



FOXBORO (M) SDN BHD
197701002292 (33244-T)

**ANTI-MONEY LAUNDERING
AND
COUNTER FINANCING TERRORISM
POLICY**

Reference No.:	FOXBORO/HRP/01/2026	Revision No.:	0
Effective Date:	12 August 2026	Revision Date:	0

ANTI-MONEY LAUNDERING & COUNTER FINANCING TERRORISM POLICY

1. INTRODUCTION AND PURPOSE

1.1 Money laundering is the process of introducing money, property or other assets derived from illegal and criminal activities into the legal financial and business cycle to give it a legitimate appearance. It is a process to clean 'dirty' money in order to disguise its criminal origin. Money Laundering is an offence under the Anti-Money Laundering, Anti-Terrorism Financing and Proceeds of Unlawful Activities Act 2001 (Act 613) ("the Act").

1.2 The purpose of this AML Policy is to provide guidance to all FoxMay employees concerning how to strengthen anti-money laundering governance and it reiterates FoxMay's commitment to full compliance to the AMLATFA.

Foxboro (M) Sdn Bhd and its subsidiaries (if applicable) (collectively "FoxMay") is committed in exercising fair trade and business competition activity based on integrity, product(s), service quality and price in all of its business operations. FoxMay recognize the importance and its responsibility to ensure that its business practices to fully comply with all applicable laws including the the Act. FoxMay is committed in adopting the principles under the Act in all business operations in order to seek objectives and to safeguard the process of free and fair competition in commercial markets opportunities, the benefit of consumer welfare, efficiency of enterprises and the development of the economy as a whole.

2. SCOPE

This Policy is applicable to FoxMay, its controlled organisations, business associates acting on FoxMay's behalf, the Board of Directors and all employees within FoxMay.

Joint-venture companies in which FoxMay is non-controlling or co-venture and associated companies are encouraged to adopt these or similar principles. Clients, external providers including but not limited to vendors, suppliers, contractors and consultants are also expected to comply with this Policy in relation to all work conducted with FoxMay, or on FoxMay's behalf.

It is FoxMay's policy that an employee participating in the violation of such Policy will be punished for any misconduct. Any behaviour even suggestive of being in breach of this Policy is against FoxMay's policy and any employee engaging in such conduct should expect to face disciplinary action by FoxMay.

3. GENERAL DESCRIPTION OF MONEY LAUNDERING

- 3.1 In principle, money laundering generally involves proceeds of unlawful activities that are related directly or indirectly, to any offence, that is processed through transactions, concealments, or other similar means, so that they appear to have originated from a legitimate source.
- 3.2 The process of money laundering comprises three stages, during which there may be numerous transactions that could alert a business unit (especially a reporting institution) to the money laundering activities. These stages are:
- (a) **Placement:** The physical disposal of proceeds / benefits of unlawful activities by introducing illegal funds (generally in the form of cash) into the financial system;
 - (b) **Layering:** The separation of the illicit proceeds/ benefits of unlawful activities from their source by creating layers of financial transactions designed to disguise the audit trail; and
 - (c) **Integration:** Placement of laundered funds back into the economy so that they re-enter the financial system appearing to be legitimate funds.

4. MONEY LAUNDERING OFFENCE

Pursuant to Section 4 of the Act, a money laundering offence is committed when a person :

- (a) engages, directly or indirectly, in a transaction that involves proceeds of an unlawful activity or instrumentalities of an offence;
- (b) acquires, receives, possesses, disguises, transfers, converts, exchanges, carries, disposes of or uses proceeds of an unlawful activity or instrumentalities of an offence;
- (c) removes from or brings into Malaysia, proceeds of an unlawful activity or instrumentalities of an offence; or
- (d) conceals, disguises or impedes the establishment of the 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.

5. PUNISHMENT FOR MONEY LAUNDERING OFFENCE

Under the prevailing Act, 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 Ringgit Malaysia Five (5) million, whichever is the higher.

6. GENERAL DESCRIPTION OF TERRORISM FINANCING

6.1 Financing of terrorism 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.

6.2 Section 3(1) of the Act 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.

7. POLICY STATEMENT

7.1 FoxMay strongly objects to all practices related to money laundering, including dealing in the proceeds of criminal activities and terrorism financing. As a general rule, reasonable degree of due diligence must be carried out in order to understand the business and background of any prospective customer, vendor, third party or business partner that intends to do business with FoxMay to determine the origin and destination of money or assets involved. Any suspected activities relating to money laundering or terrorism financing should be reported immediately to Bank Negara Malaysia and relevant authorities.

7.2 FoxMay prohibits all involvement in money laundering activities and terrorism financing either directly or indirectly. The activities may include, but not limited to the following:

- (a) Payments 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.

8. CUSTOMER DUE DILIGENCE

8.1 As a general principle, the Supply Chain Management, Business Development, Finance, Operations or other departments that initiates, manages or is responsible for the relevant business relationship with a customer are required to perform Customer Due Diligence (“CDD”) procedures:

- (a) before establishing a new business relationship;
- (b) when it has any suspicion of money laundering or terrorism financing activities regardless of the amount transacted;
- (c) it has any doubt about the adequacy or authenticity of previously obtained information.

8.2 The Supply Chain Management, Business Development, Finance, Operations or other department that initiates, manages or is responsible for the relevant business relationship with a customer is responsible to implement the appropriate CDD procedures relevant to the nature of their business transactions. The relevant departments should adopt a risk-based approach when deciding the degree of CDD to apply. Risks are assessed at the outset of a business relationship and updated regularly.

8.3 The CDD procedures should minimally include :-

- (a) identifying the customer (including foreign body corporate) and verify such customer’s identity using reliable, independent source of documents, data or information;
- (b) verifying that any person purporting to act on behalf of the customer is authorised, and identifying and verifying the identity of that person;
- (c) identifying and take 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 of opening an account and the intended nature of the business relationship; and

- (e) 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 Ministry of Home Affairs (MOHA) and United Nations Security Council.

9. SUSPICIOUS TRANSACTION REPORTING

9.1 If any suspicious money laundering or financing of terrorism activities are detected or any attempted transaction fits the list of “Red Flags” as in the table below, these transactions must be reported to the Group Chief Financial Officer (“GCFO”) immediately – via an Internal Suspicion Report.

9.2 Examples of “Red Flags” – Possible Suspicious Transactions

- (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 payment 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.

9.3 Upon receiving the Internal Suspicion Report, the GCFO shall evaluate the grounds for suspicion and if suspicion is confirmed he or she shall submit a suspicious transaction report to the Financial Intelligence Unit in Bank Negara Malaysia on the next working day through any of the following modes:-

No	Mode	To Whom
1.	Mail	The Director, Financial Intelligence Unit Bank Negara Malaysia Jalan Dato’ Onn 50480 Kuala Lumpur (To be opened by addressee only)
2.	Fax	+603-2693 3625
3.	E-Mail	str@bnm.gov.my
4.	Online	https://bnmapp.bnm.gov.my/fins2

10. RECORDS KEEPING AND THE RETENTION OF RECORDS

10.1 All departments within FoxMay which deals with business transactions must keep record of all transactions and ensure they are up to date and relevant. The records must at least include the following information for each transaction:

- (a) Documents relating to the identification of the customer in whose name the account is opened or transaction is executed;
- (b) The identification of the beneficial owner or the person on whose behalf the account is opened or transaction is executed;
- (c) Records of the relevant account pertaining to the transaction executed;
- (d) The type and details of transaction involved;
- (e) The origin and the destination of the funds, where applicable; and
- (f) Any other information as required by the authorities.

10.2 All departments within FoxMay which deals with business transactions are required to retain, for at least six (6) years, the records of transactions, relevant customer due diligence information and other relevant records including agreements, financial accounts, business correspondences 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.

11. RESPONSIBILITY FOR THE POLICY

11.1 The Board of Directors and the Management team of FoxMay set the tone at the top providing leadership and support for the Policy and take responsibility for its effectiveness within its business units. FoxMay Management is responsible for the implementation of the Policy and all communication and training activities in relation to the Policy to ensure that those reporting to them are made aware of, and understand, this Policy.

11.2 The Management team of FoxMay shall provide appropriate levels of AML/CFT training for its employees at all levels throughout the organisation.

12. EFFECTIVE DATE

The Policy is approved by the Board of Directors and effective as of 12 August 2026.