Policy Name:	Know Your Customer (KYC), Customer Due Diligence (CDD), Anti Money Laundering (AML), Combating Financing Of Terrorism (CFT) Policies and Procedures
Approval Authority:	Board of Directors

1. INTRODUCTION

1.1 This document outlines **Amanah Investments Limited**'s policies, procedures, and practices in relation to **Know Your Customer (KYC)**, **Customer Due Diligence (CDD)**, **Anti-Money Laundering (AML)**, and **Combating the Financing of Terrorism (CFT)**.

1.2 This document supersedes the KYC policy previously approved in 2010 and the KYC/CDD, AML/CFT policy created on January 2, 2018.

2. OBJECTIVE

2.1 To protect the Company from the increasing risk of organized criminal activity, money laundering, and terrorist financing.
2.2 To perform an overall risk assessment of the Company in relation to **Money Laundering (ML)** and **Terrorist Financing (TF)**.
2.3 To align company procedures and practices with:

- Securities Act, 2015 and related regulations issued thereunder
- Anti-Money Laundering Act, 2010
- Securities and Exchange Commission of Pakistan (Anti-Money Laundering and Countering Financing of Terrorism) Regulations, 2018
- International best practices as recommended by the Financial Action Task Force (FATF), February 2012
  (https://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/FATF_Recommendations.pdf)
- SECP Guidelines on AML & CFT Regulations, 2018

2.4 To develop and implement policies and procedures that discourage money laundering and help identify and monitor suspicious transactions or parties.

3. SCOPE

3.1 This policy applies to all operations of **Amanah Investments Limited**, including business of other financial institutions routed through the Company. It ensures compliance with national regulations on KYC, CDD, AML/CFT as well as SECP rules and FATF recommendations—whichever are more exhaustive.

4. DEFINITIONS

4.1 **Know Your Customer (KYC)** is the process of identifying and verifying a customer's identity and collecting relevant information required for establishing a business relationship. This includes:

- Verifying identity and address documentation at the start of the relationship
- Gathering details about the customer's source of income and nature of business

4.2 **Customer Due Diligence (CDD)** refers to collecting factual information to assess the level of risk a customer presents, including risks of money laundering and terrorist financing.

4.3 A **Customer** is any person or entity that applies for or maintains a trading account with the Company.

4.4 All terms used in this policy carry the definitions provided in the Anti-Money Laundering Act, 2010 and SECP AML/CFT Regulations, 2018.

5. ELEMENTS OF THE POLICY

This KYC/CDD Policy includes the following elements:

- A. Entity Risk Assessment in relation to ML/TF
- B. Customer Risk
    - B1. Customer Identification
    - B2. Risk Assessment of Customer
    - B3. High-Risk Classification Factors
    - B4. Low-Risk Classification Factors

- C. Ongoing Due Diligence
- D. Compliance Function
- E. Monitoring and Reporting
- F. Data Retention
- G. Training and Employee Screening
- H. Audit Function

A. ENTITY RISK ASSESSMENT IN RELATION TO ML/TF

A1. The Company will annually conduct a risk assessment to identify and understand its exposure to ML and TF risks across:

- Its customer base
- Jurisdictions or countries customers are from or located in
- Jurisdictions or countries the Company operates in
- Products, services, transactions, and delivery channels

A2. The process will include:

- Documenting risk areas and contributing factors
- Evaluating all risk factors before finalizing risk level and mitigation plan
- Defining the Company's risk tolerance
- Categorizing risks as high, medium, or low
- Maintaining updated assessments responsive to regulatory or operational changes
- Sharing the risk assessment with the SECP when required

A3. The assessment will also consider the distinct nature of **Terrorist Financing**, which may involve legally sourced funds. Hence, risk assessment for ML is also relevant for TF.

A4. The Compliance Department will prepare the entity-level risk document, which will be reviewed by the COO and CEO and submitted to the Board of Directors with the year-end Compliance Report.

A5. Key considerations for assessing ML/TF risks:

- Understand the inherent risks in customer base, services, channels, jurisdictions, and operations
- Classify risks using categories like high, medium, or low

- Evaluate both the **likelihood** and **impact** of identified risks (e.g., regulatory fines, reputational damage)
- Use this evaluation to form the Company's total risk profile

A5.5. Risk Mitigation and Risk-Based Approach
The Company will:

- Implement Board-approved policies and controls to manage identified risks
- Monitor compliance and implementation
- Apply enhanced due diligence where necessary
- Incorporate AML compliance into the internal audit plan
- Use MIS for improved AML oversight

A6. Products, Practices and Technologies

A6.1 Assess ML/TF risks associated with:

- New products and business practices
- New or developing technologies

A6.2 Risk assessments should be conducted before launch and appropriate safeguards implemented.

A6.3 Extra attention must be given to innovations that enhance anonymity or reduce transparency.

A7. Risk assessments will follow the format outlined in SECP AML/CFT Guidelines (Annexure I).

A8. System adequacy and controls will be periodically assessed using the Compliance Assessment Checklist (Annexure II).

A9. Additional mitigation measures may include:

- Tailored verification scope for high-risk customers

- Transaction limits
- Senior management approval for certain transactions (e.g., PEPs)
- Refusing/terminating high-risk accounts

A10. Residual Risk Evaluation

- Compare residual risks (post-mitigation) with Company's risk tolerance
- If residual risk remains too high, strengthen control measures accordingly