AMLCFT STATEMENT

1. INTRODUCTION

1.1 It is the general policy of GEM Asset Management Pte. Ltd. ("**GEMAM**") to fully comply with anti-money laundering ("**AML**") and counter-financing of terrorism ("**CFT**") laws and regulations (together, the "**AML/CFT Laws**"). This policy ("**Policy**") sets out the guidelines and requirements of GEMAM relating to compliance with AML/CFT Laws.

1.2 Singapore is a member of the Financial Action Task Force ("**FATF**") and is obligated to implement FATF's recommendations regarding measures to combat money laundering, terrorist financing and other related threats to the integrity and security of the international financial systems ("**FATF Recommendations**"). To the extent applicable to GEMAM, this Policy takes into account the FATF Recommendations relating to the financial sector and designated non-financial businesses and professions.

1.3 GEMAM depends upon the conduct and diligence of its directors, officers and employees to ensure full compliance with this Policy. All directors, officers and employees are therefore required to act in a manner consistent with this Policy.

2. DEFINITION

Money Laundering

2.1 Money laundering is the process by which the illegal origin of wealth is disguised to avoid suspicion of law enforcement authorities and to wipe the trail of incriminating evidence. Criminals are interested in concealing the destination and the purpose for which the money is collected. It is an offence to use funds (even for otherwise legitimate purposes) which are derived from criminal or illegitimate means.

2.2 The objective of AML laws is traditionally to eliminate the movement of illegally obtained funds.

Terrorism Financing

2.3 Acts of terrorism seek to coerce governments into a particular course of action and/or to intimidate the public. Terrorists require funds to carry out acts of terrorism and terrorism financing is the provision of such funds. These funds may be derived from criminal activities such as robbery, drug-trafficking, kidnapping, extortion, fraud or hacking of online accounts. In such cases, there may be an element of money laundering to disguise the source of funds.

2.4 Terrorist acts and organisations may also be financed from legitimate sources such as donations from charities, legitimate business operations, individual self-funding. In these cases, which often does not require the involvement of large sums of money, terrorism financing can be hard to detect.

3. Laws and Regulations

CDSA and TSOFA

3.1 Singapore has put in place strong laws and regulations to punish crimes and protect its financial system. Generally, the laws are focused on detection, prevention and reporting of suspicious transactions to deter money laundering.

3.2 Singapore's primary legislation to combat money laundering is the Corruption, Drug Trafficking and Other Serious Crimes (Confiscation of Benefits) Act 1992 ("**CDSA**"). The primary Singapore legislation to combat terrorism financing is Terrorism (Suppression of Financing) Act 2002 ("**TSOFA**"). In addition, there are regulations that are relevant to the conduct of GEMAM.

4. APPROACH

4.1 Aligning with the FATF recommendations, GEMAM adopts a risk-based approach in complying with AML/CFT Laws and determines the appropriate type and extent of mitigation to be applied after considering relevant risk factors, such as the following:

a) nature of business or operations conducted by GEAMAM (the "**Business**"), including products, services, transactions and delivery channels;
b) country or jurisdiction where the Business is conducted; and
c) country or jurisdiction of the Counterparty with which the Business is conducted.

4.2 GEMAM screens customers and associated parties against lists issued by MAS and international bodies [i.e., U.S. Department of Treasury Office of Foreign Asset Control ("**OFAC**"), EU Sanction, UN Sanction, and UK Asset Freezing Unit of the Treasury]. Therefore, GEAMAM ensures that customer profiles are monitored regularly.

5. OBLIGATIONS

5.1 The main obligations under this Policy are:
a) Counterparty Due Diligence;
b) Suspicious Transaction Reporting;
c) Record Keeping; and
d) Training

5.2 Apart from the above main obligations, an entity within GEMAM that has obtained a Capital Markets Services Licence to conduct a regulated activity has additional obligations under notices and guidelines issued by the MAS or equivalent regulatory requirements in the relevant local jurisdiction(s), as the case may be.

Counterparty Due Diligence ("**CDD**")

5.3 The term "Counterparty" refers to any counterparty with which GEMAM comes into contact within the course of its Business, including the following:
a) a "Customer" of GEMAM, which holds a Capital Markets Services Licence;
b) providers of services or goods to GEMAM (on a risk-proportional basis); and

c) counterparties to transactions with GEMAM that involve the payment or receipt of substantial sums of money, such as the entry into a joint venture for the acquisition or development of a project.

5.4 Prior to establishing a business relationship or entering a transaction with a Counterparty, CDD measures must be undertaken to obtain knowledge regarding the Counterparty to guard against establishing any business relationship or entering any transaction which is or may relate to or may facilitate money laundering or terrorism financing.

5.5 Employees undertaking the CDD measures must be vigilant to any suspicious circumstances in the proposed transaction with a Counterparty ("**Red Flag**").

5.6 If there is any Red Flag, the relevant Head of Department or his or her authorised delegate or representative (collectively, "**HOD**") shall adopt a risk-based approach in determining whether to undertake enhanced due diligence measures ("**Enhanced CDD**") and/or the extent of Enhanced CDD to be undertaken. Where Enhanced CDD is assessed to be required, screening of the Counterparty shall be undertaken.

5.7 Following the completion of Enhanced CDD, the relevant HOD shall assess if there are further or other Red Flags and determine whether to proceed with the transaction with the Counterparty.

5.8 Ongoing monitoring. On an ongoing basis, employees must be alert to changes in a Counterparty's circumstances that may require updates to or review of CDD conducted prior to the commencement of the business relationship with or prior to the transaction with the Counterparty. When there is a change of circumstances, the relevant HOD shall perform a targeted review of the relationship and manage the future relationship with the Counterparty.

Suspicious Transaction Reporting

5.9 Under the CDSA, there is an obligation to report any knowledge or suspicion of Relevant Circumstances (as defined below) to the Singapore Police Force Commercial Affairs Department ("**CAD**"). A report to the CAD is made by filing a "Suspicious Transaction Report" (or "**STR**") to the Suspicious Transactions Reporting Office ("**STRO**") via the STRO Online Notices & Reporting ("**SONAR**") platform.

5.10 If, as a result of the CDD measures undertaken on a Counterparty for a business transaction to be entered into in Singapore or other business activity in Singapore, any employee:

(a) becomes aware that; or

(b) has reasonable grounds to believe that,

a property[1] represents the proceeds of or was used or is intended to be used in connection with criminal conduct or is terrorist property or is to be used for terrorist purposes ("**Relevant Circumstances**"), the requisite work shall be carried out to determine whether there is actual knowledge of or there are reasonable grounds to believe that there are Relevant Circumstances to be reported as a suspicious transaction ("**Suspicious Transaction**") by filing a STR to the STRO.

[1] means money and all other property, movable or immovable, including things in action and other intangible or incorporeal property.

5.11 During this period of time, the employee should not abruptly cease all communications with the Counterparty so as not to run the risk of tipping off the Counterparty. The employee should continue communications as usual. However, the employee should not complete the transaction with the Counterparty.

5.12 If and after filing a STR, GEMAM will comply with any instructions from CAD about how to proceed with the transaction with the Counterparty. In proceeding with the transaction, the relevant employee shall act according to the instructions of his or her HOD.

5.13 Ongoing monitoring. On an ongoing basis, employees must be alert to changes in a Counterparty's business activity that may give rise to Relevant Circumstances.

Record Keeping

5.14 Employees conducting CDD shall prepare, maintain and retain records of any data, documents and information obtained (including any analysis performed) to comply with this Policy. Such records may be retained as originals or copies, in paper or electronic form, and shall be retained for a period of at least **five (5)** years after entry into the business relationship with the Counterparty or the completion of the transaction with the Counterparty, or any longer period required under the AML/CFT Laws, or any other applicable local laws, as the case may be.

5.15 The CDD documents and records shall be maintained in a manner that would facilitate the timely retrieval of and access to such documents and records in response to requests by government authorities or otherwise.

5.16 Records of data, documents and information pertaining to a transaction or matter which is under investigation or which has been the subject of an STR shall be retained for as long as requested or ordered by CAD or other relevant authorities.

6. REPORTING

6.1 Any person may report any instance of non-compliance with this Policy to the Compliance department.

6.2 Any non-compliance with this Policy may potentially result in criminal and civil liabilities on the part of the relevant employees under applicable laws and may additionally expose the GEMAM to the same. If GEMAM finds that its employee has not complied with this Policy may institute disciplinary action and have a reasonable basis to terminate his or her employment. The employer is not obligated to wait for the outcome of any civil or criminal action against the employee before taking any disciplinary action or terminating his or her employment.

Approved and adopted by:
GEM Asset Management Pte. Ltd. on **20 May 2026**.