IOIPG Malaysia REIT
Management

IOIPG REIT MANAGEMENT SDN BHD
Company Registration No. 202501026083 (1627496-A)
(Incorporated in Malaysia)

ANTI-MONEY LAUNDERING, COUNTER-TERRORISM FINANCING AND COUNTER-PROLIFERATION FINANCING POLICY

CONTENTS

1. INTRODUCTION 3
2. KEY PRINCIPLES 3
3. ROLES AND RESPONSIBILITIES 4
4. KEY COMPONENTS OF THE AML/CTF/CPF FRAMEWORK 4
5. ESCALATION AND REPORTING 6
6. INDEPENDENT REVIEW 6
7. POLICY MAINTENANCE 6

1. INTRODUCTION

IOIPG REIT Management Sdn Bhd ("Manager"), in its capacity as the Manager of IOIPG Malaysia Real Estate Investment Trust ("IOIPG REIT"), is the responsible entity of IOIPG REIT.

The purpose of this Anti-Money Laundering, Counter-Terrorism Financing and Counter-Proliferation Financing Policy ("Policy") is to establish a clear framework for preventing, detecting, and responding to money laundering ("ML"), terrorism financing ("TF"), and proliferation financing ("PF") risks to which the Manager and IOIPG REIT is exposed.

This Policy forms the foundation of the Manager's Anti-Money Laundering, Counter-Terrorism Financing and Counter-Proliferation Financing ("AML/CTF/CPF") framework, setting out the minimum principles, standards, and responsibilities that guide the Manager's approach to safeguarding IOIPG REIT and the Manager against ML/TF/PF activities.

In applying this Policy, the Manager adopts a risk-based and proportionate approach, recognising that the ML/TF/PF risks associated with the activities of the Manager and IOIPG REIT are primarily linked to tenant, operator, vendor and service provider relationships rather than high-volume financial transactions.

Accordingly, the nature and intensity of AML/CTF/CPF measures implemented under this Policy shall be calibrated to the Manager's business model, relevant asset classes, and assessed risk exposure, while ensuring full compliance with applicable legal and regulatory requirements.

This Policy is to facilitate compliance with the provisions of the Anti-Money Laundering, Anti-Terrorism Financing and Proceeds of Unlawful Activities Act 2001 ("AMLA"), 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"), and the relevant AML/CTF/CPF policy documents issued by Bank Negara Malaysia ("BNM") from time to time.

This Policy applies to the Board of Directors ("Board"), all employees of the Manager and any parties acting for or on behalf of the Manager or IOIPG REIT.

The Manager shall ensure all service providers comply with this Policy, by incorporating appropriate contractual obligations and implementing ongoing compliance monitoring to mitigate risks arising from outsourcing arrangements.

2. KEY PRINCIPLES

The AML/CTF/CPF framework is guided by the following principles:

- Zero Tolerance – IOIPG REIT and the Manager do not tolerate any ML/TF/PF activities.
- Know Your Customer ("KYC") – Robust customer due diligence shall be performed before onboarding or establishing a business relationship.
- Risk-Based Approach ("RBA") – The extent, depth and frequency of due diligence and monitoring shall be proportionate to the ML/TF/PF risk level.
- Transparency and Traceability – All transactions must be transparent, properly documented, and capable of independent verification and audit.
- Accountability – Roles and responsibilities shall be clearly defined across the Board, the Risk and Sustainability Committee ("RSC"), the Audit Committee ("AC"), Key Management Personnel, the Head of Legal and Compliance and employees.

- Continuous Monitoring and Escalation – Ongoing monitoring and escalation mechanisms shall be in place to detect, investigate, and report suspicious transactions or activities.
- Audits and Independent Review - Independent testing of the AML/CTF/CPF framework shall be performed periodically by Internal Audit or an external party. The results and findings, including matters relating to the adequacy and effectiveness of internal control systems, shall be reported to the AC.

3. ROLES AND RESPONSIBILITIES

The effective implementation of this Policy depends on the active participation, collaboration and accountability of the Board, the RSC, the AC, Key Management Personnel, Head of Legal and Compliance, and employees. Each plays a distinct yet complementary role in safeguarding IOIPG REIT and the Manager from ML, TF and PF risks.

Clear allocation of responsibilities ensures that AML/CTF/CPF measures are applied consistently, that risks are identified and mitigated in a timely manner, and that reporting obligations to regulators are fulfilled transparently. The following outlines the key responsibilities of the respective roles within the Manager's AML/CTF/CPF framework.

Role	Responsibilities
Board	• Approves the Policy and holds ultimate responsibility and accountability for AMLA compliance. • Provides guidance and direction on high-risk AML/CTF/CPF matters, where necessary.
AC	• Oversees the adequacy of internal controls and governance arrangements.
RSC	• Provides oversight of AML/CTF/CPF compliance and monitors the Manager's and IOIPG REIT's ML/TF/PF risk exposure. • Reviews compliance reports, including findings, risk assessments, and trends in suspicious transactions. • Monitors the remediation progress of identified deficiencies or control gaps.
Key Management Personnel/ Heads of Department	• Implements AML/CTF/CPF controls and procedures across the operations of IOIPG REIT and the Manager. • Ensures adequate resources, staffing, training, and systems are in place. • Approves high-risk business relationships or transactions. • Embeds AML/CTF/CPF obligations into operational processes.
Head of Legal and Compliance	• Acts as the designated focal point for AML/CTF/CPF compliance. • Monitors regulatory updates and integrates them into procedures. • Reviews and escalates suspicious transaction reports ("STRs"). • Coordinates training, awareness, and regulatory engagement.
Employees	• Perform KYC and Customer Due Diligence ("CDD") diligently. • Report suspicious transactions or activities to their immediate supervisor or reporting manager and, where appropriate, to the Head of Legal and Compliance. • Adhere strictly to AML/CTF/CPF procedures. • Maintain vigilance in their roles and escalate anomalies promptly.

4. KEY COMPONENTS OF THE AML/CTF/CPF FRAMEWORK

4.1 Risk Assessment

a) Periodic ML/TF/PF risk assessments shall be conducted, taking into account customer, tenant, operator, vendor and service provider profiles, geographic exposure, distribution channels, products/services, and transaction characteristics.

b) The outcomes of the ML/TF/PF risk assessment shall inform the level of customer due diligence, enhanced due diligence ("EDD"), sanctions screening, transaction monitoring, and review frequency applied under this Policy.
c) The risk assessment shall be documented and reviewed periodically, or earlier where necessary, if there are material regulatory developments, significant changes in the asset portfolio, or operational changes that may impact the Manager's RBA.

4.2 CDD

a) CDD must be performed before onboarding or entering into a contractual relationship with any customer, tenant, business partner or external party, and maintained on an ongoing basis throughout the duration of the relationship.
b) CDD measures shall include identification and verification of legal identity, determination of beneficial ownership, confirmation of authorised representatives, and assessment of the purpose/nature of the business relationship.
c) EDD shall apply to high-risk customers, including politically exposed persons ("PEPs"), or customers from high-risk jurisdictions.
d) CDD measures shall be applied on a risk-based and proportionate basis. Simplified due diligence may be applied to demonstrably low-risk counterparties (e.g. regulated entities, entities within IOI Properties Group Berhad, or established corporate tenants), while EDD shall be applied where higher ML/TF/PF risks are identified.

The Manager may deploy technology-enabled systems to support customer due diligence, sanctions screening, record traceability, and ongoing transaction monitoring. These systems shall be calibrated to the Manager's business model, customer profile, and ML/TF/PF risk exposure.

Where the Manager relies on a third party to perform any CDD or other AML/CTF/CPF measures, such reliance shall be risk-based and documented. The Manager remains ultimately accountable for AMLA compliance and shall maintain unrestricted access to relevant information, and the right to conduct appropriate review and audit, to ensure compliance.

4.3 Sanctions Screening

a) Where required based on the assessed ML/TF/PF and sanctions risk, sanctions screening shall be performed as part of CDD on the names of customers, tenants, vendors or suppliers, to ensure that transactions or dealings are not made with persons or entities on applicable sanctions lists (e.g. United Nations sanctions, Ministry of Home Affairs (MOHA) lists, or other applicable regulatory lists).
b) Immediate freezing, rejection, and termination of contractual relationships apply where a match is confirmed.

4.4 Suspicious Transaction/Activity Reporting

a) Employees must promptly report red flags to their respective immediate supervisors or reporting managers and, where appropriate, to the Head of Legal and Compliance.
b) The Head of Legal and Compliance shall assess, document, and lodge STRs with the Financial Intelligence and Enforcement Department (FIED), BNM, if required.
c) STRs and related information must be kept strictly confidential, with secure escalation protocols.

4.5 Training and Awareness

a) AML/CTF/CPF training shall be mandatory for all Directors and employees at a frequency and depth commensurate with their roles and exposure to ML/TF/PF risks, and at least annually for staff in higher-risk or frontline functions.

b) Training shall include identification of ML/TF/PF typologies, red flags, sanctions compliance, and reporting procedures.

4.6 Record Keeping

a) Records of CDD, transactions, and STRs shall be maintained for at least seven (7) years after termination of a business relationship or transaction.
b) Records must be in an accessible format suitable for regulatory review and admissible as evidence in legal proceedings.

5. ESCALATION AND REPORTING

Material breaches, suspicious activities, or regulatory concerns shall be escalated to the Key Management Personnel, particularly the Head of Legal and Compliance. The Head of Legal and Compliance shall further escalate to the RSC and the Board and, where required under applicable laws and regulations, to the SC or BNM. All reports to regulators, including matters such as freezing actions or sanctions reporting, shall be submitted in accordance with prescribed timelines and formats.

6. INDEPENDENT REVIEW

a) The AML/CTF/CPF framework shall be subject to periodic independent review, either by the internal auditor or external qualified parties, to assess its adequacy, effectiveness and alignment with regulatory requirements.

b) Independent review shall evaluate:

- The adequacy of risk assessments, CDD/EDD processes, and sanctions screening;
- The timeliness and quality of STRs;
- The adequacy of record-keeping, training, and governance arrangements; and
- The effectiveness of technology-enabled systems for screening, monitoring, and reporting.

Findings from independent reviews shall be documented and reported to the RSC and the Board.

c) Independent review shall be conducted at least once every three (3) years, or more frequently if required by regulatory developments, material incidents, elevated AML/CTF/CPF risk assessments, or a directive from the RSC.

d) Audit or review results and remedial actions shall also be made available to the SC or BNM upon request.

7. POLICY MAINTENANCE

This Policy, together with all supplementary policies and procedures, shall be treated as a living document and will be reviewed at least annually, or earlier where necessary, to ensure that it continues to reflect evolving business needs, regulatory requirements, industry best practices, and any material changes in applicable laws, regulations, or the Manager's business operations.