
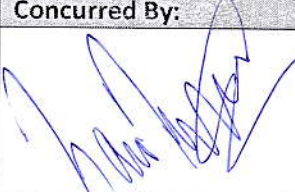

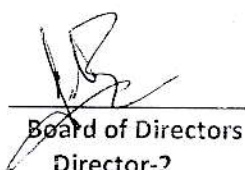




## AML/CFT POLICY OF NAEL CAPITAL (PVT) LIMITED ("NCPL")

APPROVAL SHEET
Policy Owner: Compliance Department
Implementation Responsibility: Compliance Officer
Custodian: Compliance Department
Operation Jurisdiction: All Departments of NCPL
Review Frequency: Every Year End or earlier if required
Review Responsibility: Compliance Department
Approval Date: 11-November-2019

Recommended By:	Concurred By:
 Muhammad Yousuf Compliance Officer	 Nasir Muqet CEO, NCPL

Approved By:	
 Board of Directors Director-1	 Board of Directors Director-2



## A. GENERAL PRINCIPLES:

### 1. DEFINITION OF MONEY LAUNDERING AND TERRORIST FINANCING:

Money Laundering (“ML”) and Terrorist Financing (“TF”) are economic crimes that threaten a country’s overall financial sector reputation and expose financial institutions to significant operational, regulatory, legal and reputational risks, if used for ML and TF.

### 2. PURPOSE AND SCOPE OF AML AND CFT REGIME:

An effective Anti-Money Laundering and Countering the Financing of Terrorism (“AML/CFT”) regime requires financial institutions to adopt and effectively implement appropriate ML and TF control processes and procedures, not only as a principle of good governance but also as an essential tool to avoid involvement in ML and TF. AML and CFT Regime is governed under Anti-Money Laundering Act, 2010 (“AML Act”), Anti-Money Laundering Rules, 2008 (“AML Rules”) made under the Anti-Money Laundering Ordinance, 2007 (“AML Ordinance”), Securities and Exchange Commission of Pakistan (Anti Money Laundering and Countering Financing of Terrorism) Regulations, 2018 (“SECP AML/CFT Regulations”) made under the Securities and Exchange Commission of Pakistan Act, 1997 (“SECP Act”), upon recommendation of Financial Monitoring Unit (“FMU”) established under AML Act and Guidelines on SECP AML/CFT Regulations issued by SECP in September 2018 and Pakistan National Risk Assessment (“PNRA 2019”) Report on Money Laundering and Terrorist Financing issued in September 2019.

### 3. CUSTOMER DUE DILIGENCE (CDD):

#### 3.1. For Natural Persons:

3.1.1. The Nael Capital (Pvt.) Limited (“House”) is required to carry out KYC and anonymous accounts or accounts in fictions names are, as a policy, not allowed. The House takes the following steps to ensure that its Customers are who they purport themselves to be:

- 3.1.1.1. identify and verify the customers including their beneficial owners;
- 3.1.1.2. understand the intended nature and purpose of the relationship;
- 3.1.1.3. know actual ownership; and
- 3.1.1.4. know control structure of the customer.

3.1.2. The House conducts ongoing due diligence on the business relationship and scrutinize transactions undertaken throughout the course of that relationship to ensure that transactions being conducted are consistent with:

- 3.1.2.1. Knowledge of the customer;
- 3.1.2.2. Assessment of Business and Risk Profiles;
- 3.1.2.3. Where necessary, the source of funds.



- 3.1.3. The House conducts CDD when establishing a business relationship if:
  - 3.1.3.1. There is a suspicion of ML/TF; or
  - 3.1.3.2. There are doubts as to the veracity or adequacy of the previously obtained customer identification information.
  
- 3.1.4. In case of suspicion of ML/TF, the House:
  - 3.1.4.1. Seeks to identify and verify the identity of the customer and the beneficial owner(s), irrespective of any specified threshold that might otherwise apply; and
  - 3.1.4.2. File a Suspicious Transaction Reporting ("STR") with the FMU, in accordance with the requirements under the Law.
  
- 3.1.5. The House monitors transactions to determine whether they are linked and restructured into two or more transactions of smaller values to circumvent the applicable threshold.
  
- 3.1.6. The House verifies the identification of a customer using reliable independent source documents, data or information including verification of CNICs from Verisys.
  
- 3.1.7. The House ensures that they understand the purpose and intended nature of the proposed business relationship or transaction.
  
- 3.1.8. The house also verifies whether that authorized person is properly authorized to act on behalf of the customer while conducting CDD on the authorized person(s) using the same standards that are applicable to a customer and ascertaining the reason for such authorization and obtain a copy of the authorization document.
  
- 3.2. **Beneficial Ownership of Legal Persons and Legal Arrangements:**
  - 3.2.1. The House identifies and verifies the identity of the customer, and understands the nature of its business, and its ownership and control structure.
  
  - 3.2.2. The purpose of the requirements set out regarding the identification and verification of the applicant and the beneficial owner is twofold:
    - 3.2.2.1. First, to prevent the unlawful use of legal persons and arrangements, by gaining a sufficient understanding of the applicant to be able to properly assess the potential ML/TF risks associated with the business relationship; and
    - 3.2.2.2. Second, to take appropriate steps to mitigate the risks.
  
  - 3.2.3. If the House has any reason to believe that an applicant has been refused facilities by another House due to concerns over illicit activities of the customer, it should consider classifying that applicant:
    - 3.2.3.1. as higher-risk and apply enhanced due diligence procedures to the customer and the relationship;
    - 3.2.3.2. filing a STR; and/or



- 3.2.3.3. not accepting the customer in accordance with its own risk assessments and procedures.
  - 3.3. The House accepts copies of the documents for identifying a Customer verified by seeing originals during establishing business relationship.
  - 3.4. **Identification of Customers that are not physically present:**
    - 3.4.1. The House applies equally effective Customers identification procedures and ongoing monitoring standards for Customers not physically present for identification purposes as for those where the client is available for interview.
    - 3.4.2. Consequently, there are increased risks and practices must carry out at least one of the following measures to mitigate the risks posed:
      - 3.4.2.1. further verifying the Customer's identity on the basis of documents, data or information referred in Annexure-1 to AML/CFT Regulations, but not previously used for the purposes of verifying the client's identity; and
      - 3.4.2.2. taking supplementary measures to verify the information relating to the client that has been obtained by the practice.
  - 3.5. **If Customer Due Diligence Measures are Not Completed.**

Where the House is unable to complete and comply with CDD requirements as specified in the Regulations:

    - 3.5.1. **For New Customers:**
      - 3.5.1.1. it shall not open the account;
      - 3.5.1.2. commence a business relationship; or
      - 3.5.1.3. perform the transactions.
    - 3.5.2. **For Existing Customers:**
      - 3.5.2.1. The House shall terminate the relationship.
      - 3.5.2.2. Additionally, the House shall consider making a STR to the FMU.
4. **ENHANCED CUSTOMER DUE DILIGENCE MEASURES:**
- 4.1. **High Risk Persons or Transactions:**
    - 4.1.1. The House performs Enhanced Due Diligence on the following:
      - 4.1.1.1. Persons or transactions involving a country identified as higher risk by FATF;
      - 4.1.1.2. Persons or transactions involving higher risk countries for ML, TF and corruption or subject to international sanctions; and
      - 4.1.1.3. Any other situation representing a higher risk of ML/TF including those that you have identified in your Risk Assessment.
  - 4.2. **High Risk Business Relationship:**
    - 4.2.1. The House applies enhanced CDD measures for high risk business relationships include:

- 4.2.1.1. Obtaining additional information on the applicant/customer (e.g. occupation, volume of assets, information available through public databases, internet, etc.);
- 4.2.1.2. Updating more regularly the identification data of applicant/customer and beneficial owner;
- 4.2.1.3. Obtaining additional information on the intended nature of the business relationship;
- 4.2.1.4. Obtaining additional information on the source of funds or source of wealth of the applicant/customer;
- 4.2.1.5. Obtaining additional information on the reasons for intended or performed transactions;
- 4.2.1.6. Obtaining the approval of CEO, Compliance Officer and Head of Sales to commence or continue the business relationship; and
- 4.2.1.7. Conducting enhanced monitoring of the business relationship, by increasing the number and timing of controls applied, and selecting patterns of transactions that need further examination.

#### 4.3. High Risk Countries and Territories:

- 4.3.1. The house consults the following to identify above persons or transactions to be aware of the high risk countries/territories:
  - Publicly available information;
  - Sanctions list issued by the UN;
  - National Risk Assessment Report 2019;
  - FATF high risk and non-cooperative jurisdictions; and
  - FATF and its regional style bodies (FSRBs) and Transparency international corruption perception index.

#### 4.4. Complex and Unusual Transactions:

The House examines the background and purpose of all complex, unusual large transaction, and all unusual patterns of transactions, that have no apparent economic or lawful purpose and conduct enhanced CDD Measures consistent with the risk identified.

#### 4.5. Suspicious Accounts:

- 4.5.1. The house applies enhanced CDD measures on the following accounts:
  - Customers who instructs not to issue any correspondence to the account holder's address;
  - Customers who have 'Hold mail' accounts; and
  - Where the evidence of identity of the account holder is not already in the file.

### 5. SIMPLIFIED DUE DILIGENCE MEASURES ("SDD"):

#### 5.1. General Principles of SDD:

- 5.1.1. The House conducts SDD in case of lower risks identified by it. However, the House ensures that the low risks it identifies are commensurate with the low risks identified by



- the country or the Commission. While determining whether to apply SDD, the House will pay particular attention to the level of risk assigned to the relevant sector, type of customer or activity.
- 5.1.2. SDD is not acceptable in higher-risk scenarios where there is an increased risk, or suspicion that the applicant is engaged in ML/TF, or the applicant is acting on behalf of a person that is engaged in ML/TF.
- 5.1.3. Where the risks are low and where there is no suspicion of ML/TF, the law allows the House to rely on third parties for verifying the identity of the applicants and beneficial owners.
- 5.1.4. Where House decides to take SDD measures on an applicant/customer, it should document the full rationale behind such decision and make available that documentation to the Commission on request.

**5.2. Category of Low Risk Customers:**

5.2.1. The House rates a Customer as low risk justifying it in writing and low risk Customers my included the following:

- regulated persons and banks provided they are subject to requirements to combat money laundering and terrorist financing consistent with the FATF recommendations and are supervised for compliance with those requirements;
- public listed companies that are subject to regulatory disclosure requirements to ensure adequate transparency of beneficial ownership; and
- financial products or services that provide appropriately defined and limited services to certain types of customers, so as to increase access for financial inclusion purposes.

**5.3. SDD Measures:**

5.3.1. The House applies following Simplified Due Diligence measures on Low risk Customer:-

- reducing the frequency of customer identification updates;
- reducing the degree of on-going monitoring and scrutinizing transactions, based on a reasonable monetary threshold; and
- not collecting specific information or carrying out specific measures to understand the purpose and intended nature of the business relationship, but inferring the purpose and nature from the type of transaction or business relationship established:

**6. POLITICALLY EXPOSED PERSONS:**

**6.1. DEFINITION OF PEP:**

6.1.1. A Politically Exposed Person (PEP) is defined by the Financial Action Task Force (FATF) as an individual who is, or has been entrusted with a prominent public function. Due to their position and influence, it is recognized that many PEPs are in positions that potentially can be abused for the purpose of committing money laundering (ML) offences and related predicate offences, including corruption, bribery, and conducting activity related to terrorist financing (TF). The potential risks associated with PEPs justify the application of

additional anti-money laundering/counter-terrorist financing (AML/CFT) preventative measures with respect to business relationships with PEPs.

## 6.2. POLITICALLY EXPOSED PERSONS CATEGORIES

6.2.1. The difference between foreign and domestic PEPs may be relevant for making specific risk assessments to help gain a holistic view of potential risk. In the first instance PEPs are classified at a high level in the following categories:

### 6.2.2. Foreign PEPs

Individuals who are, or have been entrusted with prominent public functions by a foreign country, for example heads of state or government, senior politicians, senior government, judicial or military officials, senior executives of state owned corporations, important political party officials.

### 6.2.3. Domestic PEPs

Individuals who are, or have been entrusted domestically with prominent public functions, for example heads of state or of government, senior politicians, senior government, judicial or military officials, and senior executives of state owned corporations, important political party officials.

### 6.2.4. International organization PEPs

A person who is, or has been entrusted with a prominent function by an international organization, refers to members of senior management or individuals who have been entrusted with equivalent functions i.e. directors, deputy directors, and members of the board.

### 6.2.5. Family members

Individuals who are related to a PEP, either directly (consanguinity) or through marriage.

### 6.2.6. Close associates

Individuals who are closely connected to a PEP, either socially or professionally.

## 6.3. Seeking approval from senior management:

6.3.1. The House shall obtain CEO, CO and Head of Sales' approval to determine the nature and extend of EDD where the ML/TF risks are high. In assessing the ML/TF risk of a PEP, the Houses shall consider factors such as whether the Customer who is a PEP:

6.3.1.1. Is from a high risk country;

6.3.1.2. Has prominent public function in sectors know to be exposed to corruption;

6.3.1.3. Has business interests that can cause conflict of interests (with the position held).

## 6.4. Taking adequate measures to establish source of wealth and source of funds:

6.4.1. The House consider following red flags (in addition to the Red Flags considered for other applicants):





- 6.4.1.1. The information that is provided by the PEP is inconsistent with other (publicly available) information, such as asset declarations and published official salaries;
  - 6.4.1.2. Funds are repeatedly moved to and from countries to which the PEP does not seem to have ties;
  - 6.4.1.3. A PEP uses multiple bank accounts for no apparent commercial or other reason;
  - 6.4.1.4. The PEP is from a country that prohibits or restricts certain citizens from holding accounts or owning certain property in a foreign country.
- 6.4.2. The House shall take a risk based approach in determining whether to continue to consider a customer as PEP who is no longer a PEP. The factors that they should consider include:
- 6.4.2.1. the level of (informal) influence that the individual could still exercise; and
  - 6.4.2.2. Whether the individual's previous and current function are linked in any way (e.g., formally by appointment of the PEPs successor, or informally by the fact that the PEP continues to deal with the same substantive matters).
- 6.4.3. Additionally, where appropriate, House shall consider filing a STR.

## **7. SUSPICIOUS TRANSACTION REPORTING:**

### **7.1. Defining what is a suspicious transaction?**

A suspicious transaction is one for which there are reasonable grounds to suspect that the transaction is related to a money laundering offence or a terrorist activity financing offence. A suspicious transaction can include one that was attempted.

### **7.2. How you and your employees/agents will identify suspicious transactions:**

- 7.2.1. The House may assess the following transactions as suspicious where a transaction is inconsistent in amount, origin, destination, or type with a Customer's know, legitimate business or personal activities;
- 7.2.2. The House shall put on enquiry if transaction is considered unusual.
- 7.2.3. The House shall pay special attention to the following transactions:
  - 7.2.3.1. All complex transactions;
  - 7.2.3.2. Unusual large transactions; and
  - 7.2.3.3. Unusual pattern of transactions.
  - 7.2.3.4. Which have no apparent economic or visible lawful purpose.

### **7.3. Reporting to Compliance Officer:**

Where the enquiries conducted by the House do not provide a satisfactory explanation of the transactions, respective sales agent may consider that there are grounds for suspicion requiring disclosure and escalating the matter to the Compliance Officer.

### **7.4. Reporting to Relevant Authority:**

- 7.4.1. The Compliance Officer of the House shall conduct enquiries regarding complex, unusual large transaction, and unusual patterns of transactions, their background and document their results properly. He may make such transaction available to relevant authorities upon their request.





7.4.2. Activities which should require further enquiry may be recognizable as falling into one or more of the following categories:

- 7.4.2.1. any unusual financial activity of the Customer in the context of the Customer's own usual activities;
- 7.4.2.2. any unusual transaction in the course of some usual financial activity;
- 7.4.2.3. any unusually-linked transactions;
- 7.4.2.4. any unusual method of settlement;
- 7.4.2.5. any unusual or disadvantageous early redemption of an investment product;
- 7.4.2.6. any unwillingness to provide the information requested.

**7.4.3. Reporting to Commission and FMU:**

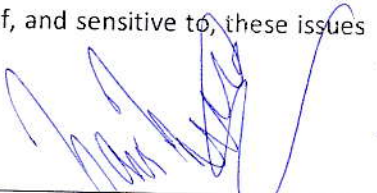
- 7.4.3.1. House is required to report total number of STRs filed to the Commission on bi-annual basis within seven days of close of each half year.
- 7.4.3.2. Vigilance systems should require the maintenance of a register of all reports made to the FMU. Such registers should contain details of:
  - 7.4.3.2.1. the date of the report;
  - 7.4.3.2.2. the person who made the report;
  - 7.4.3.2.3. the person(s) to whom the report was forwarded; and
  - 7.4.3.2.4. reference by which supporting evidence is identifiable.
- 7.4.3.3. Where an applicant or a Customer is hesitant/fails to provide adequate documentation (including the identity of any beneficial owners or controllers), the House shall consider filing a STR.
- 7.4.3.4. Where an attempted transaction gives rise to knowledge or suspicion of ML/TF, the Securities Broker shall report attempted transaction to the FMU.
- 7.4.3.5. Once suspicion has been raised in relation to an account or relationship, in addition to reporting the suspicious activity The Securities Broker shall ensure that appropriate action is taken to adequately mitigate its risk being used for criminal activities.
- 7.4.3.6. The House may include a review of either the risk classification of the Customer or account or of the entire relationship itself.
- 7.4.3.7. Appropriate action may necessitate escalation to the appropriate level of decision-maker to determine how to handle the relationship, taking into account any other relevant factors, such as cooperation with law enforcement agencies or the FMU.

**7.5. Tipping-off & Reporting:**

**7.5.1. The Law prohibits tipping-off:**

- 7.5.1.1. A risk exists that Customers could be unintentionally tipped off when the House is seeking to complete its CDD obligations or obtain additional information in case of suspicion of ML/TF.
- 7.5.1.2. The applicant/customer's awareness of a possible STR or investigation could compromise future efforts to investigate the suspected ML/TF operation.
- 7.5.1.3. If the House forms a suspicion of ML/TF while conducting CDD or ongoing CDD, it will take into account the risk of tipping-off when performing the CDD process.

- 7.5.1.4. The House reasonably believes that performing the CDD or on-going process will tip-off the applicant/customer, it may choose not to pursue that process, and should file a STR.
- 7.5.1.5. The House ensures that their employees are aware of, and sensitive to, these issues when conducting CDD or ongoing CDD.



---

**Nasir Muqet**  
*Chief Executive*