Anti-Money Laundering & Counter Financing of Terrorism (AML/CFT) Policy

Version	1.0
Effective Date	01 June 2025
Approved By	Compliance & Risk Committee
Next Review Date	01 June 2026

1. Purpose

The purpose of this policy is to establish a framework to prevent Bayarcash Sdn. Bhd. (Registration Number: 202201040365 (1486062-H)) ("**Bayarcash**") from being used for money laundering (ML) or terrorist financing (TF) activities. The policy ensures compliance with applicable laws, regulations, and international standards, including those set forth by the Financial Action Task Force (FATF) and relevant national authorities.

2. Scope

This policy applies to:

- All Bayarcash employees, managements, and directors.
- Contractors, agents, service providers, and third parties acting on behalf of Bayarcash.
- All business units, subsidiaries, and affiliates of Bayarcash.

3. Definitions

Term	Definition
Money Laundering (ML)	The process of disguising the origins of illegally obtained money to make it appear legitimate.
Terrorist Financing (TF)	Providing or collecting funds, directly or indirectly, with the intent or knowledge that they will be used to support terrorist acts or organizations.
Customer Due Diligence (CDD)	Procedures used to identify and verify the identity of customers.
Know Your Customer (KYC)	The process of gathering and verifying customer information before establishing a business relationship.

4. Policy Statement

The organization is committed to:

- Preventing and detecting any attempt to use its operations for ML/TF purposes.
- Fully complying with all applicable AML/CFT laws and regulations.
- Promoting a culture of compliance and ethical conduct among all staff.

No business relationship or transaction should be undertaken if it violates AML/CFT laws or poses an unacceptable risk.

5. Responsibilities

Role	Responsibilities
Board of Directors & Senior Management	Approve AML/CFT policy; ensure adequate resources and oversight.
Compliance Officer (MLRO)	Implement AML/CFT program, monitor compliance, report suspicious activities.
Employees	Adhere to AML/CFT procedures, conduct CDD, report suspicious transactions promptly.

6. Customer Due Diligence (CDD) & KYC

The organization must:

- Identify and verify the identity of all customers using reliable, independent documents.
- Understand the nature and purpose of customer relationships.
- Conduct ongoing monitoring of transactions to ensure consistency with customer profiles.
- Apply Enhanced Due Diligence (EDD) to high-risk customers (e.g., politically exposed persons, non-resident clients).

7. Record Keeping

All records related to identification, verification, and transactions shall be retained for at least 7 years (as required by law) and be readily available to competent authorities upon request.

8. Reporting of Suspicious Transactions

Employees must promptly report any suspicious activity to the Money Laundering Reporting Officer (MLRO).

The MLRO will:

- Review and investigate all reports.
- File a Suspicious Transaction Report (STR) with the relevant Financial Intelligence Unit (FIU) if warranted.
- Maintain confidentiality at all stages.

9. Risk-Based Approach

The organization adopts a Risk-Based Approach (RBA), identifying and assessing ML/TF risks associated with:

- Customers and beneficial owners.
- Products and services.
- Geographic locations.
- Delivery channels.

Resources and controls are applied proportionately to the level of risk identified.

10. Training & Awareness

Regular AML/CFT training will be provided to all staff to ensure understanding of:

- Relevant laws and internal procedures.
- How to recognize and report suspicious activities.
- Updates on emerging risks and typologies.

11. Internal Controls & Independent Audit

- Internal controls must ensure effective implementation of AML/CFT procedures.
- Periodic independent audits or reviews shall assess the adequacy and effectiveness of the AML/CFT program.

12. Sanctions Compliance

The organization must comply with United Nations, national, and regional sanctions lists. Customers and transactions will be screened against applicable sanctions lists before onboarding or processing.

13. Breach of Policy

Any violation of this policy may result in disciplinary action, up to and including termination of employment, and may also lead to legal penalties.

14. Review & Updates

This policy shall be reviewed at least annually or when there are significant changes in regulatory requirements or business operations.