and documents of transactions, in particular, those obtained during customer due diligence procedures, for at least seven (7) years after the transaction has been completed or after the business relations with Tenants have ended. This is to enable it to comply swiftly with information requests from the SC and Financial Intelligence and Enforcement Department ("**FIED**") of BNM or any law enforcement authorities for investigative purposes and to create an audit trail on transactions that are traceable by SC and BNM, the relevant supervisory and/or law enforcement agencies.

The record-keeping (in either hard and/or soft copy) should be easily accessible and readily available and enable the Manager to establish the history, circumstances and reconstruction of each transaction. The records shall, where relevant, include the following:

i. Memorandum & Articles of Association/Constitution
ii. Company Search
iii. Notice of Registration under Section 15 of the Companies Act 2016 ("CA 2016") (known as Form 24 under CA 1965)
iv. Return for allotment of shares under Section 78 of CA 2016 (known as Form 24 under CA 1965)
v. Form 44 or Notification for change in the registered address under Section 26 of the CA 2016 (if applicable);

vi. Form 49 or Notification of change in the register of directors, managers, and secretaries under Section 58 of the CA 2016 (if applicable)
vii. Annual Return of a company having a share capital under Section 68 of the CA 2016 (if applicable);
viii. Board of Directors' Resolution;
ix. Application for Recommendation;
x. Letter of Offer;
xi. Tenancy Agreement;
xii. Letter of Guarantee (if applicable);
xiii. Payment records on the duration of the Tenant; and
xiv. Correspondence(s) between the Manager's respective malls' personnel and the Tenant

In situations where the records are subject to on-going investigations, prosecution in court or Suspicious Transaction Report has been lodged, they shall be retained beyond the stipulated retention period until it is confirmed by the FIED, SC or any law enforcement authorities that such records are no longer needed.

The Compliance Officer shall maintain a register of all enquiries made by the law enforcement authority. The register shall be kept separate from other records and contain the following details: -

- the date and nature of the enquiry.
- the name and agency of the enquiring office.
- the powers being exercised.
- the identity(ies) of the person(s) being investigated.

10 Effective Date / Next Review Date

Effective Date of Revised AML/CFT Policy

This Policy shall take effect upon approval by the Board of Directors.

Next Review Date

The Compliance Officer is responsible for reviewing this Policy as and when required and in any event not later than 24 months from the last review date.