ANTI-MONEY LAUNDERING

AND

SUPPRESSION OF TERRORIST FINANCING POLICY

NDB CAPITAL HOLDINGS LIMITED

APPROVED BY BOARD AUDIT RISK AND COMPLIANCE COMMITTEE ON 05th JUNE 2024

ADOPTED BY THE BOARD OF DIRECTORS OF NDB CAPITAL HOLDINGS LIMITED ON 07th JUNE 2024

INFORMATION SHEET

<table>
<tr><td>Policy Title</td><td>Anti-Money Laundering and Suppression of Terrorist Financing Policy</td></tr>
<tr><td>Target Audience</td><td>All Directors and Employees of NDB Capital Holdings Limited & its subsidiaries</td></tr>
<tr><td>Issued By</td><td>Head of Compliance, NDB Capital Holdings Limited</td></tr>
<tr><td>Reviewed By</td><td>Compliance Department and Risk Department of National Development Bank (“NDB Bank”)</td></tr>
<tr><td>Approved By</td><td>Board Audit, Risk and Compliance Committee</td></tr>
<tr><td>Adopted By</td><td>Board of Directors- NDB Capital Holdings Limited and Boards of Directors of NCAP Subsidiaries</td></tr>
<tr><td>Implementation Date</td><td>December 2017</td></tr>
<tr><td>Next Review Date</td><td>July 2026</td></tr>
<tr><td>Responsible Person for Policy</td><td>Head of Compliance – NDB Capital Holdings Limited</td></tr>
<tr><td>Responsible Person for implementation</td><td>Head of Compliance of NCAP and designated Compliance Officers of NCAP Group</td></tr>
<tr><td>Document History</td><td>
<table>
<tr><td>Date</td><td>Version</td><td>Amendments</td></tr>
<tr><td>February 2014</td><td>1</td><td>N/A</td></tr>
<tr><td>December 2017</td><td>2</td><td>New Policy</td></tr>
<tr><td>September 2022</td><td>3</td><td>Amendment</td></tr>
<tr><td>July 2024</td><td>4</td><td>Amendment</td></tr>
</table>
</td></tr>
<tr><td>Further Information</td><td>Head of Compliance, NDB Capital Holdings Limited</td></tr>
</table>

Table of Contents **Page**

1.0 INTRODUCTION

1.1 PURPOSE OF THE POLICY

Over the years, Sri Lanka has continuously strived to enhance its anti-money laundering and terrorists financing framework in order to bring itself in line with the international anti-money laundering standards and has introduced several important legislative enactments. The revised Anti-Money Laundering and Suppression of Terrorist Financing Policy ("the Policy") is adopted by the NCAP Group (NDB Capital Holdings Limited and its subsidiaries which include NDB Wealth Management Limited, NDB Securities (Private) Limited, NDB Investment Bank Limited and NDB Zephyr Lanka Limited will be collectively referred to as the "NCAP Group" in this policy) in order to further strengthen the anti-money laundering compliance and in response to the recent developments and guidelines for capital market intermediaries. Further, this Policy is aligned to the Anti-Money Laundering and Suppression of Terrorist Financing Policy of NDB Bank which is the parent company of NCAP Group.

1.2 POLICY STATEMENT

NCAP Group is committed to the highest standards of anti-money laundering and combatting of terrorist financing compliance. The Group as a leading financial services conglomerate which is involved in various capital market transactions and investment activities takes every step to comply with the requirements of the legislative enactments and understands the importance of minimizing the risk of its businesses being used by money launderers or other criminals.

It is the policy of NCAP to comply with all applicable laws and regulations relating to the prevention of money laundering and suppression of terrorist financing and to adhere to the highest standards to prevent use of the products and services of NCAP Group for money laundering purposes and to maintain an effective anti-money laundering compliance program and procedures.

1.3 APPLICATION OF THE POLICY

This Policy applies to all Directors and Employees of the NCAP Group and they are required to comply with this Policy in all business transactions. This policy shall be implemented by each of the group companies as practicably applicable to them based on the nature of the business carried out by each of the companies. The business operations of NDB Investment Bank Limited differs from NDB Stockbrokers (Pvt)

Limited and NDB Wealth Limited which deals with client funds. The application of AML checks would vary based on this fundamental difference.

1.4 VIOLATIONS OF THE POLICY

A violation of this Policy carries serious repercussions. All concerns about violations of this Policy is dealt with promptly according to the standard procedures. The Group takes disciplinary or preventive actions deemed appropriate to address the existing or potential violations, up to and including termination of the employment of employees and directorship of directors. Violations of this Policy may constitute violations of law, which may result in criminal or civil penalties for individuals and the Company. If anyone becomes aware of any existing or potential violations of this Policy, it should be promptly notified to the Compliance Officer or to relevant authorities in accordance with the NCAP Group Whistleblowing Policy.

2.0 MINIMUM REQUIREMENTS OF THE POLICY

2.1 COMPLIANCE WITH LAWS, RULES, REGULATIONS AND GUIDELINES

It is the policy of NCAP Group to fully comply with laws and regulations issued on anti-money laundering and combatting of terrorist financing. Each entity in NCAP Group is also required to adopt necessary policies and procedures in order to comply with the requirements of the applicable laws and regulations and guidelines issued for the capital market intermediaries.

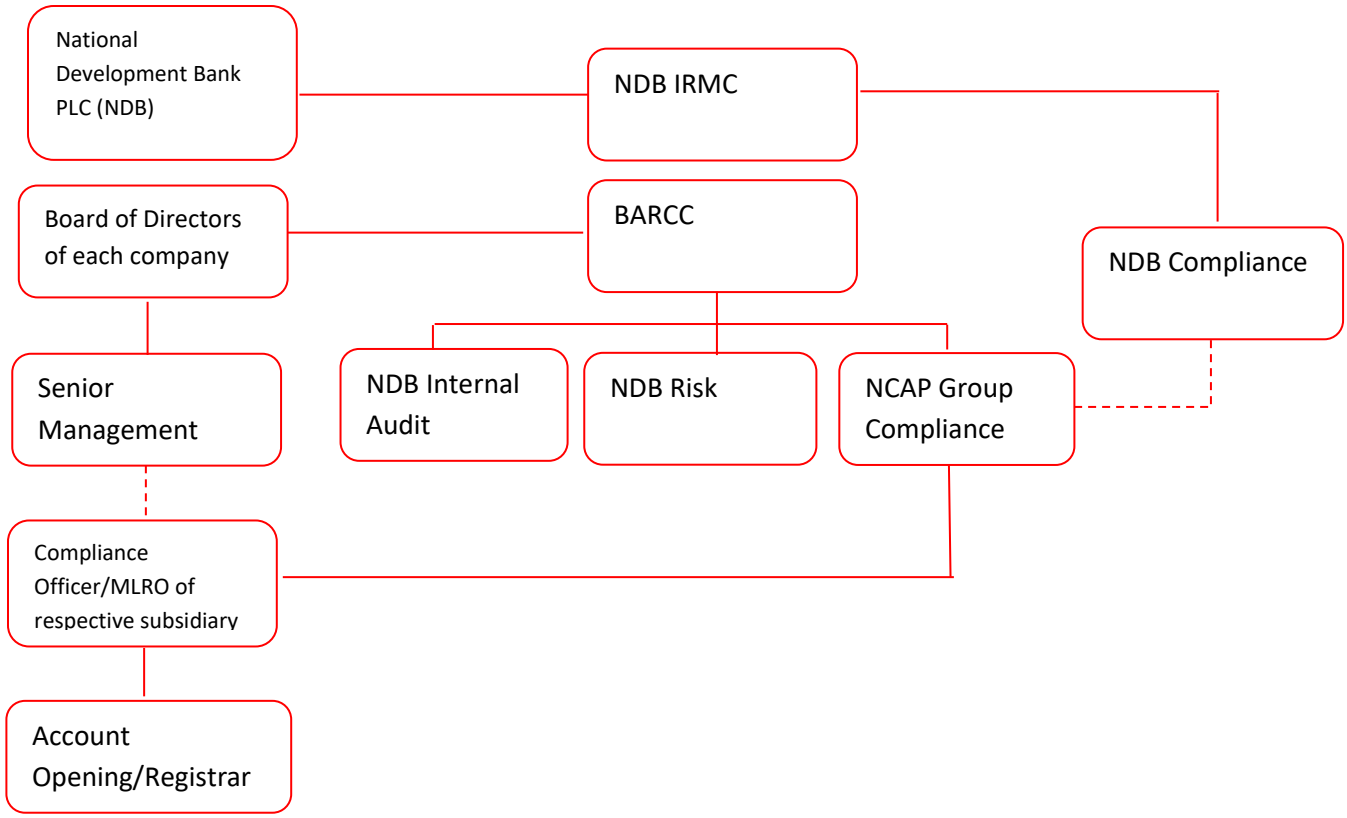
The laws applicable in Sri Lanka are the following:

- Prevention of Money Laundering Act No.5 of 2006 (as amended)
- Financial Transactions Reporting Act No. 6 of 2006
- Convention on the Suppression of Terrorist Financing Act No.25 of 2005 (as amended)
- Mandatory Know Your Customer and Customer Due Diligence Rules for the Securities Industry in terms of Provisions of the Financial Transaction Reporting Act No. 6 of 2006
- Financial Institutions (Customer Due Diligence) Rules, No 1 of 2016 – Extraordinary Gazette No 1951/13- 27th January 2016
- All other regulations, directions and guidelines issued by the Financial Intelligence Unit (FIU) of the Central Bank of Sri Lanka (CBSL)

The foreign subsidiaries of the Group are required to adopt an anti-money laundering compliance program that is also consistent with the requirements of the above regulatory framework to the extent that local laws and regulations permit. Wherever their local regulations are stricter than the requirements set out in this Policy, the subsidiaries may apply the stricter standards.

2.2 ORGANIZATIONAL STRUCTURE

Each entity in the NCAP Group has a proper organizational structure for anti-money laundering/combating financing of terrorism (AML/CFT) compliance and the roles and responsibilities should be clearly defined. The requirements of laws, regulations, Circulars of the regulators and group internal policies and procedures and international standards and best practices should be taken in to account in designing the organizational structure for AML/CFT compliance purposes. The Group AML/CFT organizational structure is as follows;



2.3 APPOINTMENT OF COMPLIANCE OFFICER AND MONEY LAUNDERING REPORTING OFFICER

Each entity with NCAP Group shall appoint a compliance officer who is responsible for ensuring the Company's compliance with the requirements of the AML/CFT laws. The Compliance Officer must be at management level who will be in charge of the application of the AML related internal programs and procedures, including proper maintenance of records and reporting of suspicious transactions. The Group AML/CFT Compliance program is headed by the Head of Compliance of NCAP Group and the Internal Compliance Officer of each entity is responsible for AML/CFT functions within their entity. The Compliance Officers through the Head of Compliance of NCAP Group reports to the Board through Board Audit Risk and Compliance Committee (BARCC).

The Compliance Officers of the Group shall also act as the Money Laundering Reporting Officer (MLRO) for all regulatory and reporting purposes in relation to anti money laundering and combatting of terrorist financing unless otherwise decided by the Board. In the absence of the MLRO, the Company should appoint an Alternate MLRO who should have knowledge and experience in client onboard processes of the Company.

2.4 CLIENT DUE DILIGENCE

The Group must, when establishing a business relationship with a client for business and on an ongoing basis as applicable, apply appropriate Client Due Diligence (CDD) measures on the business relationship, including identifying and verifying the identity of the client. The NCAP Group should ensure that there is consistency between the information it holds on the client and the nature of transactions or proposed transactions. Where there is any indication of abnormal or potential suspicious activity within the context of the product or service being provided, the Group must take additional measures to verify the information obtained.

2.4.1 Ascertaining of Client's Identity

The Group shall preserve correct and complete information of identification of all clients when they enter into a business relationship or when performing a single transaction or a deal. Each company may develop their own processes based on their business and the client relationship on ascertaining Client's identity. No account shall be opened in fictitious/false or anonymous name. Unless the approval has been obtained in accordance with Section 2.4.6 of this Policy, no business relationship should be proceeded without establishing the identity of potential clients.

Where any client is rated as posing a high AML risk, the Group shall take enhanced CDD measures for such client.

2.4.2 Verifying of Client's Identity

The identity of clients should be verified by obtaining documentary evidence in accordance with the guidelines issued by the FIU/regulator and must be verified before or during the course of entering into a business relationship with the client. Provided however, where the risk level of the client is low according to the risk profile of the client and verification is not possible at the point of entering into the business relationship, the Group may, subject to the following conditions conduct a delayed verification of the client;

- Verification shall be completed as soon as it is reasonably practicable but not later than fourteen working days from the date of opening of the account;
- The delay shall be essential so as not to interrupt the Group's normal conduct of business; and
- No suspicion of money laundering or terrorist financing risk shall be involved.

To mitigate the risk of delayed verification, the company shall impose conditions under which the customer may utilize the business relationship prior to verification and such conditions shall be documented in the as part of the SOP of each of the company. Where the identity of a client cannot be established and verified as mentioned above, the Group shall;

- In relation to a new customer, not open the account or enter into the business relationship to perform the transaction; and
- In relation to an existing customer, terminate the business relationship, with such customer and consider making a suspicious transaction report in relation to the customer.

For NDBS, The Colombo Stock Exchange by way of the Trading Participant Rules has suggested a verification procedure whereby the stockbroker may rely on documentary, non-documentary methods or a combination of both to identify and verify the identity of investors[1].

The Group shall periodically review the adequacy of customer information and ensure that the information is kept up to date.

2.4.2.1 Enhanced Customer Due Diligence

Any Group companies onboarding clients posing a high risk shall take enhanced CDD measures for such client in addition to the usual CDD measures mentioned above. The following categories of clients shall be compulsorily subjected to enhanced CDD measures;

- Existing client providing unsatisfactory information relating to CDD;
- Business relationships and transactions with clients and Financial Institutions from high risk countries (as notified by the FIU from time to time);
- Politically exposed persons; and
- Non-Governmental Organization/Not-for-Profit Organization and charities as well as the individuals who are authorized to operate the accounts and members of their governing bodies. All international and national level foreign funded voluntary social services organizations/non-governmental organizations who are not registered with the National Secretariat for Non-Governmental Organizations or with any other institution including the District Secretariat or the

[1] Annexure 3 of the Trading Participant Rules of the Colombo Stock Exchange

Divisional Secretariat and receives direct foreign funds/remittances into their accounts must be monitored and reported to the FIU.

2.4.3 Customer Identification and Verification Process via eKYC/vKYC

Any of the Group companies onboarding clients on a digital platform shall conform to the FIU guidelines on non face to face customer identification using the electronic interface provided by the Department of Registration of Persons (DRP).

This process will be used to onboard Sri Lankans residing in Sri Lanka as well as outside Sri Lanka. The customer must have a NIC issued by DRP to request for account opening through this channel. However, for NDBS, the CSE rules allow for identity verification for foreigners to be established through Passport .

The staff involved in onboarding customers through the eKYC/vKYC process shall identify the customer and verify the identification document using the electronic interface provided by DRP as outlined below,

Verification of the NIC Details and the picture in the NIC provided by the customer will be verified against the records available at DRP and with the details in the original NIC document sighted by the vKYC/eKYC officer during the video conference call.

Verification of the permanent address

If the permanent address entered by the customer is the same as appearing in the NIC it can be used as a verification document for the permanent address.

If the permanent address entered by the customer differs from the address given in the NIC, the customer will be required to provide an address verification document.

The originals of these documents shall be sighted by the vKYC/eKYC officer, verified with the document uploaded by the customer and an image is captured during the video call.

The document submitted by the customer and the image of the original document shall be retained as per NCAP Group's record retention policy.

Identification of customer's location

The geo location of the customer will be used to verify the location from where the customer is requesting the account opening. This will be used to check whether the customer is residing within or outside Sri Lanka and ensure relevant accounts are opened to the customer. Further, if the distance between the customer's location and the given permanent address is significantly high, the vKYC Officer shall clarify reasons for the difference and same is kept on record. If the vKYC Officer identifies that the customer is deliberately providing false information on the actual location the account opening should not be continued, and the request shall be rejected.

vKYC Officers shall be trained to evaluate the behavior and surroundings of the customer during the call to be alert for any possible fraud attempts.

Information provided by the customer shall be verified against the overall profile to understand deviations and inappropriate data.

Anomalies if observed shall be verified to the satisfaction of the company particularly during an enhanced due diligence inquiry.

Identification of the customer

The vKYC Officer shall verify the customer's image provided in the NIC picture against the physical image during the video call. If the customer on the video call differs from the NIC picture, or if the picture in the given NIC differs from the picture in the DRP the customer will be instructed to visit the company to complete the account opening process.

Sanction screening

All customers shall be screened against sanction list/s prior to onboarding to identify any nexus to a sanction and circumstances associated with non-face-to-face customer identification and verification[2] must be considered in order to identify suspicious behavior indicators as morefully described below.

2.4.3 Identification of Ultimate Beneficial Owner

The Group shall ensure that it establishes and verifies the identity of the ultimate beneficial owner who owns or controls the client or its assets or on whose behalf the transaction/s is/are carried out or the business relationship is established (if any). For the purpose of this Policy, the following elements must be considered;

- Natural person (s) who owns or controls more than ten percent (10%) of the shareholding of a legal person.
- Natural person (s) who has "effective control"[3] of the legal person;
- Natural person on behalf of whom the transaction is being conducted

For clients which are listed in a stock exchange, relevant identification information available from reliable sources may be used to identify Directors and major Shareholders No beneficial owner or related account shall be opened in fictitious/false or anonymous name. Once the beneficial owner is identified, at least

[2] Part V of the revised Guideline for Non Face-to-Face Customer Identification and Verification issued by the FIU on 30th December 2020

[3] "Effective Control" as described in Guideline No. 04/2018 issued by the FIU on Identification of Beneficial Ownership for Financial Institutions.

the following information in relation to each individual beneficial owner must be obtained via the Declaration for Ultimate Beneficial Ownership form as applicable for each of the Companies;

- Full name and permanent/residential address;
- Official person identification or any other identification number (eg: NIC/Passport); and
- PEP status

Information on beneficial owners must be reviewed periodically to ensure information is up to date. Delayed verification of the identity of beneficial owners is allowed when;

- Risk level of the customer is low and verification is not possible at the point of entering into the business relationship;
- There is no suspicion of money laundering or terrorist financing risk involved; and
- Delay will not interrupt the normal conduct of business.

2.4.4 Guidelines on Identification of Politically Exposed Persons (PEPs)

PEPs can be identified under the following categories;

1. Domestic PEPs: individuals who are entrusted with prominent public functions in Sri Lanka.
2. Foreign PEPs: individuals who are entrusted with prominent public functions by a foreign country.
3. International organization PEPs: persons who are entrusted with a prominent function by an international organization.
4. Immediate Family members[4]: individuals who are related to a PEP either directly (on grounds of consanguinity) or through marriage or similar (civil) forms of partnership.
5. Close associates[5]: individuals who are closely connected to PEP, either socially or professionally.

A PEP includes a head of a state or a government, a politician, a senior government officer, judicial officer or military officer, a senior executive of a state owned corporation/government or autonomous body but does not include middle ranking or junior ranking individuals.

Following details shall be looked at in relation to PEPs for clearance prior to senior management approval for entering into a new business relationship/continuing an existing relationship. This is applicable for all new and ongoing business relationships with clients.

a) The basis of the client being classified as a PEP - Relationship with the PEP, full name and the details of the prominent public function of the PEP If the customer is a family member or a close associate of the a PEP etc

[4] Immediate family members and close associates of PEPs and International Organizations as morefully described in Guidelines on Identification of Politically Exposed Persons, No. 03 of 2019 issued by the FIU on 01st October 2019
[5] ibid

b) Source of funds

c)Expected volume of transactions

d)Expected type/nature/purpose of transactions

e)Brief profile of the customer/entity

f)Tenure of holding the PEP designation

g)Date of incorporation if the customer is an entity

i)Is any other close associates or Immediate family Members of this PEP has been already on board with the Company. If yes their details to be provided.

A non-exhaustive list of PEPs and the time limits applicable for PEP after leaving office is provided in Annexure 1.

There is no single method of identifying PEPs but where a self-declaration is obtained from a client regarding their PEP status as part of the Customer Due Diligence process, the entity should ensure that they do not rely solely on such self-declaration as clients may not be able to determine their PEP status. The entity is advised to actively engage with clients to determine their PEP status and screen clients using commercial databases complied for this purposes, eg: WorldCheck. Additionally, the group may share information amongst themselves on PEPs for Anti Money Laundering and Countering the Financing of Terrorism (AML/CFT) purposes, provided there are adequate safeguards on the confidentiality and use of information exchanged.

The existing PEP database of the entity shall be subject to periodic review.

Guidelines for Financial Institutions on Suspicious Transaction Reporting and Enhancing quality of STR reporting. This guideline aims at assisting employees of the Group companies in improving the quality of STR submissions, the following areas are identified.

a) Prerequisites for detecting and reporting suspicious transactions
b) Avoid defensive reporting

c) Reporting Suspicious Transaction Reports via system
d) Timing of forming and reporting suspicion
e) Content of reporting
f) Maintaining the confidentiality of the supporting documents
g) Failure to report STRs
h) Attending to further information request
i) Obligation for the company in relation to the STRs submitted

2.4.5 Implementation of AML/CFT measures on parties involved with online payment platforms

The companies should pay an enhanced emphasis on the following in relation to the parties involved in facilitating transactions through online payment platforms,

a) Identification and verification of customers
b) Conduct ongoing due diligence on customers and scrutiny of transactions
c) Identification and reporting of Suspicious Transactions
d) Wire transfer requirements (in particular, originating financial institution shall make originator information available to the beneficiary financial institution)
e) Targeted financial sanctions screening
f) Record keeping
g) Other reporting requirements

2.4.6 Assessing risks of legal structures in Sri Lanka

The complexity of structures of legal entities [both legal persons and arrangements], ownership and the country of incorporation makes such organizations vulnerable and can be abused for Money Laundering, Terrorist financing and other criminal activities.

The NCAP Group uses, robust systems, policies, procedures such as Customer/Transaction Due Diligence measures, sanction screening; periodic customer reviews and transaction monitoring measures to enable accurate identification of individuals/ entities, ultimate beneficial owners of entities, legal structures being abused for unlawful activities.

The staff involved in onboarding clients and in operations of customer accounts shall be vigilant of the typologies associated with legal entities.

Typologies to be vigilant about;

a) Multi-jurisdiction splitting -
b) Foreign ownership/control by shell entities–
c) Anomalous complex ownership/control structures –
d) Control through power of attorney
e) Use of trusts or foundations in ownership/control structures -
f) Use of nominee directors/nominee shareholders/"front men"
g) Use of legal persons as company directors
h) Use of bearer shares
i) Use of private investment funds/hedge funds

j) Use of International business corporation / exempt companies
k) Use of fictitious entities
l) Abuse of professional privilege
m) Use of large professional firms
n) Use of fake IDs for formation/registration
o) Use of deceptive names of legal structures

2.4.7Establishment of Purpose of Business Relationship

If the Group enters into a business relationship, it should obtain information to determine the purpose if this is not clear from the business relationship itself.

2.4.8 Establishment of Source of Funds and Wealth

It is a pre-requisite for the Group to understand the origin or source of funds or property underlying a business relationship with a client. Therefore understanding the client's source of funds/property and as appropriate, the client's source of wealth is an important aspect of the Group's client due diligence process.

2.4.9 Timing

The Company must take all reasonable measures to complete all CDD measures for all clients prior to the establishment of a new client relationship and prior to providing any financial service. Where it is necessary to provide financial services to a client prior to completion of CDD measures, adequate measures (such as amending client agreements / mandates etc) should be put in place to cover the liability of the company to terminate a business relationship if AML clearance cannot be granted.

Where the client's identity is yet to be verified, the Group needs to adopt risk management procedures with respect to the conditions under which a client may utilise the account or investment prior to verification. These procedures should include a set of measures such as a limitation of the number, types and/or amount of transactions that can be performed, and the monitoring of large transactions being carried out of expected norms for that type of relationship. Where it is not possible after reasonable efforts to verify the identity of a client, the Group should consider halting transactions or terminating its relationship and also should consider making a Suspicious Activity Report to the appropriate authorities in relation to the client. It may be appropriate for the Group to consult with its regulators and appropriate law enforcement agencies prior to halting transactions in a particular account or terminating its relationship with any client.

2.5 RISK PROFILING

The Group should assess the risk level of its clients and the level of risk exposure considering the clients background (resident/non-resident, occasional/one-off, legal persons, politically exposed persons etc), country of origin of the client/geographical location of the business and products/services/transactions/delivery channels (cash-based/face-to-face/non face to face/cross border) of the client. The guide provided by the FIU on categories of customers posing a high risk of Money Laundering (ML) or Terrorist Financing (TF), products/services more attractive for ML/TF, countries with high risk of ML/TF and risk involved with business delivery methods[6] may be used by the Group to develop its own risk assessment. Risk assessment and findings shall be documented and the risk assessment must be kept up to date through periodic review including as and when required by the FIU. Based on the basis of risk, it should further conduct due diligence of clients and transactions as necessary from time to time. Potential risks of a business relationship would, interalia, include criminal risk of money laundering, reputational risk, legal risk, fiduciary risk, regulatory risk and operational risk. Based on the risk based approach, the Company should determine whether the client's profile is a high risk profile or a low risk profile and apply appropriate enhanced or reduced due diligence measures accordingly. A client's risk profile based on his level of money laundering and terrorist financing risk shall be reviewed and updated regularly. High risks countries list circulated by the FIU should be considered in the review of risk profiles of clients.

2.6 SUSPICIOUS TRANSACTION MONITORING

The Group shall have processes to monitor the client accounts and transactions in order to detect unusual or suspicious transactions. All companies must develop its own operating definition for a suspicion which must pass the test of reasonableness taking into consideration the size of the company, nature of business, identified risks of the company and indicators/red flags.

Guidelines for Financial Institutions on Suspicious Transaction Reporting and Enhancing quality of STR reporting to be followed. This guideline aims at assisting employees of the Group companies in improving the quality of STR submissions, the following areas are identified.

a) Prerequisites for detecting and reporting suspicious transactions
b) Avoid defensive reporting
c) Reporting Suspicious Transaction Reports via system
d) Timing of forming and reporting suspicion

[6] Guidelines on Money Laundering & Terrorist Financing Risk Management for Financial Institutions issued by the FIU dated 11th January 2018.

e) Content of reporting
f) Submission of supporting documents confidentiality
g) Failure to report STRs
h) Attending to further information request
i) Obligation for the company in relation to the STR s submitted

2.7 REPORTING OF SUSPICIOUS TRANSACTIONS

NCAP Group shall report all suspicious transactions as required by applicable laws and the Financial Intelligence Unit (FIU) guidelines which at present is no later than two working days of formation of suspicion i.e. the suspicion itself must be reported even if the company's processes have not been completed. If after sending the report, the company discovers additional facts and circumstances to either support or refute the initial suspicion, the FIU must be informed appropriately. There shall be a reporting process internally to report all suspicious transactions to the FIU by way of a Suspicious Activity Report and Suspicious Transaction Report submitted to the GoAML system as applicable from time to time and all such reports shall be complete and accurate. All suspicious events must be informed to the Compliance Officer/MLRO of the said Entity. Continuing business relationships with clients about whom STRs have been reported or suspicion has been formed, is not prohibited and all entities are advised to ensure that their behaviour towards the client does not amount to tipping off the client.

After the submission of an initial STR, the entity should continue to comply with all applicable laws, rules and regulations in all future dealings with the client, which may include a requirement to submit additional STRs/information on further suspicions identified/further developments. It is also the policy of NCAP Group to provide information required by the regulators from time to time in a timely manner.

2.7.1 REPORTING OF THRESHOLD REPORTS

All reportable threshold transactions should be reported to the goAML Live Environment within the given timeline as determined by the FIU from time to time. In respect of NDBS, threshold reporting consists of Cash Transactions (CTR), Electronic Fund Transfers (EFT) and International Fund Transfers (IFT) exceeding Rs. 1,000,000 or its equivalent in any foreign currency which shall be reported within 30 calendar days from the date of the transaction. The Group shall ensure that all systems and processes are in line with the guidelines and reporting formats issued by the FIU from time to time relating to EFTs, IFTs and CTRs as applicable.

2.8 NON-DISCLOSURE POLICY

NCAP Group shall not disclose any information related to suspicious transactions reports submitted to the FIU to any client or any person/institution in any manner unless it is required by law.

2.9 INTERNAL ANTI-MONEY LAUNDERING CONTROLS

NCAP Group together with the Compliance Officer of each entity must ensure adequate client-business related controls are in place in order to comply with all applicable AML requirements including identifying and developing red flag indicators for each entity to identify suspicious behaviors and transactions of clients A non-exhaustive and unofficial list of suspicious indicators for transactions and behaviours, including sector specific red flag indicators have been provided by the FIU as guidance[7]. Each entity shall modify and supplement this list as applicable. A non-exhaustive list of red flag indicators for PEPs have also been provided by the FIU[8] which shall compliment those developed by each entity to detect suspicious behaviours and transactions.

2.10 PREVENTION AND SUPPRESSION OF TERRORISM AND TERRORIST FINANCING OBLIGATIONS

NCAP Group shall not establish a relationship with shell companies or any entity, individual or beneficiary designated by the UN Sanction Committee or proscribed and scheduled by the Government of Sri Lanka or any other applicable jurisdiction.

NCAP Group shall adhere to all applicable embargo requirements issued by the UN Security Council, the government of Sri Lanka or any other relevant jurisdiction or regulatory or authorized authority. The Compliance Officer shall ensure that the employees are kept informed of new requirements and updated sanction lists issued by such authorities.

NDBS in particular, shall scan all clients against the list of designated individuals and entities approved by the UN Security Council Committee as well as those designated by the Government of Sri Lanka;

- At the time of onboarding; and
- Periodically, as and when amendments to the list are received from the FIU.

In the event there is a match of any of the clients with the particulars of designated individuals/entities, NDBS shall prevent such persons from conducting any transactions and freeze funds on the instructions

[7] Appendix I of Guidelines for Financial Institutions on Suspicious Transaction Reporting No. 06 of 2018 issued by the FIU on 6th August 2018

[8] Guidelines on Identification of Politically Exposed Persons, No. 03 of 2019 issued by the FIU on 01st October 2019

of the FIU, financial assets or economic resources without delay and inform the FIU not later than 24 hours of the full particulars of the funds, financial assets or economic resources held by such client with NDBS.

2.11 SCREENING OF EMPLOYEES

NCAP Group should ensure that the employees are screened before recruiting and should complete background checking of the prospective employees.

2.12 RECORD KEEPING

Records should be retained of all transaction information and records created or obtained for the purpose of client identification, as well as of all documents related to suspicious transactions reports, documentation of AML account monitoring for a minimum period of 6 years after closing of the account and/or after the completion of the transaction. The Group's Record Management Policy should be consistent with the record keeping requirements under AML laws and regulations.

2.13 AML COMPLIANCE PROGRAM

The Group should have a compliance program for anti-money laundering compliance to ensure that all laws and regulations are adhered to, that business is conducted in conformity with high ethical standards and that services are not provided where there is a good reason to suppose that transactions are associated with money laundering or terrorist financing activities.

2.14 STAFF TRAINING AND AWARENESS

In order to facilitate recognition, handling of suspicious transaction reports and to ensure the compliance with AML policies, each entity within NCAP Group must make arrangements for on-going training of all employees. All employees including trainees and temporary personnel who are responsible for carrying out transactions, dealing with clients, initiating and establishing business relationships should be covered under AML training and awareness.

It is important that staff understand the institution's inherent ML/TF risks and the nature of the measures that have been developed to mitigate these risks. Training must be provided for all staff upon joining the institution and should be an-ongoing activity. Apart from general training provided to all staff, targeted training programs should be developed for specific categories of staff in light of the nature of their work in the context of ML/FT risks. AML/CFT awareness raising programs should also be conducted for members of the BoD.

2.15 AML AUDIT

The NCAP Group should conduct periodic testing of its program to assess compliance with and the effectiveness of the AML Policy and program and to assure that the Program is functioning as designed.

3. ROLES AND RESPONSIBILITIES

3.1 BOARD/BOARD AUDIT RISK AND COMPLIANCE COMMITTEE (BARCC)

The Board of Directors and the BARCC must take such decisions as required to ensure that it is fully complying with laws and regulations regarding compliance with AML/CFT regime. The Board of Directors are committed to creating a positive compliance culture in the companies by creating a tone from the top of the organization. Additionally, the Head of Compliance NDB Capital Holdings Limited directly liaises with the NDB Bank Compliance and Risk departments.

3.2 SENIOR MANAGEMENT

The senior management including the Chief Executive Officer and other senior managers;

- should be committed to the development and enforcement of this Policy;
- should take necessary measures to assess and identify money laundering and terrorists financing risk and should have in place an appropriate mechanism to mitigate those risk;
- should issue policy guidance with the involvement of the Compliance officers of the Group to the staff to be cautious for preventing money laundering and terrorists financing when necessary

3.3 COMPLIANCE OFFICER/MLRO

The Compliance Officer among other things, shall:

- assess the various types of ML/TF risk e.g. product risk, service risk, customer risk, country risk and establish necessary measures for mitigating those risks;
- review the AML/CFT policies regularly considering the risk based approach;
- update the legal, regulatory, business or operational changes including AML/CFT rules or regulations as and when required;
- implement the necessary AML/CFT policies, procedures and controls so as to deter criminals from adopting various techniques of ML/TF using the business services;
- supervise the implementation of necessary measures for preventing ML/TF risk and assess the effectiveness of applied measures;

- arrange necessary training for the staff;
- ensure necessary steps are taken to identify suspicious transactions and report the same to the FIU directly;
- report to the Board of Directors/Head of Compliance and BARRC and Integrated Risk Management Committee of NDB (IRMC) on a quarterly basis regarding the status of the AML/CFT initiatives undertaken by the Group;
- assist the NCAP Group Compliance Officer on compliance initiatives and implementation as and when necessary;
- keep the NCAP Head of Compliance informed of any risks observed or any suspicious transactions
- extend all sorts of cooperation to NCAP Group Compliance, NDB Internal Audit Team, NDB Risk Team, FIU Inspection Team and other law enforcing agencies as and when required and appropriate;
- consider any negative information from any sources, regarding the clients, as a matter of suspicion and take appropriate actions to verify such information;
- Coordinate with NCAP Group Compliance and arrange training for the staff;

3.4 ACCOUNT OPENING OFFICERS/ REGISTRAR

The Account Opening Officer/s shall

- Perform due diligence and enhanced due diligence as applicable on prospective clients prior to opening an account;
- Ensure all client data is complete and accurate to the extent practicable at all times;
- Be vigilant regarding the identification of account holder and the suspicious behavior of a prospective client while opening an account;
- Ensure all required documentation is completed satisfactorily as per Guidelines issued by the FIU and other regulatory bodies as applicable;
- Follow the policy of identification procedure KYC and analyze the track record of the existing accounts;
- Ensure that customer information is verified and undertake reviewing of client information after a certain period;
- Perform PEP and UBO testing accurately as per Guidelines issued by the FIU;

- Communicate practical difficulties involved in onboarding clients and carrying out AML checks to the Compliance department and the Senior Management in establishing procedures and in policy making.

3.5 NCAP GROUP COMPLIANCE OFFICER

The NCAP Group Compliance Officer shall

- Introduce policies and procedures developed together with relevant department heads relating to money laundering laws and regulations and ensure Group compliance
- Monitor and assess the level of risk of money laundering and the financing of terrorism across all of the business transactions within the NCAP Group
- Monitor reporting for compliance with laws, regulations and develop a compliance program
- provide guidance to the business units and MLRO of each entity to assist them to comply with the laws and regulations
- investigate violations and enforce compliance with the AML regulations
- Inform the NCAP BARCC, Boards and also through NDB Compliance the IRMC in a timely fashion of any and all significant matters relating to the Policy
- Monitor implementation of the Policy

4. COMPLIANCE REPORTING

The Group should provide to the Board, BARCC and NDB IRMC periodic reports of the status of compliance with this Policy.

5. PROCEDURE MANUAL

All the procedures relating to prevention of money laundering and terrorist financing s of each of the respective Group companies. The entities of NCAP Group may have separate Procedure Document specifying their respective regulatory requirements. The employees should be familiar with the procedures set out in the Procedure Document. Further guidance is provided in the Guidance Notes and Frequently Asked Questions.

6. POLICY REVIEW

This Policy should be reviewed in every two years or as and when required.

Annexure 1

ANNEX - A NON-EXHAUSTIVE LIST CATEGORIES OF CUSTOMERS THAT CAN BE CONSIDERED AS PEPS

DOMESTIC PEPS

		PEP Category - Politicians	Time limits for PEP status after leaving office [No. of years]
A.	1	The President	Always
	2	The Prime Minister and all former Prime Ministers	
	3	The Speaker and the Deputy Speaker of the Parliament	Ten or more
	4	Cabinet Ministers, Non-Cabinet Ministers, State Ministers, Deputy Ministers	
	5	Members of Parliament	
	6	Leaders of Political Parties -	
B.	7	Governors of Provinces	Ten or more
	8	Chief Ministers of Provinces	
	9	Mayor, Chairman of Municipal Councils	
	10	Chairman of Provincial Councils	
	11	Members of Municipal Councils/ Provincial Councils / Local Government Bodies	
	12	Office Brearers of political Parties Commissioners/ Secretaries to Municipal Councils/ Provincial Councils / Local Government Bodies/Leaders and Treasurer	
C.	13	Chief Justice	Ten or more
	14	Attorney General	
	15	Judges of Supreme Court	
	16	Judges of the Court of Appeal	
	17	Solicitor General of the Attorney General's Department & additional Solicitor General	
	18	Judges of High Courts/Provincial High Courts	
	19	Judges of District Courts	
	20	Judges of Magistrate Courts	
	21	Registrar of Supreme Court-	
	22	Registrar of the Court of Appeal	
	23	Registrars of Judges of High Courts/Provincial High Courts	

	24	Registrars of District Courts	
	25	Registrars of Magistrate Courts	

D.	26	Ambassadors /High Commissioners	Five or More Years
	27	Consul-General/ Deputy Head of Mission/Charge d'affaires/Honorary Consul	
	28	Ministers plenipotentiary and Envoys Extraordinary	
	29	Representatives of UN agencies and Heads of other international organizations	

E.	30	Secretary/ Senior Additional Secretaries/ Additional Secretaries to the President	Five or More Years
	31	Secretary/ Senior Additional Secretaries/ Additional Secretaries to the Prime Minister	
	32	Secretary /Senior Additional Secretaries/ Additional Secretaries to the Cabinet of Ministers, Non-Cabinet Ministers, State Ministers, Deputy Ministers	
	33	Deputy Secretary to the Treasury	
	34	Secretary/ Senior Additional Secretaries /Additional Secretaries/ Deputy Secretaries to Ministries	
	35	Members of the Monetary Board	Five or More Years
	36	Governor / Deputy Governors / Assistant Governors and Heads and Additional Heads of Department of the Central Bank of Sri Lanka	
	37	Advisors to the President/ Prime Minister / Ministers/ Ministries	
	38	Chief of staff of presidential secretariat	
	39	Auditor General, Additional Auditor General & Assistant Auditor General	
	40	Secretary General of Parliament	
	41	District Secretaries/ Government Agent and Secretaries	
	42	Heads and Senior Officials of Government Departments	Five or More Years

		*Government Departments-Director /Commissioner and Above *Corporations-General Manager and Above *Ministries-Additional Secretry and Above *State Own Enterprises –Head and Deputy Head Of the entity *Statutory Board-Head and Deputy Head Of the Entity *Government Apointed Commissions-Chairman,Members and Senior Officers *Diplomatic Represantatives Of the government Serving in Foreign Countries	
	43	Chairmen and Senior Officials of State Enterprises	Five or More Years
	44	Chairmen and Senior Officials of State Corporations / Statutory Boards/ Authorities/ Public Corporations	
F	45	Field Marshall / Admiral of the Fleet/ Marshal of the Air Force	Ten or More Years
	46	Chief of Defence Staff	
	47	General of Sri Lanka Army/Admiral of Sri Lanka Navy/ Air Chief Marshal of Sri Lanka Air Force	
	48	Officers in the Rank of Lieutenant Colonel and above of Sri Lanka Army	
	49	Officers in the Rank of Commander and above of Sri Lanka Navy	
	50	Officers in the Rank of Wing Commander and above of Sri Lanka Air Force	
	51	Inspector General of Police	
	52	Police officers above the rank of Asst. Superintendent of Police	
G.	53	Chairman/ members and senior officers of the Public Service Commission	Five or More Years
	54	Chairman/ members and senior officers of the National Police Commission	
	55	Chairman/ members and senior officers of the Human Right Commission	

	56	Chairman/ members and senior officers of the Commission to Investigation Allegations of Bribery or Corruption	
	57	Chairman/ members and senior officers of the Finance Commission	
	58	Chairman/ members and senior officers of the Election Commission	
	59	Members of Constitutional Council	
	60	Chairman/ members and senior officers of the Audi Service Commission	
	61	Chairman/ members and senior officers of the Delimitation Commission	
	62	Chairman/ members and senior officers of the National Procurement Commission	
	63	Members of Cabinet appointed committees	
H.	64	Chairman, Members and senior officers of University Grant Commission	Five or More Years
	65	Chairman, members of University Councils	
	66	Chancellor	
	67	Vice Chancellor	
	68	Registrar of universities	

I	69	A private company where a PEP LISTED in this Annexure (Annexure1) is a Director or a significant shareholder (Exceeding 10%)	Two more years
	70	Other Business concerns (propriertorships, partnerships) in which a PEP LISTED IN Annex A, has a material Interest/Control	
	71	Any Other Person whom the compliance officer together with the Senior management decides as PEP base on information available in public domain- Continuation of the PEP status is decided by the company at the periodic reviews of the customer	
	72	Any other person Compliace Department decides based on the information available in the public domain or based on the name screening process carried out- Continuation of the PEP status is decied by the company at the periodic reviews of the customer	

FOREIGN PEPS

	73	Officials of international organizations who hold or have held, in the course of the last 5 years, management positions in such organizations (directors, heads of the boards or their deputies)
	75	Officials of international organization who perform or performed any other management functions on the highest level, particularly in international and intergovernmental organizations,
	76	Members of international parliamentary assemblies
	77	Judges and management officials of international courts-