BACKERS & PARTNERS (PVT) LIMITED

TREC Holder of "Pakistan Stock Exchange Limited"

ANTI-MONEY LAUNDERING/ COUNTERING FINANCING OF TERRORISM (AML/CFT) POLICIES, PROCEDURES AND CONTROLS

POLICY CONTENT

SR. NO	DESCRIPTION	PAGE NO.
01	Introduction of Entity	03
02	Introduction to Policy	03
03	Scope and Objective	03
04	AML Compliance Officer Designation and Duties	05
05	Communication of AML/CFT Policy and procedures	05
06	Policies, Procedures and controls	05
07	Risk Assessment Classification and Management	07
08	General	14
09	Compliance Check	14
10	Internal Audit Process	15
11	Risk Classification and Management	15
12	Supervisory Procedures for Opening of Accounts	19
13	Monitoring Accounts For Suspicious Activity	20
14	Red Flags	20
15	Responding to Red Flags and Suspicious Activity	22
15	Suspicious Transactions Reporting	22
17	Independent audit of AML/CFT Compliance Program	24
18	Controls Measures And Controls Put In Place	25
19	Training Programs	27
20	Monitoring Employees, Employee Conduct, and Trading Accounts	28
21	Confidential Reporting of AML Non-Compliance	28
22	Future Amendments	28
23	Overriding effect	28
24	Approval from Board of Directors	28
25	Effective Date	28

1. Introduction of Entity

Backers & Partners (Pvt.) Ltd. is one of the brokerage companies at Pakistan Stock Exchange. The company is the TREC holder of PSX and was established in year 2014 under the name A.N. Equities (Pvt.) Limited, the name was later changed to Backers & Partners (Pvt.) Ltd. in year 2016.

The company provides its customers access to all the markets traded at PSX that include Ready, Futures and MTS. Further B&P is also eligible to provide Margin Financing as a financier through NCCPL. The registered office of the company is located in Gulberg, Lahore. It has two branches one at Main Canal Bank Road, Johar Town, Lahore and the other in Gujranwala.

2. Introduction to the Policy

2.1 This policy has been developed to ensure compliance with Anti-Money Laundering laws to ensure prohibition and actively preventing activities that may facilitate money laundering and the funding of terrorist or criminal activities.

2.2 Generally, money laundering occurs in three stages. Cash first enters the financial system at the "placement" stage, where the cash generated from criminal activities is converted into monetary instruments, such as money orders or traveler's cheques, or deposited into accounts at financial institutions. At the "layering" stage, the funds are transferred or moved into other accounts or other financial institutions to further separate the money from its criminal origin. At the "integration" stage, the funds are reintroduced into the economy and used to purchase legitimate assets or to fund other criminal activities or legitimate businesses.

2.3 Terrorist financing may not involve the proceeds of criminal conduct, but rather an attempt to conceal the origin or intended use of the funds, which will be used later for criminal purposes.

3. Scope and Objective

3.1 An effective Anti-Money Laundering and Countering the Financing of Terrorism (“ ML/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;

GOVERNING LAWS, RULES AND REGULATIONS

- Anti-Money Laundering Act, 2010;
- Anti-Money Laundering Rules, 2008, made under the Anti-Money Laundering Ordinance, 2007 (" ML Ordinance");
- Securities and Exchange Commission of Pakistan (Anti Money Laundering and Countering Financing of Terrorism) Regulations, 2018 ("SECP ML/CFT Regulations");
- Guidelines on SECP AML/CFT Regulations issued by SECP in September 2018; and
- The Companies Act, 2017.
- Pakistan National Risk Assessment 2019 (NRA 2019)

GUIDELINES ON SECP AML/CFT REGULATIONS

3.2 The Guidelines are applicable to all Regulated Persons ("RPs") including Securities Brokers as defined under the SECP AML/CFT Regulations conducting relevant financial business and designed to assist RPs in complying with the Regulations. It supplements the Regulations and the AML/CFT regime by clarifying and explaining the general requirements of the legislation to help RPs in applying national AML/CFT measures, developing an effective AML/CFT risk assessment and compliance framework suitable to their business, and in particular, in detecting and reporting suspicious activities.

POLICY, PROCEDURES AND CONTROLS

3.3 As required under clause 4 (a) of the SECP AML/CFT Regulations, BNP is required to:

- develop and implement policies, procedures and controls with the approval of its Board of Directors for enabling the Company to effectively manage and mitigate the risk that are identified in the risk assessment of ML/TF or notified to it by the Commission;
- monitor the implementation of those policies, procedures and controls and enhance them, if necessary;
- perform enhanced measures where higher risks are identified, to effectively manage and mitigate those higher risks; and
- have an independent audit function to test the system.

3.4 The Policies, Procedures and Controls should contain a clear description for employees of their obligations and instructions as well as guidance on how to keep the activity of the reporting entity in compliance with the Regulations. There should be internal

procedures for detecting, monitoring and reporting suspicious transactions.

4. AML Compliance Officer Designation and Duties

4.1 The Company has designated Head of Compliance as its AML/CFT program Compliance Officer, who shall report directly, and periodically to the Board of Directors ("Board") or to another equivalent executive position or committee of the Company.

4.2 AML/CFT Compliance Officer shall primarily be responsible for the areas including, but not limited to:

- ensure effective compliance with all governing laws and regulations;

- ensure that the internal policies, procedures and controls for prevention of ML/TF are approved by the board of directors and are effectively implemented;
- monitoring, reviewing and updating AML/CFT policies and procedures;
- providing assistance in compliance to other departments and branches of the regulated person;
- timely submission of accurate data/ returns as required under the applicable laws; monitoring and timely reporting of Suspicious and Currency Transactions to FMU; overseeing communication and training for employees
- regular audit of the AML/CFT program; and
- Responding to requests for information by the SECP/FMU/Law enforcement agencies.
- The AML Compliance Officer will also ensure that proper AML records are maintained by the Company.
- The AML Compliance Officer will also ensure that proper AML/CFT Risk Assessment is made in the light of NRA 2019.

4.3 The Compliance Officer will submit Cash Transaction Report (CTR) if any; and / or Suspicious Transaction Report (STR) to Financial Monitoring Unit (FMU) in the manner as prescribed in relevant rules and regulations or respond to request about accounts or transactions made by the relevant authorities in respect of identity of the specified individual or organization, the account number, all identifying information provided by the account holder when the account was established, and the date and type of transaction.

5. Communication of the AML/CFT Policy and Procedures to the Employees

5.1 This AML/CFT Policy & Procedures will be disseminated to all the employees of the Company including branches and liaison offices for necessary understanding and compliance.

6. Policies, Procedures and Controls

6.1 BNP has already in place following three (3) lines of Defense to combat ML/TF for establishing business relationship by the new clients:

- Front Office (Customer-Facing ativity)
- Approval of Compliance Department
- Internal audit process

FRONT OFFICE (CUSTOMER-FACING ACTIVITY)

6.2 Front Office / Dealers / Sale Persons shall be required to know and carry-out the AML/CFT due diligence related procedures when a customer opens an account with the BNP which include the following:

i. KYC/CDD Forms (Annexure - A) shall be completed by the Front Officer representative based on the information gathered from the new client and necessary supporting documents prescribed in KYC/CDD Form shall be obtained;

ii It will be ensured that all documents, as given **Annexure - B,** have been collected before opening of account.

iii. AML checklist shall be completed by Front Office Foreign desk representative, based on information gathered from new International broker dealer /Foreign Institution.

iv. Initial deposit amount shall be accepted in the form of cross cheque/pay-order/demand draft or through any other banking channel after ensuring that such banking instrument has been drawn from the clients' own bank account.

v. Front Office shall maintain a copy of the instrument used for initial deposit in its record.

vi. Front Office staff shall forward the Account Opening Form along with KYC/CDD form to Account Maintenance Division of the Company where KYC/CDD details shall be entered into the back-office of the Company.

vii. Afterward, such complete set of AOF shall be forwarded to Compliance Department for their approval.

Beneficial Ownership of Legal Persons and Legal Arrangements:

6.3 BNP shall identify and verify the identity of the customer, and understand the nature of its business, and its ownership and control structure.

6.4 The purpose of the requirements set out regarding the identification and verification of the applicant and the beneficial owner is twofold:

- 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
- second, to take appropriate steps to mitigate the risks.

6.5 For any reason to believe that an applicant has been refused facilities by another Securities Broker due to concerns over illicit activities of the customer, it should consider classifying that applicant:
- as higher-risk and apply enhanced due diligence procedures to the customer and the relationship;
- filing an STR; and/or
- not accepting the customer in accordance with its own risk assessments and procedures.

6.6 BNP shall accept copies of the documents for identifying a Customer verified by seeing originals during establishing business relationship.

Identification of Customers that are not physically present

6.7 Verification of customer identity with non-documentary evidence is mandatory in the following situations:
- When the customer is unable to present an unexpired/valid identification card with a photograph or other biometric safeguard; or
- When the documents the customer presents for identification verification are unfamiliar to the Company; or
- When the customer and the Company do not have face-to-face contact; and
- When other circumstances increase the risk that the Company will be unable to verify the identity of the customer through documentary means.

6.8 Under the above circumstances, the Company will use the following non-documentary methods of verifying identity:
- Contact the customer after the account has been opened (although the Company cannot rely solely on customer contact as a means for verification);
- Obtain financial statements from the customer (in case of a corporate customers);
- Compare information obtained from customer with information available from a trusted third-party source (such as a credit report or an existing client or broker);
- Check references with other financial institutions i.e. bank statements or verification; and
- Any other non-documentary means deemed appropriate in the situation.

7. Risk Assessment Classification and Management

The BNP shall conduct the Risk Assessment as under;

7.1 Methodology of conducting Risk assessment

Risk assessment is about finding out what are the risks, where they are and matters most and how to mitigate the risks identified to an acceptable level for business to go on. It is a rather

intensive process. Not only must the assessor find out all the systems, processes and people that are involved, he must also know what are the threats and vulnerabilities that are relevant.

The methodology for this NRA refers to the following concepts as defined by the 2013 FATF Guidance on NRA:

- A threat is a person or group of people, object or activity with the potential to cause harm to, for example, the state, society, the economy, etc. In the ML/TF context this includes criminals, terrorist groups and their facilitators, their funds, as well as past, present and future ML or TF activities.
- Vulnerabilities comprise those things that can be exploited by the threat or that may support or facilitate its activities. In the ML/TF risk assessment context, looking at vulnerabilities as distinct from threat means focusing on, for example, the factors that represent [weaknesses in AML/CFT systems or controls or certain features of a country. They may also include] the features of a particular sector, a financial product or type of service that make them attractive for ML or TF purposes. Note: this revised NRA focuses on inherent vulnerabilities, so we have put the reference to weaknesses in AML/CFT in brackets.
- Inherent risk: refers to ML/TF risk prior to the application of AML/CFT controls.
- Consequence refers to the impact or harm that ML or TF may cause and includes the effect of the underlying criminal and terrorist activity on financial systems and institutions, as well as the economy and society more generally.
- Likelihood of ML/TF: the likelihood of ML/TF threat actors exploiting inherent vulnerabilities.

The process of ML/TF risk assessment has four stages:

1) Identifying the area of the business operations susceptible to ML/TF;
2) Conducting an analysis in order to assess the likelihood and impact of ML/TF;
3) Managing the risks; and
4) Regular monitoring and review of those risks.

Further The NRA 2019 considers ML threats separately from the TF threats. Although there is some overlap, warranting separate ML and TF threat assessments.

7.2 Assessment of Money Laundering/Terrorist Financing Threats

- Identification of any Customer or their nominee or authorized persons or directors or beneficial owner or major shareholder who belongs to high-risk jurisdictions within Pakistan as identified in NRA update 2019.
- Identification of any Customer or their nominee or authorized persons or directors or beneficial owner or major shareholder who belongs to high-risk jurisdictions outside Pakistan as identified in NRA update 2019.

- Asses the size, source and the nature of transaction whether incoming or outgoing by the customers pertaining to high risk jurisdictions both domestic and foreign

7.3 Assessment of Transnational Risk

Analysis of the transnational risk of BNP in light of threats and vulnerabilities as highlighted in NRA 2019 which are as under;

- Identification and assessment of the customers of the BNP involving transactions with overseas jurisdictions and asses the degree of risk associated with these customers with the customers with respect to the transnational TF risk.
- Identification and evaluation of the customers or their nominees or authorized persons or directors or sponsors or major shareholders who are Afghan National or Afghan Refugee or national of Iran or Democratic People's Republic of Korea.
- Identification of, if any in the category of domestic NPOs/NGOs who is funded by foreign NPOs or NGOs that have presence in jurisdictions monitored by FATF as high risk or jurisdictions identified as high risk by the BNP who could have possibly links with proscribed entities or individuals.
- Assessment of funding of organizations / individuals at overseas jurisdictions by INGOs/NPOs/NGOs/individuals (including but not limited to Madrassas & religious charitable organizations), if any
- Assessment of the inflow and outflow of funds poured into the accounts of designated / proscribed persons and entities maintained with the BNP, if any, prior to the freezing of the account.
- Where outward remittances were processed through the accounts of exchange companies by the BNP, if any, ensure the CDD/EDD measures which were taken by the exchange company.
- Assessment of the customers involved in practices of hundi / hawala with a view to identify nexus of such customers with other individuals / entities and their methodology of operations.
- Evaluation of the possibility of the cyber frauds involving transfer of funds to accounts maintained in foreign jurisdictions and subsequently transferring these funds into the local jurisdiction by any of the existing customers.
- Assessment of the possible involvement in any criminal activity by any of the existing customers, which has a strong transnational element, such as drug trafficking or smuggling across the borders.

7.4 Assessment of TF Threats posed by Terrorist Organizations

The assessment of the TF threats looked primarily at two main factors:

1 The threat based on terrorism, and

The first goal is to determine level of both internal and external terrorism threat. The analysis looked at terrorists and terrorist organizations (TOs) operating both within the country and in other countries, and at individuals associated with TOs.

2 The threat based on the direction of financial flows, sources, and channels.

The second goal is to identify the impact of the terrorism threat on TF. The assessment aimed at determining the funding needs of different TOs, groups and individuals. In addition, the assessment analyzed where funds were being;

- received or sent,
- the sources of those funds, and
- the channels used for transmission.

Direction of financial flows

The assessment looks at the possible directions of TF flows to determine to what extent the TF threat is primarily internal (generated domestically and used to finance domestic terrorism), external (either generated domestically and used to finance foreign terrorism, or vice versa) or a combination of both.

i Sources

The assessment also aimed at determining the source of TF. It may come from legitimate sources or from the commission of predicate offences.

ii Channels

In order to assess the level and magnitude of threat that certain sectors, products, or services can be exposed to, the assessment examined which channels are being used, or are suspected of being used, for TF.

Entities of concern

Given below is the summary position of ratings assigned to the TOs posing significant and lower TF threats:

No. of TOs	Risk	Names of Terrorist Organizations (TOs)
2	High	Daesh and TTP.
10	Medium High	AQ, JeM, JuD/ FIF, TTA, LeT, HQN, JuA, BLA, LeJ and BLF.

8	Medium	SSP, LeJ-Al-Almi, UBA, BRA, BLT, BRAS, HuA and Unknown.
21	Medium Low and Low	Jesh-ul-Islam, Lashkar-i-Islam, SMP, Lashkar-e-Balochistan, Balochistan Republican Guards, Self-radicalized (lone wolf) terrorists, Hazb-ul–Tehrir, Ahl-e-Sunnat Wal Jamat, Tehreek-e-Jafaria Pakistan, Jeay Sindh Mottahida Mahaz, Harkat-ul-Mujahideen, Tehreek - e- Taliban Swat, Al-Badar Mujahideen, Ansar-ul-Shariya, Balochistan Waja Liberation Army, Baloch Republican Party Azad, Balochistan United Army, Balochistan National Liberation Army, Balochistan Liberation United Front, Baloch Student Organization Azad, Balochistan Muslla Defa Tanzeem.

7.5 DNFBPS and its related ML/TF threats and vulnerabilities

An assessment of the customers whose business and professions pertains to DNFBPs which has M/L threats and vulnerabilities as highlighted in NRA 2019. These are as under

1. Real Estate Dealers (High Vulnerability)
2. Dealers in Precious Metals And Stones (Medium High Vulnerability)
3. Accountants, Auditors and Tax Advisors (Medium Vulnerability)
4. Lawyers (Medium High Vulnerability)

7.6 Assessment of inherent vulnerability levels by type of legal persons

Identification of the customers;

- who are legal persons as private limited companies.
- who are legal person as Foreign companies.
- who are legal person as Domestic limited liability partnerships.
- who are legal person as Domestic Foreign limited liability partnerships.
- who are legal arrangement as WAQF.
- who are legal arrangement as Trust.
- who are NPO

Assessment as to how various types of crimes and their ML threats will affect in assigning appropriate risk rating.

- various legal and natural persons
- customers and /or their nominees or authorized persons
- directors or sponsors or major shareholders in light of NRA 2019

7.8 Analyses of various types of crimes and their ML ratings

Assessment as to how various types of crimes and their ML threats will change the existing ratings assigned to various customer types such as the following:

- Illicit Trafficking in Narcotic Drugs and Psychotropic Substances;
- Corruption and Bribery;
- Smuggling; (Including in Relation to Customs and Excise Duties and Taxes);
- Tax Crimes (Related to Direct Taxes and Indirect Taxes);
- Illegal MVTS/Hawala/Hundi,
- Cash Smuggling;
- Terrorism, Including Terrorist Financing;
- Participation in an Organized Criminal Group and Racketeering,
- Trafficking in Human Beings and Migrant Smuggling;
- Illicit Arms Trafficking;
- Fraud and forgery; Kidnapping,
- Illegal Restraint and Hostage-Taking;
- Robbery or Theft; Extortion;
- Insider Trading and Market Manipulation Cyber Crime Sexual Exploitation,
- Including Sexual Exploitation of Children;
- Illicit Trafficking in Stolen and Other Goods,
- Counterfeiting Currency;
- Counterfeiting and Piracy of Products;
- Murder,
- Grievous Bodily Injury;
- Environmental Crime; Piracy;

7.9 POLITICALLY EXPOSED PERSONS:

DEFINITION OF PEP:

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.

POLITICALLY EXPOSED PERSONS CATEGORIES

PEPs are classified at a high level in the following categories:

1. 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.

2. 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, senior executives of state owned corporations, important political party officials.

3. International organization PEPs

Persons who are, or have 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 or equivalent functions.

4. Family members

Individuals who are related to a PEP either directly (consanguinity) or through marriage or similar (civil) forms of partnership.

5. Close associates

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

7.9.1 In assessing the ML/TF risk of a PEP, following factors should be considered:

- Is from a high risk country;
- Has prominent public function in sectors know to be exposed to corruption;
- Has business interests that can cause conflict of interests (with the position held).

Measures to establish source of wealth and source of funds of PEP

7.9.2 Following additional red flags should be considered for PEP:

The information that is provided by the PEP is inconsistent with other (publicly

available) information, such as asset declarations and published official salaries;

- Funds are repeatedly moved to and from countries to which the PEP does not seem to have ties;
- A PEP uses multiple bank accounts for no apparent commercial or other reason;
- The PEP is from a country that prohibits or restricts certain citizens from holding accounts or owning certain property in a foreign country.

7.9.3 BNP shall take a risk based approach in determining whether to continue to consider a customer as a PEP who is no longer a PEP. The factors that they should consider include:

- the level of (informal) influence that the individual could still exercise; and
- 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).

7.9.4 Approval by senior management (CEO/Director/COO) shall be sought before establishing business relationships with PEPs. Additionally, where appropriate, a STR shall be filed.

8. General

8.1 The concerned employee will verify the information at the time new accounts are opened, if possible, but in most situations not later than five business days after opening.

8.2 Customer's identity shall be verified through documentary evidence, non-documentary evidence, or both. In light of the increased instances of identity fraud, verification may be supplemented with the use of non-documentary evidences as well. In verifying customer identity, any logical inconsistencies in the information obtained shall also be taken into account.

8.3 If the true identity of the customer is still in question the customer shall be notified the same and additional information to verify the customer's identity will be requested. Same case shall be forwarded to Compliance Officer.

9. COMPLIANCE CHECK

9.1 The Compliance Officer shall check the account opening forms along with all annexures before allowing the Customer to start Business Relation with the BNP;

9.2 If there is any discrepancy in the Account Opening process, the Compliance Officer shall communicate the same to Front Office/Dealer/Sale Person for rectification of the same;

9.3 The Compliance Officer shall do the Risk Assessment of the Customer as per AML/CFT

Risk Assessment Matrix annexed to SECP Guideline on AML/CFT Regulations; and

9.4 The Compliance Officer shall do the Risk Profiling of the Customer based on Risk Assessment of the Customer.

10. INTERNAL AUDIT PROCESS

10.1 Internal Auditor shall periodically conduct AML/CFT audits on an Institution-wide basis;

10.2 In case of discrepancies/non-compliances observed during audit process, the findings and along with recommendations shall be communicated to the Audit Committee including Compliance Officer;

10.3 Internal Auditor shall follow-up their findings and recommendation until their complete rectifications.

11. Risk Classification and Management

11.1 On the basis of detailed assessment, each client shall be allotted a Risk profile, from any of the following categories:

- High
- Medium
- Low

11.2 BNP shall assess and analyze as a combination of the likelihood that the risk will occur and the impact of cost or damages, if the risk occurs. The impact of cost or damage may include financial loss to the Company, monitory penalty from regulatory authorities and reputational damages to the business or the entity itself.

11.3 BNP shall analyze and identify the likelihood that these types or categories of risk will be used for ML and/or for TF purposes. This likelihood is for instance:

- High if it can occur several times per year;
- Medium if it can occur once per year; and
- Low if it is unlikely, but not possible.

11.4 In either case, Compliance Officer will be notified so that he can determine whether we should report the situation to FMU. The Company may also refuse any account which is determined to be “high risk” by the compliance officer and for which there is any suspicion and such suspicion in not removed by the customer.

11.5 Based on the risk, and to the extent reasonably practicable, the concerned employees
will ensure that they believe that they know the true identity of the customers by using risk-based procedures to verify and document the accuracy of the information that is obtained from

the customers.

11.6 BNP should update its risk assessment every 12 to 18 months considering all relevant factors.

11.7 BNP shall have appropriate mechanism to provide risk assessment information to the Commission if required.

11.8 Following factors shall be considered for the assessment of inherent ML/TF risks:

HIGH-RISK CLASSIFICATION FACTORS

- The business relationship is conducted in unusual circumstances (e.g. significant
- unexplained geographic distance between BNP and the Customer);
- Non-resident Customers;
- Customer having equity of 20,000,000 and above at any reporting date, and accordingly risk re-profiling of customers is required who meets this threshold. This will be done on quarterly basis.
- Legal persons or arrangements;
- Companies that have nominee shareholders; Business that is cash-intensive;
- The ownership structure of the Customer appears unusual or excessively complex given the nature of the Customer's business such as having many layers of shares registered in the name of other legal persons;
- Politically Exposed Persons;
- Shell companies, especially in cases where there is foreign ownership which is spread across jurisdictions;
- Trusts and other legal arrangements which enable a separation of legal ownership and beneficial ownership of assets; and
- Requested/Applied quantum of business does not match with the profile/particulars of client.
- Crimes, person, business activity, legal arrangements or organization who may pose transnational threat of ML/TF.
- Persons or organization included in list of proscribed persons and organization by any authority.
- the customers whose business and professions pertains to DNFBPs which has M/L threats and vulnerabilities
- Legal persons, as private limited companies, Foreign companies, Domestic limited liability partnerships, Domestic Foreign limited liability partnerships, WAQF, NPO and Trust except pension, provident fund or employees benefit trust of any kind of the listed companies.
- Customers who may be suspected of their involvement in criminal activities as provided in the NRA 2019 and pose a ML threat.
- Customers who belong to High Risk Jurisdiction either within or outside of Pakistan.

COUNTRY OR GEOGRAPHIC RISK FACTOR

- Countries identified by credible sources, such as mutual evaluation or detailed assessment reports or published follow-up reports by international bodies such as the FATF, as not having adequate AML/CFT systems;
- Countries subject to sanctions, embargos or similar measures issued by, for example, the United Nations;
- Countries identified by credible sources as having significant levels of corruption or other criminal activity; and
- Countries or geographic areas identified by credible sources as providing funding or support for terrorist activities, or that have designated terrorist organizations operating within their country.
- The Customer or their nominee or authorized persons or directors or beneficial owner or major shareholder who belongs to high-risk jurisdictions in Pakistan as identified in NRA update 2019
- The customer whose nominee or their authorized persons or directors or beneficial owner belongs to high-risk jurisdictions within Pakistan as identified in NRA update 2019
- The customer who may belong to high-risk jurisdictions outside Pakistan as identified by FATF and mentioned at following web link:

http://www.fatf-gafi.org/countries/#other-monitored-jurisdictions

PRODUCT, SERVICE, TRANSACTION OR DELIVERY CHANNEL RISK FACTOR:

- BNP taking into account the potential risks arising from the products, services, and transactions that it offers to its Customers and the way these products and services are delivered, shall consider the following factors:
- Anonymous transactions (which may include cash);
- Non-face-to-face business relationships or transactions;
- Payments received from unknown or un-associated third parties;
- International transactions, or involve high volumes of currency (or currency equivalent) transactions;
- New or innovative products or services that are not provided directly by the Company, but are provided through channels of the institution;
- Products that involve large payment or receipt in cash; and One-off transactions.

RISK MATRIX

11.9 BNP may use risk matrix annexed as Annexure-1 to SECP Guideline on AML/CFT Regulations as a method of assessing risk in order to identify the types or categories of Customers that are:

- in Low Risk category;
- those that carry somewhat higher risk, but still acceptable risk; and
- those that carry a high or unacceptable risk of money laundering and terrorism financing. RISK MITIGATION AND CONTROLS MEASURES

11.10 The Securities Broker shall consider the following Risk Mitigation Measures:

determining the scope of the identification and verification requirements or ongoing monitoring based on the risks posed by particular customers;

- setting transaction limits for higher-risk Customers such as:
- Individual customers Rs. 5 million net of Sale and Purchase for a particular date
- Corporate customers Rs. 25 million net of Sale and Purchase for a particular date
- Foreigner Individual $ 1 million net of Sale and Purchase for a particular day
- Foreigner Corporate $ 5 million net of Sale and Purchase for a particular day
- requiring senior management approval (CEO/Director/COO) for higher-risk transactions, including those involving PEPs;
- determining the circumstances under which they may refuse to take on or terminate/cease high risk customers;
- determining the circumstances requiring senior management approval (e.g. high risk or large transactions, when establishing relationship with high risk customers such as PEPs)

ENHANCED DUE DILIGENCE (EDD)

11.11 BNP shall be required to perform Enhanced Due Diligence for the following High risk customers and transactions:

- Persons or transactions involving a country identified as higher risk by FATF
- Persons or transactions involving higher risk countries for ML, TF and corruption or subject to international sanctions; and
- Any other situation representing a higher risk of ML/TF including those that you have identified in your Risk Assessment.

11.12 BNP shall apply enhanced CDD measures for high risk business relationships which include:

- Obtaining additional information on the applicant/customer (e.g. occupation, volume of assets, information available through public databases, internet, etc.);
- Updating more regularly the identification data of applicant/customer and beneficial owner;
- Obtaining additional information on the intended nature of the business relationship;
- Obtaining additional information on the source of funds or source of wealth of the applicant/customer;
- Obtaining additional information on the reasons for intended or performed transactions;
- Obtaining additional information on the reasons for which the customer has been categorized as High Risk.
- Obtaining the approval of senior management to commence or continue the business relationship; and
- 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.

11.13 Following factors should be considered to identify persons or transactions from the high risk countries/territories

- Publicly available information;
- Sanctions list issued by the UN;
- FATF high risk and non-cooperative jurisdictions;
- FATF and its regional style bodies (FSRBs) and Transparency international corruption perception index;
- Useful websites include:
    - FATF website: www.fatf-gafi.org ; and
    - Transparency International website: www.transparency.org

11.14 Unusual large and complex transactions and all unusual patterns of transactions that have no apparent economic or lawful purpose should be examined and conduct enhanced CDD Measures consistent with the risk identified.

11.15 Enhanced CDD measures should be taken for following type of suspicious accounts :

- The Customer instructs not to issue any correspondence to the accountholder's address;
- Hold Mail" accounts; and
- Where the evidence of identity of the account holder is not already in the file.

11.16 EDD measures include but are not limited to the following-

a) obtain approval from senior management (CEO/Director/COO) to establish or continue business relations with such customers;

b) establish, by appropriate means, the sources of wealth and/or funds or beneficial ownership of funds, as appropriate including regulated person' own assessment to this effect; and

c) conduct during the course of business relations, enhanced monitoring of business relations with the customer.

12. Supervisory Procedures for Opening of Accounts

12.1 The Accounts Maintenance Department (AMD) will keep all the documents used for verification, including all identifying information provided by a customer (all times during the period such customer has business relationship with us, and for minimum of six years after the termination of business relation with the customer), the methods used and results of verification, and the resolution of any discrepancy in the identifying information.

12.2 Approval by senior management (CEO/Director/COO) shall be sought before establishing business relationships with high-risk customers.

12.3 Either a description or copy of any document that was used to verify identity shall be

for five years after the record is made (a description must note the type of documents and any identification number contained on the document, the place of issuance and the expiration date); a description of the non-documentary verification methods or additional methods used to verify and the results for five years after the record is made.

12.4 Before opening an account, and on an ongoing basis, the AMD will also check to ensure that a customer does not appear on a list provided of known or suspected terrorists or terrorist organizations issued by a Federal government agency or other authorities and to follow all federal directives issued with respect to these lists.

12.5 Information about customer's occupation shall be obtained to assess sources of income to detect and deter possible money laundering and terrorist financing.

12.6 Depending on the nature of the account and requested transactions, the Company may refuse to complete a transaction unless verified the information has been provided, or in some instances may restrict the types of transactions or dollar amount of transactions due to pending verification.

12.7 In case of Trading Accounts of a foreign national or foreign institution approval from respective Head of Department / COO / CEO and Compliance Officer shall be mandatory.

13. Monitoring Accounts For Suspicious Activity

13.1 Operations Department System shall identify suspicious transactions for identification of patterns of unusual size, volume, pattern or type of transactions etc. Transactions, including deposits and wire transfers, in the context of other account activity to determine if a transaction lacks financial sense or is suspicious because it is an unusual transaction for that customer.

13.2 Such transactions shall be reported to the Compliance Officer or his or her designee who will be responsible for monitoring, and will document when and how it is carried out, and will report suspicious activities to the appropriate authorities.

13.3 AML Compliance Officer will conduct an appropriate investigation before filing such report to the FMU keeping in mind that investigation shall not be in the manner that may be categorized as tipping-off to the customer.

14. Red Flags

14.1 Red flags that signal possible money laundering or terrorist financing may include, but are not limited to:

i. Customers who are unknown to the Company and verification of identity/ incorporation proves difficult;

ii. Customers who wish to deal on a large scale but are completely unknown to BNP;
iii. Customers who wish to invest or settle using cash;
iv. Customers who use a cheque that has been drawn on an account other than their own;
v. Customers who change the settlement details at the last moment;
vi. Customers who accept relatively uneconomic terms, when with a little effort they could have a much better deal;
vii. Customers who refuse to explain why they wish to make an investment that has no obvious purpose;
viii. Customers who are introduced by an overseas agent based in a country noted for drug trafficking or distribution.
ix. Customers who carry out large numbers of transactions with the same counterparty in small amounts of the same security, each purchased for cash and then sold in one transaction, particularly if the proceeds are also then credited to an account different from the original account;
x. Customer trades frequently, selling at a loss
xi. Customers who constantly pay-in or deposit cash to cover requests for bankers drafts, money transfers or other negotiable and readily marketable money instruments;
xii. Customers who wish to maintain a number of trustee or customers' accounts which do not appear consistent with the type of business, including transactions which involve nominee names;
xiii. Any transaction involving an undisclosed party;
xiv. transfer of the benefit of an asset to an apparently unrelated third party, or assignment of such benefit as collateral; and
xv. Significant variation in the pattern of investment without reasonable or acceptable explanation
xvi. Transactions appear to be undertaken in a structured, sequential manner in order to avoid transaction monitoring/ reporting thresholds.
xvii. Transactions involve penny/microcap stocks.
xviii. Customer requests a securities provider to execute and/or clear a buy order and sell order for the same security or similar or correlated securities (and/or on behalf of the same beneficial owner), in close chronology.
xix. Transfers are made to the same person from different individuals or to different persons from the same individual with no reasonable explanation.
xx. Unusually large aggregate wire transfers or high volume or frequency of transactions are made with no logical or apparent reason.
xxi. Customer invests in securities suddenly in large volumes, deviating from previous transactional activity.
xxii. Customer conducts mirror trades.
xxiii. Customer closes securities transaction before maturity, absent volatile market conditions or other logical or apparent reason.

10. Responding to Red Flags and Suspicious Activity

10.1 Conducting comprehensive KYC/CDD of the customer at the time of opening of account and tagging all red flags customers as "High risk customers" and make enhanced due diligence of these red flag customers at the time of account opening.

14.2 Receiving cash and cash equivalents at Company's premises will be strictly prohibited

14.3 Payments from any customer are only acceptable through proper banking channel, from customers' own account, third party cheques are not acceptable.

14.4 Funds shall not be transferred from one account to any other customers' accounts in any case;

14.5 In case of withdrawals cheque must be issued in customer's name and no payments shall be made to any third party on behalf of the customers in any case. However, funds can be transferred in the name of the company issuing right shares, in order to purchase right shares, on instructions of the customer.

14.6 No withdrawal shall be allowed to be made in cash.

14.7 Enhanced due diligence procedures should be applied, if the customer's trading limits exceed internal sanction trading limits of the customer based on his declared source of income. Sanctioned criteria on daily basis is given as under:

S. No.	CUSTOMER TYPE	TRADING LIMITS
1	Individuals	Not more than net worth if disclosed with evidence otherwise Rs. 5,000,000 net buy/ Sell position in a particular day.
2	Company Accounts / Trust Accounts	50% of total latest available balance sheet amount. In case audited balance is not available Rs. 5 Million.
3	Financial Institutions	Rs. 100 Million

14.8 When any person in the Company detects any red flag s/he will investigate further under the direction of the AML Compliance Officer. This may include gathering additional information (in the manner that may not be categorized as tipping-off to the customer) internally or from independent sources, contacting the authorities, freezing the account etc.

15. Suspicious Transactions Reporting

Filing a Suspicious Transaction Report - STR

15.1 STRs for any transaction or series of transactions that are conducted, attempted by, at

or through the Company involving an aggregate of at least Rs. 500,000 in funds or other assets (not limited to currency) or more which is known, suspected, or have reason to suspect shall be made if:

a) The transaction involves funds derived from illegal activity or is intended or conducted in order to hide or disguise funds or assets derived from illegal activity as part of a plan to violate or evade federal law or regulation;

b) The transaction is designed to evade the any requirements of the AML regulations;

c) The transaction has no business or apparent lawful purpose or is not the sort in which the customer would normally be expected to engage, and we know, after examining the background, possible purpose of the transaction and other facts, of no reasonable explanation for the transaction, or

d) The transaction involves the use of the Company to facilitate criminal activity.

15.2 The Compliance Officer shall investigate the matter to his satisfaction before filing STR.

15.3 STRs filed (if any) and any supporting documentation shall be kept confidential by the Compliance Officer.

15.4 No information shall be passed on to anyone outside of a law enforcement or regulatory agency and / or securities regulators about STR.

15.5 Disclosure prohibition shall not limited to the person involved in the transaction that is the subject to the STR, but rather applies to all persons except as specifically authorized by regulations. For example, the Company may reveal the existence of the STR with certain affiliates such as a parent company provided the affiliate is subject to STR regulation. Since the affiliate may not reveal the existence of that STR with an affiliate of its own, the Company has policies and procedures in place to ensure that the affiliate protects the confidentiality of the STR. The Company will obtain assurance that the affiliate has appropriate AML policies to maintain the confidentiality of such information.

15.6 The Company will limit access of information to a “need to know” basis, and restrict areas for reviewing STRs and maintain a log of access to STRs, as well as highlight the confidentiality concerns before a person may access information to STRs.

15.7 Request for any information regarding STR’s should be handled only by the Company’s AML compliance officer. The compliance officer is responsible for verifying the request comes from an appropriate law enforcement or enforcement agency and the request should come in form of E-mail or written format so the compliance officer can verify the authenticity of such request by replying to the e-mail or checking the authenticity of the address and calling

the person making such request.

15.8 AML Compliance Officer and his designee will be responsible to ensure that AML records are maintained properly and that STRs are filed as required.

15.9 If any law enforcement agency request that the Company keep an account open, such request must be in writing and must be maintained for a period of five years after the request has expired. (It should be noted that the Company does not have to honor such request and can close such account)

Filing a Currency Transaction Report - CTR

15.10 CTRs are filed only for certain transactions involving "currency." "Currency" is defined as "coin and paper money of the Islamic Republic of Pakistan or of any other country" that is "customarily used and accepted as a medium of exchange in the country of issuance."

15.11 Receipt of currency from the customer is strictly prohibited and the Company has implemented the procedures to prevent its receipt therefore, no CTR will be required to be filed.

Records Required

15.12 As part of our AML program, the Company will create and maintain STRs & CTRs and relevant documentation on customer identity and verification, and funds transfers and transmittals as well as any records related to customers required by the implemented AML rules and regulations.

15.13 The Company shall maintain STRs and their accompanying documentation for at least five years from the date of creation or the date the customer closes his account, if later. Other documents will be kept according to the requirements of existing rules and regulations.

16. Independent audit of AML/CFT Compliance Program

16.1 BNP shall, on a regular basis, conduct an AML/CFT audit to independently evaluate the effectiveness of compliance with AML/CFT Policies and Procedures;

16.2 The frequency of such audit shall at least be on annual basis. However such audit may be conducted on need basis based on the quantum and quality of risks identified during the period.

16.3 The AML/CFT audits shall be conducted to assess the AML/CFT systems of the Company in accordance with the applicable law, rules, regulations and guidelines related to Anti-Money Laundering Law. Such AML/CFT audit may be conducted as a separate assignment or

alongwith other internal audit plan.

17. Record Keeping

17.1 It shall be ensured that all information obtained in the context of CDD is recorded for at least 5 years after termination of the transaction, including but not limited to:

- all the documents received by BNP from clients when verifying the identity of the Customer or the beneficial owner; and
- transcription of the relevant CDD information contained in such documents or obtained by other means.

17.2 All the record of transactions, customers or accounts which involved litigation or required by Court / other competent authorities shall be retained more than 5 years till the resolution/ clearnace of such matters.

17.3 Following records should be maintained at minimum, for a period of at least 5 years after the business relationship has ended:

- Account opening forms & KYC forms
- Copy of identification documents
- All verification documents
- Business correspondence
- Records pertaining to enquiries about:
    - Complex and unusual large transactions
    - Unusual patterns of transactions

17.4 Beneficial ownership information must be maintained for:

- at least five (5) years after the date on which the customer (a legal entity) is dissolved or otherwise ceases to exist; or
- five (5) years after the date on which the customer ceases to be a customer of the Securities Broker.

18. CONTROLS MEASURES AND CONTROLS PUT IN PLACE TO ADDRESS THE ENHANCED RISKS.

Prior to opening of a new account the following controls have been placed;

1 Assessment of all crimes based on the seriousness and magnitude of the crimes as per NRA 2019, both domestically and internationally and in case of suspicion the relationship shall not be established and the STR shall be initiated.

2 Assessment of Transnational Risk including but not limited to source of funds, the flow of money in and out of Pakistan, the channels used for transmission of funds and in case

of suspicion of ML/TF the relationship shall not be established and the STR shall be initiated.

3 Procedure for Screening of Proscribed Persons, entities, terrorist organization and PEPs shall be adopted and in case of suspicion of ML/TF the relationship shall not be established and the STR shall be initiated.

Other Controls include;

4 Develop system and procedure to highlight inward remittances outward remittances received from high-risk jurisdictions.
5 Develop and train the staff to have adequate understanding of the transnational TF risk emanating from financial operations.
6 The Internal Audit to include review of assessment of transnational TF risk of the BNP in its review?
7 Perform screening of your customer database at the time of induction.
8 Perform the screening of customer database on regular basis
9 Filing of STRs relating to TF risk whenever necessary without delay.
10 Keep record of all the accounts which have been rejected during CDD process
11 Maintain the record of all those accounts of clients which have been closed on CDD process
12 High Net worth Individuals are assigned High Risk category and thus are subject to Enhanced Due Diligence. Whereas PEPs are already rated as High Risk.
13 Acceptance of cash is allowed only to the extent of Rs. 25,000/-. Generally, as matter of policy cash transactions are extremely discouraged and are only acceptable under exceptional circumstances warranting exceptional situation.
14 In case of internet based payment it is ensured that the payment comes directly from the customers' bank account and necessary evidence/verification and documents for this purpose are obtained from the customer prior to giving credit in his account.
15 Payments from and to third parties are completely unacceptable and are not practiced at all.
16 Business relationship shall not be established with the clients based in the high risk based jurisdictions, whether local or foreign.
17 Neither any distributor/agent shall be appointed nor shall any office be operated in the high risk based jurisdictions, whether local or foreign.
18 All the existing clients shall again be assessed in the light of the NRA 2019 and their risk rating shall be changed / reassigned wherever applicable.
19 All the new and existing clients shall be assessed for Designated Non-Financial Businesses and Professions (DNFBPs)and shall be assigned risk assessment rating accordingly
20 No business relationship shall be established with the following legal persons and entities
    i. Companies formed under the Companies Act, namely:
        a. Public interest companies.

b. Public sector companies.
c. Companies limited by guarantee (s 2 (19)).
d. Foreign companies (registered under Part 12 of the Companies Act).
e. Associations (formed as charities and not for profit companies) under s 42.

ii. Limited liability partnerships (LLPs) formed under the Limited Liability Partnership Act 2017 and defined under that Act as having separate legal personality, namely:
a. Domestic limited liability partnerships.
b. Foreign limited liability partnerships.

iii. Cooperatives formed under the Cooperative Societies 1925. These entities have independent legal status as legal persons upon registration.

21 No branch alongside porous borders/in different provinces or business through agents/distributors belonging to porous borders, KPK, Baluchistan and Gilgit Baltistan should be opened.

22 No business relationship from high-risk jurisdictions local including KPK, Baluchistan and Gilgit Baltistan or international high-risk jurisdictions will be accepted by the BNP.

19. Training Programs

19.1 The Company will arrange training on AML by arranging internal or external programs periodically and on need basis.

19.2 All key employees of sales, operations, account maintenance department must complete training within 3 months of their hire date (for new employees). For existing employees, the training must be done on an annual basis, and will generally be done within the 4th quarter of the year.

19.3 Training will include, at a minimum:

a) how to identify red flags and signs of money laundering that arise during the course of the employees' duties
b) what to do once the risk is identified; what employees' roles are in the Company's compliance efforts and how to perform them;
c) the Company's record retention policy; and the disciplinary consequences (including civil and criminal penalties) for non-compliance with the AML Act, rules and regulations.

19.4 Records shall be kept to show the persons trained the dates, and the subject matter of their training.

20. Monitoring Employees, Employee Conduct, and Trading Accounts

20.1 The Company's HR Department will conduct a background check, including a check of any criminal records, on all new employees hired by the Company.

20.2 Any suspicious or questionable background information will be discussed with the Company's CEO and Compliance Officer prior to making any final employment decision.

20.3 Employee's trading accounts will be subject to the same ML procedures as customer accounts, under the supervision of the AML Compliance Officer.

20.4 Employees are strictly prohibited to disclose the fact to the customer or any other that a STR or related information is being or has been reported to any authority, except if required by law.

21. Confidential Reporting of AML Non-Compliance

Employees will report any violations of the Company's ML compliance program to the ML Compliance Officer, unless the violations implicate the Compliance Officer, in which case the employee shall report to the CEO. Such reports will be confidential, and the employee will suffer no retaliation for making them.

22. Future Amendments

The management will review and may amend or otherwise modify this Policy Statement from time to time with the approval of Board of Directors of the Company. Such review will preferably be carried out every year and will take into account among others the revisions in applicable regulatory framework specifically.

23. Overriding effect

In case of any inconsistency in this Policy and prevailing Law, Rules and Regulation, the relevant Law, Rules and Regulations will prevail. Moreover, in case of any requirement is not listed in this policy but mentioned in the applicable Law, Rules and Regulations, same should be treated as part and parcel of this policy.

24. Approval from Board of Directors

This policy has been approved by the Board of Directors on November 9, 2019 and access has been provided to the relevant employees of Backers & Partners (Pvt.) Ltd.

25. Effective Date

This policy shall become effective from the November 9, 2019.