



ORKIM SDN BHD

**ANTI MONEY LAUNDERING, COUNTER FINANCING OF
TERRORISM AND COUNTERING PROLIFERATION POLICY
AND PROCEDURES**



DOCUMENT TITLE	ANTI MONEY LAUNDERING, COUNTER FINANCING OF TERRORISM AND COUNTERING PROLIFERATION POLICY AND PROCEDURES		
DOCUMENT REF	ORKIM/AML/P&P/01/00/25		
OWNER	RISK, AUDIT AND COMPLIANCE DEPARTMENT		
ISSUE	1	ISSUE DATE	15 MAY 2025
REVISION	0	REVISION DATE	NIL
PREPARED BY	SYED EFFIZAN (HEAD OF RISK, AUDIT AND COMPLIANCE)	SIGNATURE	
		DATE	
REVIEWED BY	TAHIRAH MOHD NOR (CHIEF FINANCIAL OFFICER)	SIGNATURE	
		DATE	
APPROVED BY	CAPT CHEAH SIN BI (CHIEF EXECUTIVE OFFICER)	SIGNATURE	
		DATE	
FINAL APPROVED BY	(NAME) (CHAIRMAN, BOARD RISK AND AUDIT COMMITTEE)	SIGNATURE	
		DATE	



TABLE OF CONTENTS

POLICY

POLICY STATEMENT AND OBJECTIVES	1
CIRCULATION AND REVIEW	1
APPLICATION.....	1
DEFINITIONS.....	2
MONEY LAUNDERING	2
TERRORISM FINANCING	3
PROLIFERATION FINANCING.....	3
ROLES AND RESPONSIBILITIES.....	4

STANDARD OPERATING PROCEDURES

RISK ASSESSMENT PROCESS IN CLIENT/CUSTOMER PROFILING	6
CUSTOMER DUE DILIGENCE PROCESS	6
SUSPICIOUS TRANSACTION REPORTING	7
RECORD KEEPING AND RETENTION	8
COMMUNICATION AND TRAINING	8
REPORTING POLICY VIOLATIONS.....	8

ORKIM SDN BHD ANTI MONEY LAUNDERING, COUNTER FINANCING OF TERRORISM AND COUNTERING PROLIFERATION POLICY AND PROCEDURES	ISSUE	REVISION	PAGE
	01	00	Page 1 of 8
	DATE: 15 MAY 2025		

SECTION 1 – POLICY STATEMENT AND OBJECTIVE

1. The purpose of the Anti-Money Laundering, Counter Financing of Terrorism and Counter Proliferation Financing ("AML/ CFT/ CPF") Policy and Procedures is to provide consistent guidance to Orkim Sdn Bhd and its Group of Companies (hereinafter referred to as "Orkim" or "the Group" or "Orkim Group") on matters concerning anti-money laundering governance. This Policy and Procedures addresses the risk management and the prevention of the Group's businesses from being used as a conduit for money laundering, terrorism financing or proliferation financing activities.
2. The Group strongly objects to all practices related to money laundering, including dealing in the proceeds of criminal activities, terrorism financing and proliferation financing. Reasonable degree of due diligence must be performed to understand the business and background of any prospective clients or customers that intend to do business with the Group. The Group is committed to:
 - a) Adopt a zero tolerance on money laundering, financing of terrorism and proliferation financing.
 - b) Comply with the requirements of this Policy and Procedures and all other internal policies of the Group.
 - c) Comply with the requirements of all applicable laws and practice guidance, failure which, will constitute an offence, in accordance with the:
 - Anti-Money Laundering and Anti-Terrorism Financing Act 2001 ("AMLATFA")
 - 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") ("AML/CFT/CPF Guidelines").

SECTION 2 - CIRCULATION AND REVIEW

This Policy and Procedures shall be reviewed by the Risk, Audit and Compliance ("RAC") Department annually, or as and when required with the requirements of all applicable and evolving laws. RAC Department shall be responsible for the administration, interpretation and application of this Policy and Procedures. This Policy and Procedures shall be made available in the internal centralized document repository system and in Orkim's official website for access to Orkim board members, employees and relevant regulatory stakeholders.

SECTION 3 – APPLICATION

1. The Policy and Procedures apply to Orkim Group Board of Directors ("Board") and all Orkim employees inclusive of those employed or working on board Orkim's vessels and in Orkim's offices ashore.
2. The Policy and Procedures is consistent with the AMLATFA and AML/CFT/CPF Guidelines and shall be read in conjunction with the Group's Limits of Authority ("LOA"), the associated procedures provision in the Management Procedure Manual ("MPM"), Code of Ethics ("COE"), Human Resource and Administration ("HRA") Manual Procedures, Whistleblowing Policy and Procedures, Compliance Policy and Procedures and Internal Audit Policy and Procedures. In the event of a conflict between this Policy and associated internal procedures, this Policy shall govern.
3. In cases where there is a conflict between mandatory laws ("AMLATFA") and the principles contained in this and other internal policies, the law shall prevail.
4. All Orkim's directors and employees are required to be familiar with the applicable requirements and directives of this Policy and its applicable laws. Non – compliance with and violation of this Policy and Procedure and/or applicable laws may result in disciplinary action and/or legal proceeding against those involved, where it deems fit.

ORKIM SDN BHD ANTI MONEY LAUNDERING, COUNTER FINANCING OF TERRORISM AND COUNTERING PROLIFERATION POLICY AND PROCEDURES	ISSUE	REVISION	PAGE
	01 DATE: 15 MAY 2025	00	Page 2 of 8

SECTION 4 - DEFINITIONS

- In this document, the following words shall have the meaning hereby assigned to them except where the context otherwise requires:

Term	Definition
TFS-PF	Targeted Financial Sanctions relating to Proliferation Financing
UNSCR	United Nations Security Council Resolution
Designated Person	A person who has been designated under the Second Schedule of the Strategic Trade (Restricted End-Users and Prohibited End-Users) Order 2010 (P.U. (A) 484/2010).
Orkim Personnel/Employee	A person employed by the Group (inclusive of directors), whether confirmed in a position or on probation, or any other person employed on contract, temporary basis or secondment or appointed by the Group (inclusive of interns and apprentices).

SECTION 5 – MONEY LAUNDERING

- As per the AML/CFT/CPF's Guidelines, money laundering is defined as the involvement of 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.
- The process of money laundering comprises three stages, during which there may be numerous transactions that could alert a reporting institution to the money laundering activities. These stages are:
 - Placement:** The physical disposal of proceeds / benefits of unlawful activities by introducing illegal funds (generally in the form of cash) into the financial system;
 - Layering:** The separation of benefits of unlawful activities from their source by creating layers of financial transactions designed to disguise the audit trail; and
 - Integration:** where integration schemes place the laundered funds back into the economy so that they re-enter the financial system appearing to be legitimate business funds.
- Pursuant to Section 4 of the AMLAFTA, a money laundering offence is committed when a person:
 - engages, directly or indirectly, in a transaction that involves proceeds of an unlawful activity or instrumentalities of an offence;
 - acquires, receives, possesses, disguises, transfers, converts, exchanges, carries, disposes of or uses proceeds of an unlawful activity or instrumentalities of an offence;
 - removes from or brings into Malaysia, proceeds of an unlawful activity or instrumentalities of an offence; or

ORKIM SDN BHD	ISSUE	REVISION	PAGE
	01	00	Page 3 of 8
ANTI MONEY LAUNDERING, COUNTER FINANCING OF TERRORISM AND COUNTERING PROLIFERATION POLICY AND PROCEDURES	DATE: 15 MAY 2025		

d) conceals, disguises or impedes the establishment of 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. 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.

SECTION 6 – TERRORISM FINANCING

1. As per the AML/CFT/CPF's Guidelines, financing of terrorism define as the performance of 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 organizations.
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.

SECTION 7 – PROLIFERATION FINANCING

1. In response to growing concerns over the proliferation of nuclear, biological and chemical weapons and their means of delivery which continue to pose a significant threat to international peace and security, the United Nations Security Council ("UNSC") has intensified efforts to strengthen its global sanctions regime to prevent, suppress and disrupt proliferation of weapons of mass destruction and its financing.
2. As is the case with other UNSC sanctions programmes, targeted financial sanctions on countries and specifically identified individuals and entities (i.e. designated person) is the primary aspect of its overall sanctions regime to effectively disrupt financial flows across known proliferation networks.
3. Recommendation 7 of the Financial Action Task Force ("FATF") Standards requires countries to implement Targeted Financial Sanctions relating to Proliferation Financing ("TFS-PF") made under UNSCRs. Under this standard, countries are required to implement targeted financial sanctions without delay to comply with UNSCRs relating to the prevention, suppression and disruption of the proliferation of weapons of mass destruction and its financing.
4. Proliferation financing 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 ("WMD") 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).
5. TFS-PF is applicable to person designated by the UNSC or the relevant committees set up by the UNSC. Designation or listing criteria are:
 - a) Person engaging in or providing support for, including through illicit means, proliferation-sensitive activities and program

ORKIM SDN BHD	ISSUE	REVISION	PAGE
	01	00	Page 4 of 8
ANTI MONEY LAUNDERING, COUNTER FINANCING OF TERRORISM AND COUNTERING PROLIFERATION POLICY AND PROCEDURES		DATE: 15 MAY 2025	

- b) Acting on behalf of or at the direction of designated person;
- c) Owned or controlled by designated person; and
- d) Person assisting designated person in evading sanctions or violating UNSCR provisions.

SECTION 8 - ROLES AND RESPONSIBILITIES

1. The Group's Board and all Orkim employees must be aware of the intent and requirements of this Policy and Procedures and must ensure that they read, understand and fully comply with the information contained within this document. Specific roles and responsibilities are as follows:

Roles	Responsibilities
Board of Directors ("Board")	<ul style="list-style-type: none"> a) Sets commitment towards anti-money laundering governance within Orkim Group. b) Approves the AML/ CFT/ CPF Policy. c) Maintains oversight on AML/ CFT/ CPF governance, ensuring that the best practices of AML/ CFT/ CPF management system are established, implemented, maintained and reviewed to adequately address the Group's related money laundering risks. d) Promotes appropriate AML/ CFT/ CPF culture within the Group. e) To ensure regular independent audit function to assess the compliance and effectiveness of the AML/CFT/CPF framework in relation to the AMLA and provisions of AML/CFT/CPF Guidelines in which audit report to be tabled to the BRAC and the Board.
Board Risk and Audit Committee ("BRAC")	<p>The Group's Board may delegate the responsibilities to the sub-committee i.e. Board Risk and Audit Committee ("BRAC") appointed by them that shall, in detail:</p> <ul style="list-style-type: none"> a) Provide oversight on the implementation of AML/CFT/CPF risk management. b) Ensure that the management conducts regular reviews to assess the performance, efficiency and effectiveness of the AML/CFT/CPF compliance programme. c) Monitor the performance of the appointed Compliance AML Officer to ensure sufficiency of resources in relation to the administration of policies and procedures and relevant training and development.
Orkim Chief Executive Officer ("CEO")	<ul style="list-style-type: none"> a) Provides overall direction on the establishment and implementation of AML/ CFT/ CPF Policy and Procedures. b) Ensures the integration of the AML/ CFT/ CPF Policy and Procedures requirements into key organization functions and enhance the underlying controls on these key functions to support the policy and procedure requirements. c) Supports the resource allocation and investment in a robust and effective AML/ CFT/ CPF Policy and Procedures. d) Supports adequate training and awareness programmes for related employees of the Group including the appointed compliance officer. e) Communicates on the AML/ CFT/ CPF Policy and Procedures, both internally and externally. f) Promotes appropriate AML/ CFT/ CPF culture within the Group.

ORKIM SDN BHD ANTI MONEY LAUNDERING, COUNTER FINANCING OF TERRORISM AND COUNTERING PROLIFERATION POLICY AND PROCEDURES	ISSUE 01	REVISION 00	PAGE Page 5 of 8
	DATE: 15 MAY 2025		

Roles	Responsibilities
	g) To nominate for the Board's consideration and approval on the appointment of a dedicated AML/CFT/CPF Compliance Officer who will be responsible for compliance of the AML/CFT/CPF internal programmes, policies and procedures.
AML Compliance Officer / Risk, Audit and Compliance ("RAC") Department	<p>The Group shall appoint an appropriate person as the Compliance Officer with the following responsibilities:</p> <ul style="list-style-type: none"> a) Monitor due compliance with this Policy and Procedures. b) To institute and monitor the AML/ CFT/ CPF compliance audit programme of the Group is in place and duly observed by all those concerned. c) To keep full and complete records of matters requiring approval under this Policy and Procedures. d) To report to the Board Sub-Committee i.e. Board Risk & Audit Committee ("BRAC") on a quarterly basis on the state of the Group's compliance with its AML/ CFT/ CPF compliance programme. e) Attends to inquiries about AML/ CFT/ CPF Policy and Procedures and its practices within the Group. f) Continuously update knowledge, expertise and the required authority to discharge his responsibilities effectively, including knowledge on the relevant laws and regulations and the latest AML/CFT/CPF developments.
All Orkim employees	<ul style="list-style-type: none"> a) Read, understand and comply with this Policy and Procedures. b) Attend and complete relevant AML/ CFT/ CPF training. c) Be vigilant and are responsible in preventing, detecting and reporting of money laundering incidents. d) Avoid activities that could lead to or imply that he/she is engaged in any forms of money laundering.

2. Orkim Group must ensure full compliance with the obligations stipulated under Part IV of the AMLAFTA, which include the requirements to:

- a) Implement AML/CFT/CPF 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/CPF compliance audit programme; and
- e) Report suspicious transaction report ("STR")

ORKIM SDN BHD	ISSUE	REVISION	PAGE
	01	00	Page 6 of 8
ANTI MONEY LAUNDERING, COUNTER FINANCING OF TERRORISM AND COUNTERING PROLIFERATION POLICY AND PROCEDURES	DATE: 15 MAY 2025		

SECTION 9 – STANDARD OPERATING PROCEDURES

9.1 Risk Assessment Process in Client/Customer Profiling

1. Orkim's CEO and all Divisional/Departmental Heads must take appropriate steps to identify, assess and understand its Money Laundering/ Terrorism Financing/ Proliferation Financing ("ML/TF/CP") risks, in relation to its customers, countries or geographical areas, services, transactions or delivery channels and other relevant risk factors.
2. The Commercial Division will perform risk assessment processes in risk-profiling its new and current customers, in consultation with the Risk, Audit and Compliance Department to address the following:
 - a) Documenting the risk assessments and findings;
 - b) Considering all the relevant risk factors before determining the level of overall risk and the appropriate level and type of mitigation to be applied;
 - c) Keeping the risk assessment up-to-date considering changes in surrounding circumstances affecting the industry that Orkim operates;
 - d) Having a scheduled periodic risk assessment or as and when specified by the Securities Commission ("SC") for appropriate risk assessment reporting, if required.
3. The Commercial Division may refer to Orkim's Risk Management Policy and Procedures on the process of risk identification and assessment, risk rating, risk prioritization and risk mitigation strategies/action plan. The risk control and mitigation measures implemented must be commensurate with the risk profile of the customer or type of customer.
4. Commercial Division and other internal stakeholders should be more alert to the following possible incidents, which may include, but not limited to:
 - a) Payments proposed to be 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.

9.2 Customer Due Diligence Process

1. Commercial Division shall perform customer due diligence ("CDD") procedures when:
 - a) For any potential and new, as well as regular checks of existing customers.
 - b) It has suspicion of money laundering or terrorism financing or proliferation financing activities regardless of the amount transacted.
 - c) It has reasonable doubts about the adequacy or authenticity of previously obtained information on customer's profile.
2. The Commercial Division is responsible for performing the appropriate CDD procedures relevant to the nature of their business transactions, as follows:
 - a) Identifying the customer and verifying such customer's identity using reliable, independent sources of documents, data or information.
 - b) Verifying that any person purporting to act on behalf of the customer is authorized and identifying and verifying the identity of that person

ORKIM SDN BHD	ISSUE	REVISION	PAGE
	01	00	Page 7 of 8
ANTI MONEY LAUNDERING, COUNTER FINANCING OF TERRORISM AND COUNTERING PROLIFERATION POLICY AND PROCEDURES	DATE: 15 MAY 2025		

- c) Identifying and taking 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 and the intended nature of the business relationship.
 - e) Maintain an updated and current database of names and particulars of designated persons in the UN Consolidated List and Ministry of Home Affairs ("MOHA") List to enable it to detect suspected financing of terrorism and proliferators.
 - f) 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 MOHA and UNSC.
3. If there is any name match, reasonable and appropriate measures must be taken to verify and confirm the identity of its customer. Upon such confirmation, the following steps must be taken immediately–
- a) freeze the customer's fund without delay or block the transaction, if it is an existing customer.
 - b) Reject the customer if the transaction has not commenced.
 - c) lodge a Suspicious Transaction Reporting with the Financial Intelligence and Enforcement Department ("FIED") of the Bank Negara Malaysia ("BNM")
 - d) With the approval of the Board, notify the Securities Commission ("SC").

9.3 Suspicious Transaction Reporting

1. If the Commercial Division or any other Division/Department discover or have suspicious of actual or attempted transaction on money laundering or financing of terrorism activities especially that fits the criteria of "Red Flags", these transactions must be reported to the AML Compliance Officer immediately – via a Suspicious Transaction Report ("STR").
2. Criteria of "Red Flags" – Possible Suspicious Transactions includes, but not limited to:
 - 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.
3. Upon receiving the STR, the AML/CFT/CPF Compliance Officer shall review and evaluate for confirmation. All evaluation shall be reported to the CEO for further action, including escalation endorsement to the Board and to the FIED of BNM and to the Surveillance, Authorization and Supervision Department of the SC through the available reporting channel provided for by these regulators.

ORKIM SDN BHD	ISSUE	REVISION	PAGE
	01	00	Page 8 of 8
ANTI MONEY LAUNDERING, COUNTER FINANCING OF TERRORISM AND COUNTERING PROLIFERATION POLICY AND PROCEDURES	DATE: 15 MAY 2025		

9.4 Record Keeping and Retention

Orkim Group is required to retain, for at least seven (7) years, transaction records, customer due diligence information including agreements, financial accounts, business correspondence 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.

9.5 Communication and Training

1. The Group shall ensure a copy of this Policy and Procedures to be provided to the Orkim Board and all employees stored in a centralized internal document repository system and in Orkim official website, where applicable.
2. The Group shall conduct regular trainings (including refreshers) program for targeted employees including latest regulatory update to ensure compliance to the requirements of AMLATFA and AML/CFT/CPF Guidelines and proper training records shall be maintained by the HRA Department.

9.6 Reporting Policy Violations

1. Suitable reporting channels shall be established and maintained for receiving information regarding violations of this Policy and Procedures, and other matters of integrity provided in good faith by Orkim employees and/or external parties.
2. Orkim employees who, during their activities relating to their employment at the Group, encounter actual or suspected violations of this policy are required to report their concerns to their immediate superior or respective Divisional/ Departmental Heads or to the AML Compliance Officer or may also use the reporting channels stated in Whistle Blowing Policy and Procedures. Such an escalation should be performed in writing providing sufficient details of the date, time and description of the incident citing those whom he believes are involved in the matter.
3. Reports made in good faith, either anonymously or otherwise, shall be addressed in a timely manner and without incurring fear of reprisal regardless of the outcome of any investigation. Retaliation in any form against Orkim employees where the person has, in good faith, reported a violation or possible violation of this policy is strictly prohibited.
4. Any employee found to have deliberately acted against the interests of a person who has in good faith reported a violation or possible violation of this policy shall be subjected to disciplinary proceedings which the Group may pursue. Consequently, any employee who reported a violation, in bad faith, shall also be subjected to disciplinary proceedings which the Group may pursue.
5. All reported violations of this policy will be investigated by the Compliance Officer or any other person within the RAC Department or other investigating team appointed by the CEO.
6. Where notification to the relevant regulatory authority has been made, the Group shall provide full co-operation to the said regulatory authorities.