



DJM Securities Limited

ANTI- MONEY LAUNDERING & COUNTERING FINANCING OF TERRORISM



(AML/CFT) AND KNOW YOUR CUSTOMER & CUSTOMER DUE DILIGENCE (KYC/CDD) POLICY



DJM Securities Limited




Description	Name / Designation	Signature
Drafted by	Compliance Manager	
Review and finalization by	Compliance Manager	
Approved by	Chief Executive Officer	
First Amendment	N/A	N/A
Second Amendment	N/A	N/A



TABLE OF CONTENTS

GLOSSARY	4
ABOUT DJM SECURITIES LIMITED	5
BACK GROUND	5
GOALS & OBJECTIVES.....	7
SCOPE.....	8
REGULATORY OVERSIGHT & COMPLIANCE RISK	8
AML/CFT & KYC/CDD POLICIES AND PROCEDURES.....	9-16
FOLLOWING CUSTOMERS MAY BE CONSIDERED	16
BENEFICIAL OWNERSHIP OF LEGAL PERSONS AND LEGAL ARRANGEMENTS.....	17-19
RECOGNIZING AND REPORTING OF SUSPICIOUS TRANSACTION / ACTIVITIES	20-21
ACCOUNTABILITIES AND RESPONSIBILITIES	21-22
INTERNAL AUDIT.....	22
ANNEXURE - A	23
Warning Signs/ Red Flags.....	23
ANNEXURE - B	24
LIST OF REQUIRED DOCUMENTS FROM DIFFERENT TYPES OF CUSTOMERS	24-27
ANNEXURE - C	28
RISK PROFILING OF CUSTOMER	28-30
KYC/CDD	32-33

GLOSSARY

AML	Anti-Money Laundering
AOF	Account Opening Form
BOD	Board of Directors
CCO	Chief Compliance Officer
CDD	Customer Due Diligence
CDD	Customer Due Diligence
CFT	Countering Financing of Terrorism
CIF	Customer Information File
CNIC	Computerized National Identity Card
CTR	Cash Transaction Report
EDD	Enhanced Due Diligence
FATF	Financial Action Task Force
FMU	Financial Monitoring Unit
DJML	DJM Securities Limited
ML	Money Laundering
MSB	Money Service Business
NADRA	National Database and Registration Authority
NICOP	National Identity Card for Overseas Pakistanis
OFAC	Office of the Foreign Assets Control
OFAC	Office of Foreign Assets Control
PEP	Politically Exposed Person
PEPs	Politically Exposed Persons
POC	Pakistan Origin Card
PSX	Pakistan Stock Exchange
RMA	Relationship Management Application
RO	Money Laundering Reporting Officer
SBP	State Bank of Pakistan
SDD	Simple Due Diligence
SECP	Securities and Exchange Commission of Pakistan
SNIC	Smart National Identity Card
STR	Suspicious Transaction Report
TF	Terrorist Financing
UN	United Nations
UNSC	United Nations Security Council



DJM Securities Limited

ABOUT DJM SECURITIES LIMITED

DJM Securities Limited has held a significant role in the establishment of the financial (or whatever other industry you want to write) industry since the past decade. It has been providing brokerage services to various financial Institutions, including the top players of the local capital market.

BACK GROUND (WHAT IS MONEY LAUNDERING?)

Money laundering has one purpose: to turn the proceeds of crime into cash or property that looks legitimate and can be used without suspicion. Here are some of the most common ways this is achieved.

There are usually three phases to the laundering:

Placement

Layering

Integration/Extraction

Cash businesses – adding the cash gained from crime to the legitimate takings. This works best in business with little or no variable costs, such as car parks, strip clubs, tanning studios, car washes, and casinos. False invoicing – putting through dummy invoices to match cash lodged, making it look like payment in settlement of the false invoice Surfing – lodging small amounts of money below the AML reporting threshold to bank accounts or credit cards, then using these to pay expenses etc.

Trusts and offshore companies – useful for hiding the identity of the real beneficial owners. Foreign bank accounts – physically taking small amounts of cash abroad, below the customs declaration threshold, lodging in foreign bank accounts, then sending back to the country of origin. Aborted transactions – funds are lodged with a lawyer or accountant to hold in their client account to settle a proposed transaction. After a short time, the transaction is aborted. Funds are repaid to the client from an unimpeachable source

Layering is essentially the use of placement and extraction over and over again, using varying amounts each time, to make tracing transactions as hard as possible.

The final stage is getting the money out so it can be used without attracting attention from law enforcement or the tax authorities. In this regard, criminals are often content to pay payroll and other taxes to make the “washing” more legitimate and are often happy with a 50% “shrinkage” in the wash.

Fake employees - a way of getting the money back out. Usually paid in cash and collected Loans - to directors or shareholders, which will never be repaid Dividends - paid to shareholders of companies controlled by criminals

In recent times, regulations have been exhibited globally to discourage money laundering and financing of illegal/criminal (illegal is criminal. There's repetition) activities. Furthermore, under the United Nations umbrella, several international agreements have been signed by U.N. member states, under which member states are bound to implement policies that discourage money laundering and monitor financial transactions that raise concerns about money laundering. The Islamic Republic of Pakistan is a signatory to such an agreement and is a member of relevant bodies such as Financial Action Task Force (FATF). As such, Pakistan must abide by the recommendations of FATF and other relevant bodies; implement appropriate policies and procedures. If Pakistani policies are not in line with said recommendations, the image of the country is on the risk of being compromised. Withal, local industries (financial, textile and others) can face difficulties in conducting trade across the globe. Consequently, this will manifest a gloomy economic outlook of the Pakistani economy.

Pakistan has enacted the ANTI MONEY LAUNDERING ACT 2010. Financial institutions and intermediaries are required to comply with the provisions of this Act. Apex capital market regulator, Securities and Exchange Commission of Pakistan (SECP) has provided comprehensive guidelines for Pakistani capital market institutions regarding implementation of such policies. They will help discourage money laundering and allow capital market institutions to monitor suspicious transactions and/or factions who might attempt to launder money. In the case of the brokerage industry, SECP and Pakistan Stock Exchange Limited have formulated detailed set of guidelines for brokers to help them in developing and implementing KYC and CDD policies.

DJML is committed to the comply highest standards of AML and CFT. The board members and the employees are required to adhere to these standards to protect **DJML's** prestige from being misused for money laundering and/or terrorist financing or other illegal purposes.

DJML will adhere to all applicable laws and regulation in all countries where it conducts businesses or has business relationships with, but in case of any adherence local laws will always prevail.

DJML will examine its AML and CFT strategies, goals and objectives on regular basis and for all these topics. **DJML** has implemented clear rules and regulations which must be complied by all the members of the organization.

GOALS & OBJECTIVES

The objective of this policy is to ensure that the products and services of the **DJM Securities Limited (DJML)** are not used to launder the proceeds of criminal activities. Moreover, **DJML's** staff is aware of their obligations and duties in the fight against money laundering/terrorist financing. The document also provides a structure to comply with applicable laws, regulatory guidelines related to finding and reporting of suspicious activities.

Other objectives pursued by this policy are as follows:

- Promote a “Know Your Customer” policy as a foundation principle for the Brokerage firm’s ethics and practices;
- Introduce a controlled environment where no business with a Customer is transacted until all essential information concerning the Customer has been obtained;
- Conduct self-assessments of compliance with AML/CFT policy and procedures;
- Introducing employees to the stages of money laundering process and their individual duties;
- Establishing a review process which will be used to identify opportunities that might be used to launder money;
- Providing instructions regarding taking appropriate action once a suspicious activity or a money laundering activity is suspected.

Adherence to this policy is completely primary for ensuring that the **DJML** is fully complies with applicable anti-money laundering rules and regulations.

DJML is committed to examining its anti-money laundering strategies, goals and objectives on an ongoing basis and maintaining an effective AML Policy for its business.

SCOPE

In case of any clarification contact Compliance department at info@djmtrade.com

This policy is applicable to the **DJML's** local and overseas operations, including business of other Financial Institutions routed through **DJML**.

In overseas offices (if any), **DJML** shall ensure compliance with the Regulations of the host country on KYC, CDD AML/CFT or that of the SECP whichever are more exhaustive.

REGULATORY OVERSIGHT & COMPLIANCE RISK

In the case of the brokerage industry, SECP being its Apex regulator and the PSX being its frontline regulator of the brokerage industry in Pakistan, have formulated detailed set of guidelines for brokers to help them in developing AML/CFT & KYC/CDD policies & procedures and implementing the same.

DJML is bound to use SECP, PSX and International Regulatory guidelines/standards as applicable to formulate its own AML/CFT & KYC/CDD Policy. The consequence of contravening the Regulations or failing to comply can be significant and include disciplinary measures such as imprisonment, fine or both under local laws as well as the loss of reputation for **DJML**.

Notwithstanding the statutory and regulatory penalties, increased vigilance by Management and staff will protect **DJML** from the following risks:

- Reputational
- Operational
- Legal
- Financial

Reputational risk:

Reputational risk is a threat or danger to the good name or standing of a business or entity. Reputational risk can occur through several ways: through the actions of the company itself; indirectly due to the actions of an employee or employees or tangentially through other peripheral parties, such as joint venture partners or suppliers. In addition to having good governance practices and transparency, companies need to be socially responsible and environmentally conscious to avoid or minimize reputational risk. A strong AML/CFT & KYC/CDD policy helps to prevent a business from being used as a vehicle for illegal activities.

OPERATIONAL RISK:

Operational risk is the prospect of loss resulting from inadequate or failed procedures, systems or policies. Employee errors, systems failures, fraud or other criminal activity that disrupts business processes. If AML/CFT& KYC/CDD policy is poorly implemented, then operational resources are wasted, there is an increased chance of being used by criminals for illegal purposes.

LEGAL RISK:

The risks that counterparty to a transaction will not be liable to meet its obligations under law. Such difficulties may arise due to several reasons, one of the most common being that the transaction was not sufficiently well-documented to be legally enforceable.

FINANCIAL RISK:

If a business does not adequately identify and verify customers, it may run the risk of unwittingly allowing a customer to pose as someone they are not. The consequences of this may be far reaching. If a business does not know the identity of its customers, it will also be difficult to retrieve money that the customer owes.

AML/CFT & KYC/CDD POLICIES AND PROCEDURES

KYC/CDD is closely associated with the fight against money-laundering “AML”. Supervisors around the world are increasingly recognizing the importance of ensuring that their financial institutions have adequate controls and procedures in place so that they know the customers with whom they are dealing. Adequate due diligence on new and existing customers is a key part of these controls. Without such due diligence, financial institutions can be exposed to reputational, operational, legal and financial risks.

Following key Areas has been covered:

- A. Assessment of TF Threat
- B. Customer Identification
- C. Account Opening Documentation
- D. Verification of Identity/ Know Your Customers (“KYC”)
- E. Account Opening Documentation
- F. Risk assessment of customer
- G. Circumstances where Enhanced Due Diligence is required
- H. On-going due Diligence
- I. Circumstances where simplified Due Diligence can be adopted
- J. Compliance function
- K. Data retention
- L. Training and employee screening.

A. ASSESSMENT OF TF THREAT

DJML will assess TF threats initially at the time of account opening of the clients. The assessment will be based on data available at UN sanctions committee's website, National Counter Terrorism Authority's website and different SROs issued by the Federal Government. **DJML** will also perform screening of its existing entire clientele from the data available at the above mentioned regulatory websites and with the SROs. During this exercise, in case of true match or suspicion, the authorized officer of the DJML will be responsible to comply all the sanctions obligations including:

Freeze the customer fund or block the transaction (existing customer)
Reject the customer (new client)
Lodge STR with FMU
Notify the SECP and MOFA

As per the updated NRA 2019, Pakistan is facing terrorism and TF threat from terrorist organizations in Afghanistan, Pakistan and in areas adjacent to Pak-Afghan border areas. Further, long porous border with Iran and Afghanistan is a major cause of crimes and Terrorist Financing. Therefore, in view of this information, TF threat risk of the clients would be assessed. Their transactions will be monitored periodically as part of ongoing monitoring. Inflows and outflows of the funds will be properly monitored and investigated. Screening will also be performed for entities of concern mentioned in updated NRA 2019. The policy of the company in case of true match or suspicion will be same as explained above.

DJML will not provide services to proscribed individuals, groups and entities declared by UNSC (United Nations Security Council) or notified by NACTA and those who are known for their association with such entities and persons, whether under the proscribed name or with a different name.

B. CUSTOMER IDENTIFICATION

Customer identification is very important that will protect our company from being used by immoral and/or illegal elements. In this respect minimum documents/information as prescribed by SECP must be obtained from customers at the time of opening of accounts. Further, any additional document/information may be obtained on case to case basis where considered necessary. The key point is that anonymous or obviously fictitious accounts should not be opened.

- In case a customer is acting on behalf of another person, then identity of that person shall be ascertained and relevant documents/information of that person need to be obtained also.
- For non-individual customers (e.g. companies, pension funds, government owned entities, non-profit organizations, foreign companies/organizations) additional care shall be taken to establish the ownership and control structure of such an organization and who (i.e. person(s)) owns the organization and who manages it. It shall be verified that the person who represents himself as authorized signatory with powers to open and operate the account is authorized by the organization.

- For individual customers, proper authorization shall be obtained from person authorized to act on behalf of the customer.
- It shall be ensured that accounts of Institutions/organizations/corporate bodies are not opened in the individual name(s) of employee(s)/official(s). Because of sensitive nature of public sector (government) entities and risk of potential conflict of interest,
- These accounts shall not be opened in the individual name of any employee/official. any such account, which is to be operated by an officer of a govt. owned entity, is to be operated by an officer of the Federal/Provincial/Local Government in his/her official capacity, shall be opened only on production of a special resolution/authority from the concerned administrative department, duly endorsed by the Ministry of Finance or Finance Department of the concerned Provincial or Local Government.
- Sufficient information shall be obtained and documented on the purpose and intended nature of account to be opened and a profile shall be developed based on results of customer identification and the risk assessment. Information regarding intended investment plan of the customer must be obtained to the extent possible and should be documented.
- Sufficient information shall be obtained to determine the expected source of funding for the account, particularly whether the customer shall receiving/remitting funds in foreign currency.
- It must be ensured that all receipts and payments to the customers above the prescribed threshold (i.e. Pkr.25,000/-) are made through cross cheques, bank drafts, pay orders or other crossed banking instruments. For exceptional circumstances where it shall become compulsory to accept cash from a customer, reporting of such instances with justification should be made right away to the exchanges.
- Politically exposed persons or PEPs are individuals who are entrusted with prominent public functions either domestically or by a foreign country, or in an international organization, for example Heads of State or of government, senior politicians, senior government, judicial or military officials, senior executives of state owned corporations/departments/autonomous bodies. This does not intend to cover middle ranking or more junior individuals in the foregoing categories.
- High net worth individual (HNWI) is a classification used by the financial services industry to denote an individual or a family with liquid assets above a certain figure. Although there is no precise definition of how rich someone must be to fit into this category, high net worth is generally quoted in terms of having liquid assets of a particular number. The exact amount differs by financial institution and region. In Reference to country like Pakistan it is said to be fall under HNWI when the investment amount is above Pkr 5.0 Million Rupees

C. ACCOUNT OPENING DOCUMENTATION

For each type of customer, certain documentation must be obtained and sufficient information gathered for us to be certain that:

- we know our new customer, having verified identity and address and understand the customer's business and the expected levels of transactions;
- the new customer has understood and accepted the **DJML** terms and conditions for the account;
- we are satisfied that the mandated individuals do have the authority of the account holder(s) to control the account; and
- we are satisfied that the account holder(s) and their business is legitimate and the Company is not at risk of financial loss or reputation damage.

Original identification documents must be seen, photocopied and retained in the customer's file. Care must be taken to ensure that the copies are clear and legible and that the copies are stamped, signed and dated to show that the originals have been seen.

When a prospective customer does not yet have a permanent residential address, documentary evidence of the temporary address should be obtained. Only original or certified photocopy documentation is acceptable.

A checklist has been developed and annexed (Annexure A) to these policies and procedures. Details of necessary documents, information and procedures required to be obtained/followed have been incorporated therein. Further, necessary documents/information required have also mentioned in relevant account opening forms and are not reproduced herein to avoid repetition.

D. VERIFICATION OF IDENTITY/ KNOW YOUR CUSTOMERS ("KYC")

Staff must prudently ensure that all the necessary documents have been obtained at the time of account opening. The Company has a statutory obligation to know its customers. This applies to every type of customer regardless of who they are, their personal status, or the type of account or service that they require. Knowing your customer means:

- Seeking evidence of identity and address and independently confirming that evidence at the start of a business relationship.
- Seeking information regarding the nature of the business that the customer expects to conduct with the Company
- Establishing sources of income and expected patterns of transactions
- Keeping the information up to date, to show what might be regarded as normal activity for that customer.

All prospective customers for accounts with DJM Securities Limited must be seen face to face. The appropriate account opening and customer information forms must be completed and any additional interview notes must be obtained and retained on the customer file.

E. RISK ASSESSMENT OF CUSTOMER

Risk assessment must be performed of all the existing and potential customers based on information obtained regarding their identity, nature of income, source of funding, location etc. and based on the results of such assessment, categorize customers among high risk, medium risk and low risk customers.

F. ENHANCED DUE DILIGENCE

(1) Regulated person shall implement appropriate internal risk management systems, policies, procedures and controls to determine if any customer presents high risk of ML/TF. The regulated person shall apply EDD where a customer presents high risk of ML/TF including but not limited to the following circumstances:

- (a) business relationships and transactions with natural and legal persons when the ML/TF risks are higher;
- (b) business relationships and transactions with natural and legal persons from countries for which this is called for by the FATF;
- (c) PEPs and their close associates and family members.

(2) EDD measures include but shall not be limited to the following measures:

- (a) Obtaining additional information on the customer (e.g. volume of assets, information available through public databases, internet, etc.), and updating more regularly the identification data of customer and beneficial owner;
- (b) Obtaining additional information on the intended nature of the business relationship;
- (c) Obtaining information on the source of funds or source of wealth of the customer;
- (d) Obtaining information on the reasons for intended or performed transactions.
- (e) Obtaining the approval of senior management to commence or continue the business relationship;
- (f) 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.

(3) An insurer/ takaful operator shall include the beneficiary of a life insurance policy as a relevant risk factor in determining whether EDD measures are applicable under subsection (1). where an insurer/ takaful operator determines that a beneficiary who is a legal person or a legal arrangement

presents a higher risk, it shall take EDD measures and take reasonable measures to identify and verify the identity of a beneficial owners of the beneficiary of a life insurance policy or takaful at the time of payout.

(4) In relation to 21(1)(c), the regulated person shall implement appropriate internal risk management systems, to determine if a customer or a beneficial owner is a PEP or a close associate or family member of a PEP, both prior to establishing a business relationship or conducting a transaction, and periodically throughout the course of business relationship. The regulated person shall apply, at minimum the following EDD measures:

- (a) obtain approval from senior management to establish or continue a business relationship where the customer or a beneficial owner is a PEP, close associate or family member of a PEP or subsequently becomes a PEP, close associate and family member of a PEP;
- (b) take reasonable measures to establish the source of wealth and the source of funds of customers and beneficial owners identified as a PEP, close associate or family member of a PEP; and
- (c) conduct enhanced ongoing monitoring of business relations with the customer or beneficial owner identified as a PEP, close associate and family member of a PEP.

(5) An insurer/ takaful operator shall take reasonable measures at the time of payout of a life insurance policy to determine whether the beneficiaries and/or, where applicable, the beneficial owner of the beneficiary are politically exposed persons.

(6) Where higher risks are identified under subsection (5), an insurer or takaful operator must inform senior management before the payout of the policy proceeds, to conduct enhanced scrutiny of the whole business relationship with the policyholder, and to consider making a suspicious transaction report

G. ON-GOING DUE DILIGENCE

It shall be ensured

- That on-going Due Diligence on the customer relationship and examination of transactions is undertaken to ensure that the transactions executed in a specific account are in line with the company's information of the customer, its business and risk profile, historical pattern of transactions and the pattern and source of funding of the account.
- That the customers' records are updated at regular intervals and adequate information is obtained regarding any significant change in the customers' profiles.

H. SIMPLIFIED DUE DILIGENCE

CDD measures shall be simplified or reduced in the following conditions:

- Risk of money laundering or terrorist financing is lower.
- Information on the identity of the customer and the beneficial owner of a customer is publicly accessible.
- Satisfactory checks and controls exist.

I. ON GOING MONITORING

Once the identification procedures have been completed and the business relationship is established, the DJM Securities Limited is required to monitor the conduct of the relationship to ensure that it is consistent with the nature of business stated when the relationship/account was opened. The DJM Securities Limited shall conduct ongoing monitoring of their business relationship with its Customers. Ongoing monitoring helps the DJM Securities Limited to keep the due diligence information up-to-date, and review and adjust the risk profile of the customers, where necessary. The DJM Securities Limited conduct on-going due diligence which include scrutinizing the transactions undertaken through the course of business relationship with a Customer.

The DJM Securities Limited will be required to update the Risk Assessment of their Customer as per following schedule or on the occurrence of a triggering event, whichever is earlier:

- For its High Risk Customers, their Risk Assessment shall continuously be reviewed and updated, but a comprehensive review should be done at least quarterly
- For its Medium Risk Customers, their Risk Assessment shall be updated bi-annual basis.
- For its Low Risk Customers, their Risk Assessment shall be updated annually

The DJM Securities Limited may update the Customer CDD record on triggering of following events:

- Material changes to the customer risk profile or changes to the way that the account usually operates;
- Where it comes to the attention of the DJM Securities Limited that it lacks sufficient or significant information on that particular customer;
- Where a significant transaction takes place;
- Where there is a significant change in customer documentation standards;
- Significant changes in the business relationship.

The DJM Securities Limited updates Risk Profiling of the Customer in the following circumstances:

- New products or services being entered into;
- A significant increase in a customer's salary being deposited;
- The stated turnover or activity of a corporate customer increases;
- A person has just been designated as a PEP;
- The nature, volume or size of transactions changes.

The **DJM** Securities Limited shall be vigilant for any significant changes or inconsistencies in the pattern of transactions. Inconsistency is measured against the stated original purpose of the accounts. Possible areas to monitor could be:

- transaction type;
- frequency;
- amount;
- geographical origin/destination;
- Account signatories.

The **DJM** Securities Limited shall take the following steps to ensure that its Customers are who they purport themselves to be:

- To identify and verify the Customers including their beneficial owners;
- To understand the intended nature and purpose of the relationship;
- To know actual ownership; and
- To know control structure of the Customer.

The **DJM** Securities Limited shall conduct ongoing due diligence on the business relationship and scrutinize transactions undertaken throughout the course of that relationship to ensure that transactions being conducted are consistent with:

- Knowledge of the Customer;
- Business and Risk Profile;
- Where necessary, the source of funds.

J. COMPLIANCE FUNCTION

(1) In order to implement compliance programs as set out in 7G of the AML Act, the regulated person shall implement the following internal policies, procedures and controls:

- (a) compliance management arrangements, including the appointment of a compliance officer at the management level, as the individual responsible for the regulated person's compliance with these Regulations, the AML Act and other directions and guidelines issued under the aforementioned regulations and laws;
- (b) screening procedures when hiring employees to ensure the integrity and conduct, skills, and



DJM Securities Limited

- expertise of such employees to carry out their functions effectively;
 - (c) an ongoing employee training program; and
 - (d) an independent audit function to test the system.
- (2) For purposes of (a) the regulated person shall ensure that the compliance officer:
- (a) reports directly to the board of directors or chief executive officer or committee;
 - (b) has timely access to all customer records and other relevant information which they may require to discharge their functions, as well as any other persons appointed to assist the compliance officer;
 - (c) be responsible for the areas including, but not limited to
 - i. ensuring that the internal policies, procedures and controls for prevention of ML/TF are approved by the board of directors of the regulated person and are effectively implemented;
 - ii. monitoring, reviewing and updating AML/CFT policies and procedures, of the regulated person;
 - iii. providing assistance in compliance to other departments and branches of the regulated person;
 - iv. timely submission of accurate data/ returns as required under the applicable laws;
 - v. monitoring and timely reporting of Suspicious and Currency Transactions to FMU; and
 - vi. such other responsibilities as the regulated person may deem necessary in order to ensure compliance with these regulations

K. DATA RETENTION

It is required to maintain the related documents obtained through the application of KYC/CDD/AML/CFT procedures, especially those pertaining to identification of the identity of a customer, account files and correspondence exchanged for a minimum period of five years.

L. TRAINING AND EMPLOYEE SCREENING

Appropriate on-going employee training program and knowledge refreshment shall be arranged to ensure that the employees understand their duties and are able to perform them in a suitable manner.

Diligence is required when recruiting people. All possible screening measures shall be considered, such as: - independent inquiries, information from previous employers/ colleagues etc. Further, screening process shall be an on-going exercise and shall be applied consistently to ensure that employees, particularly those working in sensitive positions, meet and maintain high values of integrity and professionalism.

Any information concerning customers and their transactions shall be provided to the exchanges, Financial Monitoring Unit or the Commission as and when required.

All requirements of Anti Money Laundering and Countering financing of Terrorism Regulations, 2018 as applicable, including the requirement to file Suspicious Transaction Reports and any directives, circulars, guidelines issued in this regard by Federal Government, Financial Monitoring Unit and SECP shall be complied.

A checklist has been developed and annexed to these policies and procedures. Details of necessary documents, information and procedures required to be obtained/ followed have been incorporated therein. Further, necessary documents/information required have also mentioned in relevant account opening forms and are not reproduced herein to avoid repetition. All relevant laws / regulations / recommendations / guidelines/directives of relevant authorities (e.g. SECP, FATF etc.) are available separately.

FOLLOWING CUSTOMERS MAY BE CONSIDERED FOR SIMPLIFIED OR REDUCED CDD:

- Financial institutions which are subject to requirements to combat money laundering and terrorist financing consistent with the FATF Recommendations and are supervised for compliance with those controls.
- Public companies that are subject to regulatory disclosure requirements.
- Government administrations or enterprises.

When opting for simplified or reduced due diligence, the FATF guidelines in this regard shall be consulted. Simplified CDD shall not be followed when there is an identified risk of money laundering or terrorist financing.

BENEFICIAL OWNERSHIP OF LEGAL PERSONS AND LEGAL ARRANGEMENTS.

The different types of legal persons that can be formed in Pakistan are as follows;

- i) Companies formed under the companies act, namely;**
 - a) Private Companies
 - b) Public Companies (also known as listed companies)
 - c) Public interest companies
 - d) Public Sector Companies
 - e) Companies limited by guarantee
 - f) Foreign Companies (registered under part 12 of the companies Act)
 - g) 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 the act as having separate legal personality, namely;**
 - a) Domestic limited liability partnerships.
 - b) Foreign limited liability partnerships
- iii) Cooperatives found under the cooperative societies 1925. These entities have independent legal status as legal persons upon registration.**

Where the customer is a legal person, in addition to other measures the company shall-

- a) Understand the nature of the customer's business and its ownership and control structure by asking questionnaires and recording on SAOF
- b) Identify and verify the identity of the natural persons (whether acting alone or together) who ultimately own the legal person by obtaining relevant information from the customer by acquiring the following Certified copies of:
 - Resolution of Board of Directors for opening of account specifying the person(s) authorized to open and operate the account;
 - Memorandum and Articles of Association;
 - Certificate of Incorporation;
 - Certificate of Commencement of Business, wherever applicable;
 - List of Directors on 'Form-A/Form-B' issued under Companies Act, 2017, as applicable; and
 - Form-29, wherever applicable.
 - Photocopies of identity documents of all the directors and persons authorized to open and operate the account;

- a) Where there is doubt under Memorandum and Article of Association as to whether the natural persons who ultimately own the legal person are the beneficial owners or where no natural persons ultimately own the legal person, identify the natural persons (if any) who ultimately control the legal person or have ultimate effective control of the legal person by probing and investigating the documents obtained.
- b) Where no natural persons are identified under clause Memorandum and Articles of Association or Certificate of Incorporation, identify the natural persons having executive authority in the legal person, or in equivalent or similar positions.

if the DJM Securities Limited has any reason to believe that an applicant has been refused facilities by another DJM Securities Limited 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.

RISK CATEGORIES

Based on the results of such assessment, categorize customers among high risk and low risk customers.

High Risk Customers

Following are general broad outline of factors that will categorize the customers into high risk category:

- non-resident customers;
- legal persons or arrangements that have complex structure;
- Foreign individual and corporate clients;
- Companies that have nominee shareholders;
- Politically Exposed Persons (PEPs) or customers holding public or high profile positions;
- customers belonging to countries where CDD / KYC and anti-money laundering regulations are lax or if funds originate or go to those countries;
- Clients from high risk jurisdictions in Pakistan as identified in updated NRA 2019;
- customers whose business or activities present a higher risk of money laundering such as cash based businesses;
- customers with links to offshore tax havens;
- high net worth customers with no clearly identifiable source of income;
- there is reason to believe that the customer has been refused brokerage services by another brokerage house;
- Non-face-to-face /on-line customers;
- establishing business relationship or transactions with counterparts from or in countries not sufficiently applying FATF recommendations;

- Establishing business relationship or transactions with counterparts from or in countries as having significant level of corruption or other criminal activities; and ✓ payments received from unknown or un-associated third parties.

Low Risk Customers

Following are general broad outline of factors that will categorize the customers into low risk category:

- customers belonging to countries as having effective AML/ CFT systems;
- customers belonging to countries as having a low level of corruption or other criminal activities;
- low net worth customers;
- Customers whose source of income are clearly identifiable.

RISK MITIGATION

DJML senior management and staff will take the following measures to mitigate the assessed risk:

- Obtain senior management (i.e. HOD, CEO and COO) approval for higher-risk transactions.
- Set Transaction limits for Customers with respect to their source of income and level of income.
- Monitor their deposit amount with their declared level of income.
- Complete KYC/CDD of each client and verify their identification and supporting documents.

Ongoing monitoring must be performed by senior management (i.e. HOD, CEO and COO) of their business relationship with its Customers that present a higher money-laundering risk might include, but are not restricted to:

- customers linked to higher-risk countries or business sectors
- customers who have unnecessarily complex or opaque beneficial ownership structures
- transactions that are unusual, lack an obvious economic or lawful purpose, are complex or large or might lend themselves to anonymity

Requiring senior management approval 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).

RECOGNIZING AND REPORTING OF SUSPICIOUS TRANSACTIONS / ACTIVITIES

The company is required to report to Financial Monitoring Unit when company receives a cash based transaction involving payment, receipt, or transfer of an amount exceeding the minimum threshold as specified by the National Executive Committee (NEC), hereinafter referred to as the NEC, “**DJML**” shall file a report of such transaction on prescribed format immediately but not later than seven working days, after the respective currency transaction.

The company manually monitors a sufficient amount of account activity to permit identification of patterns of unusual size, volume, pattern or type of transactions, geographic factors such as whether jurisdictions designated as “non-cooperative” are involved, or any of the “red flags”

identified in SECP’s guidelines on Anti Money Laundering Regulations, 2018 as mentioned in Annexure A Company will look at transactions, 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. Company will report suspicious transaction reporting to Financial Monitoring Unit immediately but not later than seven working days after forming that suspicious in respect of that particular transaction was followed through or not.

The transactions, which are out of character or inconsistent with the history, pattern, or normal operation of the account including through heavy deposits, withdrawals and transfers, etc should be viewed with the suspicion, and be properly investigated.

If Compliance officer decides to report any transaction/ account to the FMU as “Suspicious” based on the justifiable grounds, the same should be reported to FMU under intimation to the CEO/ Chairman of the board.

All the employees of **DJML** are strictly prohibited to disclose the fact to the customer or any other quarter that a suspicious transaction or related information is being or has been reported to any authority, except if required by law.

The **DJML** 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.

REPORT TO SECP

DJML will report to Securities and Exchange Commission of Pakistan (SECP) all unusual or large transactions in an equity account which apparently have no genuine economic, commercial or lawful purpose provided that the Company after complete investigation/inquiry come to a conclusion that such transactions are not for economic, commercial or lawful business purpose and relate to illegal or illicit activities, corruption or corrupt practices and narcotic activities.

All requirements of Anti Money Laundering and Countering Financing of Terrorism Regulations, 2018 as applicable, including the requirement to file Suspicious Transaction Reports and any directives, circulars, guidelines issued in this regard by Federal Government, Financial Monitoring Unit and SECP will be complied.

A register will be maintain regarding FMU report. Such register will contain the following details:

1. Date of the report;
2. Person who made the report;
3. Person to whom the report was forwarded; and
4. Reference by which supporting evidence is indefinable.

ACCOUNTABILITIES AND RESPONSIBILITIES

THE BOARD IS RESPONSIBLE FOR:

- Ensuring that adequate systems and controls are in place to deter and recognize criminal activity, money laundering and terrorist financing.
- Seeking compliance reports including coverage of AML/CFT issues) on quarterly basis and taking necessary decisions required to protect DJML from use by criminals for ML & TF activities.
- The Oversight of the adequacy of systems and controls that are in place to deter and recognize criminal activity, money laundering and terrorist financing.

COMPLIANCE OFFICER IS RESPONSIBLE FOR:

- Ensuring that staff is aware of their obligations and the Company's procedures, and that staff are adequately aware of money laundering prevention.
- Representing the DJML to all external agencies in Pakistan in relation to money laundering compliance.
- Ensuring that all segments of the Company are complying with the stated policy and therefore monitoring operations and development of the policy.
- Preparing and presenting compliance reports to the Senior Management.

- Ensuring that staff members complete the "Annual Acknowledgement Form for the Prevention of Money Laundering"
- Undertaking the internal review of all suspicions and determining whether or not such suspicions have substance and require disclosure to SECP.
- Advising Senior Management of any deviations from the policies and procedures that have been noted by Compliance Division during their reviews.
- Developing and maintaining policy in line with evolving statutory and regulatory obligations.

MANAGEMENT IS RESPONSIBLE FOR:

- Ensuring that AML/CDD/CFT policy is implemented in letter and spirit.

ALL EMPLOYEES ARE RESPONSIBLE FOR:

- Remaining vigilant to the possibility of money laundering / terrorist financing through use of DJML's products and services.
- Complying with all AML/CFT policies and procedures in respect of customer identification, account monitoring, record keeping and reporting.
- Promptly reporting to CO where they have knowledge or grounds to suspect a criminal activity or where they have suspicion of money laundering or terrorist financing whether or not they are engaged in AML / CFT monitoring activities.
- Understanding DJML's Policy and Procedures on AML/CDD/CFT and to sign-off on the require Form.
- Employees who violate any of the Regulations or the DJML's AML/CDD/CFT policies and procedures will be subject to disciplinary action.

INTERNAL AUDIT

Internal Auditor of the DJML shall also review the compliance of the Anti Money Laundering function of the Company to ensure that the AML Policy is being effectively implemented by the management of the DJML.

ANNEXURE – A

Warning Signs/ Red Flags

1. Customers who are unknown to the broker and verification of identity / incorporation proves difficult;
2. Customers who wish to deal on a large scale but are completely unknown to the broker;
3. Customers who wish to invest or settle using cash more than Rs.25000 /-
4. Customers who use a cheque that has been drawn on an account other than their own;
5. Customers who change the settlement details at the last moment;
6. Customers who insist on entering into financial commitments that appear to be considerably beyond their means;
7. Customers who are introduced by an overseas agent based in a country noted for drug trafficking or distribution
8. 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;
9. Customer trades frequently, selling at a loss
10. Customers who constantly pay-in or deposit cash to cover requests for bankers' drafts, money transfers or other negotiable and readily marketable money instruments;
11. Customers who wish to maintain several trustee or customers' accounts which do not appear consistent with the type of business, including transactions which involve nominee names;
12. Any transaction involving an undisclosed party;
13. Significant variation in the pattern of investment without reasonable or acceptable explanation
14. Transactions appear to be undertaken in a structured, sequential manner in order to avoid transaction monitoring/ reporting thresholds.
15. 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.
16. Transfers are made to the same person from different individuals or to different persons from the same individual with no reasonable explanation.
17. Unusually large aggregate wire transfers or high volume or frequency of transactions are made with no logical or apparent reason.
18. Customer invests in securities suddenly in large volumes, deviating from previous transactional activity.
19. Customer conducts mirror trades.

ANNEXURE – B

LIST OF REQUIRED DOCUMENTS FROM DIFFERENT TYPES OF CUSTOMERS

S.No.	Type of Customer	Information/ Documents to be Obtained
1.	Individuals	<p>A photocopy of any one of the following valid identity documents;</p> <ol style="list-style-type: none"> Computerized National Identity Card (CNIC) issued by NADRA. National Identity Card for Overseas Pakistani (NICOP) issued by NADRA. Pakistan Origin Card (POC) issued by NADRA. Alien Registration Card (ARC) issued by National Aliens Registration Authority (NARA), Ministry of Interior (local currency account only). Passport; having valid visa on it or any other proof of legal stay along with passport (foreign national individuals only).
2.	Sole Proprietorship	<ol style="list-style-type: none"> Photocopy of identity document as per Sr. No. 1 above of the proprietor. Copy of registration certificate for registered concerns. Copy of certificate or proof of membership of trade bodies etc, wherever applicable. Declaration of sole proprietorship on business letter head. Account opening requisition on business letter head. Registered/ Business address.
3.	Partnership	<ol style="list-style-type: none"> Photocopies of identity documents as per Sr. No. 1 above of all the partners and authorized signatories Attested copy of 'Partnership Deed'. Attested copy of Registration Certificate with Registrar. Firms. In case the partnership is unregistered, this fact shall be clearly mentioned on the Account Opening Form. Authority letter from all partners, in original, authorizing the person(s) to operate firm's account. Registered/ Business address.

4.	Limited Companies/ Corporation	<ul style="list-style-type: none"> i. Certified copies of: <ul style="list-style-type: none"> a. Resolution of Board of Directors for opening of account specifying the person(s) authorized to open and operate the account; b. Memorandum and Articles of Association; c. Certificate of Incorporation; d. Certificate of Commencement of Business, wherever applicable; e. List of Directors in 'Form-A/Form-B' Issued under Companies Act, 2017, as applicable; and Form-29, wherever applicable.
5.	Branch Office or Liaison office of Foreign Companies	<ul style="list-style-type: none"> i. A copy of permission letter from relevant authority i-e Board of Investment. ii. Photocopies of valid passports of all the signatories of account. iii. List of directors on company letter head or prescribed format under relevant laws/regulations. iv. Registered address/ Business address where applicable. v. Branch/Liaison office address.
6.	Trust, Clubs, Societies and Associations etc.	<ul style="list-style-type: none"> i. Certified copies of: <ul style="list-style-type: none"> a. Certificate of Registration/Instrument of Trust . b. By-laws/Rules & Regulations. ii. Resolution of the Governing Body/Board of Trustees/Executive Committee, if it is ultimate governing body, for opening of account authorizing the person(s)to operate the account. iii. Photocopy of identity document as per Sr. No. 1 above of the authorized person(s) and of the members of Governing Body/Board of Trustees /Executive Committee, if it is ultimate governing body. iv. Registered address/ Business address where applicable.
7.	NGOs/NPOs/Charities	<ul style="list-style-type: none"> i. Certified copies of: <ul style="list-style-type: none"> a. Registration documents/certificate b. By-laws/Rules & Regulations ii. Resolution of the Governing Body/Board of Trustees/Executive Committee, if it is ultimate governing body, for opening of account authorizing the person(s) to operate the account. iii. Photocopy of identity document as per Sr. No. 1 above of the authorized person(s) and of the members of Governing Body/Board of Trustees /Executive Committee, if it is ultimate governing body. iv. Any other documents as deemed necessary including its annual accounts/ financial statements or disclosures in any form which may help to ascertain the detail of its activities, sources and usage of funds in order to assess the risk profile of the prospective customer. v. Registered address/ Business address.

8.	Agents	<ul style="list-style-type: none"> (i) Certified copy of 'Power of Attorney' or 'Agency Agreement'. (ii) Photocopy of identity document as per Sr. No. 1 above of the agent and principal. (iii) The relevant documents/papers from Sr. No. 2 to 7, if agent or the principal is not a natural person. (iv) Registered/ Business address
9.	Executors and Administrators	<ul style="list-style-type: none"> (i) Photocopy of identity document as per Sr. No. 1 above of the Executor/Administrator. (ii) A certified copy of Letter of Administration or Probate. (iii) Registered address/ Business address.
10.	Minor Accounts	<ul style="list-style-type: none"> (i) Photocopy of Form-B, Birth Certificate or Student ID card (as appropriate). (ii) Photocopy of identity document as per Sr. No. 1 above of the guardian of the minor.

Note:

- i. The photocopies of identity documents shall be validated through NADRA verities.
- ii. In case of a salaried person, in addition to CNIC, an attested copy of his service card or certificate or letter on letter head of the employer will be obtained.
- iii. In case of an individual with shaky/immature signatures, in addition to CNIC, a passport size photograph of the new account holder will be obtained.
- iv. In case of expired CNIC, account may be opened based on attested copies of NADRA receipt/token and expired CNIC subject to condition that "DJML" shall obtain copy of renewed CNIC of such customer within 03 months of the opening of account. For CNICs which expire during the customer's relationship, "DJML" shall design/ update their systems which can generate alerts about the expiry of CNICs at least 01 month before actual date of expiry and shall continue to take reasonable measures to immediately obtain copies of renewed CNICs, whenever expired. In this regard, "DJML" are also permitted to utilize NADRA Verity's reports of renewed CNICs and retain copies in lieu of valid copy of CNICs. However, obtaining copy of renewed CNIC as per existing instructions will continue to be permissible.

- v. In case the CNIC does not contain a photograph, “**DJML**” shall obtain following-
 - a. a duly attested copy of either driving license, service card, Nikkah-Nama, birth certificate, educational degree/certificate, pension book, insurance certificate.
 - b. a photograph duly attested by gazette officer/Administrator/ officer of the “**DJML**”.
 - c. a copy of CNIC without photograph duly attested by the same person who attested the photograph.
- vi. The condition of obtaining Board Resolution is not necessary for foreign companies/entities belonging to countries where said requirements are not enforced under their laws/regulations. However, such foreign companies will have to furnish Power of Attorney from the competent authority for establishing Business Relationship to the satisfaction of the “**DJML**”.
- vii. The condition of obtaining photocopies of identity documents of directors of Limited Companies/Corporations is relaxed in case of Government/Semi Government entities, where “**DJML**” should obtain photocopies of identity documents of only those directors and persons who are authorized to establish and maintain Business Relationship. However, “**DJML**” shall validate identity information including CNIC numbers of other directors from certified copies of ‘Form-A/Form-B’ and ‘Form 29’ and verify their particulars through NADRA Verisys. The Verisys reports should be retained on record in lieu of photocopies of identity documents.

ANNEXURE - C

RISK PROFILING OF CUSTOMER

Section A: If the response to any of the statements in Section A is "yes", the entity shall NOT establish business relationship with the client		Yes /No	Remarks
1	Customer unable to provide all the required information in relevant forms		
2	Information required to be verified as per the regulations, cannot be verified to independent and reliable documents		
3	Customer, Beneficial Owner of the customer, person acting on behalf of the customer, or connected party of the customer matches the details in the following lists: a. Proscribed under the united nations security council resolutions and adopted by the government of Pakistan; b. Proscribed under the Anti-Terrorism Act, 1997		
4	There is suspicion of money laundering and/or terrorist financing		
Section B: Customer Risk Factor			
1	Is the customer, any of the beneficial owners of the client or person acting on behalf of the customer a politically exposed person (PEP), family member of a PEP or close associate of PEP?		
2	Is the customer non-resident Pakistani?		
3	Is the customer foreign national?		
4	Is the Customer High Net Worth Individual?		
5	Legal persons: Companies Local Companies Foreign Foreign Trust or Legal arrangements Local Trust or Legal arrangements Partnerships NGOs and Charities Cooperative societies		
6	Intermediaries eg. Third parties acting on behalf of customers (Lawyers, Accountants etc.).		
7	Performed further screening of details of customer, beneficial owner of the customer, person acting on behalf of the customer, or connected party of the customer against other information sources, for example, Google, the sanctions lists published and/or other third party screening database. Are there adverse news or information arising?		
8	Customer's source of wealth/ income is high risk/ cash intensive.		
9	Does the customer have nominee shareholder(s) in the ownership chain where there is no legitimate rationale?		
10	Is the customer a shell company?		

11	Does the customer have unusual or complex shareholding structure (e.g. Involving layers of ownership structure, different jurisdictions)?		
12	Do the stated source of wealth / source of funds and the amount of money involved correspond with what you know of your customer?		
Section C: Country / Geographic Risk Factors			
1	<p>Is the customer, beneficial owner of the customer or person acting on behalf of the customer from or based in a country or jurisdiction:</p> <p>a. Identified as High-risk jurisdiction by the FATF and for which financial institutions should give special attention to business relationships and transactions. (Countries having weak governance, law enforcement, and regulatory regimes).</p> <p>b. Countries subject to sanctions, embargos or similar measures issued by international authorities (E.G. UN, WB, IMF)</p> <p>c. Countries where protection for customer's privacy prevents effective implementation of AML/CFT requirements and/or facilitates the framework for establishment of shell-companies.</p> <p>d. Countries/ Geographies identified by recognized sources as having significant levels of organized crime, corruption or criminal activity.</p> <p>e. Countries/ Geographies identified by recognized sources as providing funding or support for terrorist activities or have terrorist organizations operating within them.</p>		
Section D: Services / Transaction Risk Factors			
1	Is the business relationship with the customer established through non face-to-face channel?		
2	Has the customer given any instruction to perform a transaction (which may include cash) anonymously?		
3	Has the customer transferred any funds without the provision of underlying services or transactions?		
4	Are there unusual patterns of transactions that have no apparent economic purpose or cash payments that are large in amount, in which disbursement would have been normally made by other modes of payment (such as cheque, bank drafts etc.)?		
5	Are there unaccounted payments received from unknown or unassociated third parties for services and/or transactions provided by the customer?		
6	Does the value of the transaction appear to fall within the financial means of your customer, given their income and savings?		
7	Is there any divergence in the type, volume or frequency of services and/or transactions expected in the course of the business relationship with the customer?		
8	Significant and unexplained geographic distance between residence or business location of the customer and the location where the product sale took place (or the location of the insurer's representative)		
9	Customers seek or accept very unfavorable account/policy/contract provisions or riders and rely on free look up provisions		
10	Customers transfer the benefit of a product to an apparently unrelated third party		



DJM Securities Limited

11	Customer uses brokerage accounts as long term depository accounts for funds		
12	Customer is conducting transactions that do not have apparent economic rationale		
13	Transactions appear to be undertaken in a structured, sequential manner in order to avoid transaction monitoring/ reporting Thresholds		
14	Transactions involve penny/microcap stocks		
15	Transfers are made to the same person from different individuals or to different persons from the same individual with no reasonable explanation		
16	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		
17	Unusually large aggregate wire transfers or high volume or frequency of transactions are made with no logical or apparent reason		
18	Customer trades frequently, selling at a loss		
19	Customer invests in securities suddenly in large volumes, deviating from previous transactional activity		
20	Cross border correspondent financial institutions relationships		
21	Products/ Services		
22	Transaction Amount		



DJM SECURITIES LIMITED

TREC Holder: The Pakistan Stock Exchange
 Suite # 203, 2nd Floor, Business & Finance Trade Centre, I.I. Chundrigar Road, Karachi-Pakistan,
 Ph: 021-32472030-5 Lines, Fax: 021-32472044
 url: www.djmtrade.com Email: info@djmtrade.com

Please use BLOCK LETTERS to fill the form

KNOW YOUR CUSTOMER (KYC) APPLICATION FORM				CORPORATE
A. REGISTRATION (AND OTHER) DETAILS OF CUSTOMER				
1. Full name of Customer <small>(As per constitutive documents)</small>				
2. Date of Incorporation:		3. Incorporation Number:		4. Place of Incorporation:
5. Date of Commencement of Business:			6. National Tax No. <small>(For exempted entities, reporting investment income as provided under or interpreted in, where and how set out by section 177B)</small>	
7. Industry / Sector:				
8. Registration Number / Unique Identification Number ("UIN"):				
9. Details of Contact Person of the Customer: <small>(This is only for an official representative of the Customer)</small>				
(a) Name Mr./Mrs./Ms.:				
(b) Association of the Attorney with the Customer:				
(c) Address:				
(d) CNIC/SPIC/NICOP/ARC/POC No.:				
(e) Expiry date of CNIC/SPIC/NICOP/ARC/POC:			(f) Designation of the official:	
(g) Tel. (Off.):	(h) Mobile:	(i) Fax:	(j) E-mail:	
(k) Passport details: <small>(For a passport of a non-Northern Pakistan)</small>	Passport No.:	Place of Issue:	Date of Issue:	Date of Expiry:
B. ADDRESS DETAILS OF CUSTOMER				
1. (a) Mailing Address:				
City/Town/Village:		Province/State:		Country:
(b) Tel. (Off.):	(c) Mobile:	(d) Fax:		(e) E-mail:
Specify the proof of address submitted for mailing address:				
2. (a) Registered Address:				
City/Town/Village:		Province/State:		Country:
(b) Tel. (Off.):	(c) Mobile:	(d) Fax:		(e) E-mail:
Specify the proof of address submitted for registered address:				
C. OTHER DETAILS				
1. Expected Annual Income:				
2. Net-equity / net-assets as on (date) _____ : _____				
3. Share holder's Category: <small>(Please tick (✓) the appropriate box)</small>	<input type="checkbox"/>	Investment Company	<input type="checkbox"/>	Moderata
	<input type="checkbox"/>	Insurance Company	<input type="checkbox"/>	Moderata Management Company
	<input type="checkbox"/>	Charitable Trust	<input type="checkbox"/>	Co-operative Society
	<input type="checkbox"/>	Leasing Company	<input type="checkbox"/>	Mutual Fund
	<input type="checkbox"/>	Bank/Financial Institution	<input type="checkbox"/>	Other (Please specify)
	<input type="checkbox"/>	Joint Stock Company	<input type="checkbox"/>	

1

KYC/CDD

D. BANK DETAILS**		
Bank Name:	IBAN No.:	
E. DECLARATION		
<p>I/we hereby confirm that all the information furnished above is true and correct to the best of my/our knowledge and belief and I/we undertake to inform you of any changes therein, immediately, in case any of the above information is found to be untrue or false or misleading or misrepresenting. I/we am/are aware that I/we may be held liable for it.</p>		
Signature of the Authorized Person	Date: _____ (dd/mm/yyyy)	
FOR OFFICE USE ONLY		
Signature of the Authorized Signatory	Date	Seal/Stamp of the Authorized Intermediary
<p>* Optional ** IBAN shall be mandatory for all corporate entities subject to any exception available under applicable laws, rules, regulations etc.</p>		

Terms & Conditions of the KYC Application Form:

- All terms herein shall, unless expressly stated otherwise, have the same meaning as ascribed to them in the Centralized KYC Organization Regulations.
- The information provided in KYC application form and/or CRF shall be in addition to and not in derogation of the requirements prescribed under Anti-Money Laundering and Countering Financing of Terrorism Regulations, 2018.
- All correspondence shall be sent by CKO at the mailing address and/or email address of the Customer, as stated on the KYC Application Form.
- Neither the CKO nor its directors, officers, employees or agents shall be liable for losses, damages, liabilities, costs or expenses suffered or incurred by the Customer as a result of providing its KYC Information to Authorized Intermediaries or the CKO due to any reasons whatsoever including its unauthorized disclosure.
- The Customer undertakes to indemnify the CKO against any losses, damages, liabilities, costs or expenses suffered or incurred by CKO, including any legal costs and claims by third parties, as a result of any inaccuracy, misrepresentation, misstatement or incorrect details in the information supplied by the Customer or any omission in such information or any other contravention or violation of the Centralized KYC Organization Regulations.
- The Customer agrees that in the event that it does not abide by the timelines prescribed in the Centralized KYC Organization Regulations for submission of information and confirmation to the CKO, the CKO shall be authorized to take action as prescribed in the Centralized KYC Organization Regulations. The Customer undertakes that it shall hold CKO harmless and that CKO shall not be liable for any losses, damages, liabilities, costs or expenses suffered or incurred by the Customer as a result of such actions.
- The Customer agrees that CKO may hold, store and process its KYC Information on the KYC Information System and KYC Database in connection with its KYC functions under the Centralized KYC Organization Regulations. The Customer also agrees that CKO may disclose its KYC Information as permitted under the CKO Regulations and such other disclosures as may be reasonably necessary for compliance with any other laws or regulatory requirements.
- The Customer acknowledges that KYC Information System and KYC Database, including but not limited to all the information contained therein is the legal property of CKO.
- The Authorized Intermediaries agree to pay CKO the fees and charges as prescribed by CKO from time to time in respect of its KYC functions.
- CKO has absolute discretion to amend or supplement any of the terms and conditions at any time and will endeavor to give prior notice of fifteen days wherever feasible for such changes.
- The Customer agrees and affirms that it shall be bound by and acts in accordance with the provisions of the Centralized KYC Organization Regulations.
- These terms and conditions shall be governed by the laws of Pakistan.



DJM SECURITIES LIMITED

TREC Holder: The Pakistan Stock Exchange
 Suite # 203, 2nd Floor, Business & Finance Trade Centre, I.I. Chundrigar Road, Karachi-Pakistan.
 Ph: 021-32472030 - Lines, Fax: 021-32472044

url: www.djmtrade.com Email: info@djmtrade.com

Please use BLOCK LETTERS to fill the form

KNOW YOUR CUSTOMER (KYC) APPLICATION FORM		INDIVIDUALS	
A. IDENTITY DETAILS OF APPLICANT			
1. Full name of Applicant Mr. / Mrs. / Ms. <small>(As per CNIC/SNIC/NCOP/ARC/POC/Passport)</small>			
2. Father's / Husband's Name:			
3. a. Nationality:	b. Marital status: <input type="checkbox"/> Single <input type="checkbox"/> Married	c. Status: <input type="checkbox"/> Resident <input type="checkbox"/> Non-Resident	
4. a. CNIC/ SNIC/NCOP/ARC/POC No:			
b. Expiry date:			
5. Passport details: <small>(For a foreigner or a non-resident Pakistani)</small>		Passport Number:	Place of Issue:
		Date of Issue:	Date of Expiry:
6. Date of Birth			
B. ADDRESS DETAILS OF APPLICANT			
1. (a) Mailing Address: <small>(Address should be different from registered intermediary business address except for employees of authorized)</small>			
	City/Town/Village:	Province/State:	Country:
(b) Tel. (DR):	(c) Tel. (Res.):	(d) Mobile:	(e) Fax:
(f) Email:			
Specify the proof of address submitted for mailing address:			
2. (a) Permanent Address: <small>(Mandatory for all applicants & not if different from mailing address)</small>			
	City/Town/Village:	Province/State:	Country:
(b) Tel. (DR):	(c) Tel. (Res.):	(d) Mobile:	(e) Fax:
(f) Email (if any):			
Specify the proof of address submitted for permanent address:			
C. OTHER DETAILS			
1. Gross Annual Income Details (please specify): <input type="checkbox"/> Up to Rs. 100,000 <input type="checkbox"/> Rs. 250,001 - Rs. 500,000 <input type="checkbox"/> Rs. 1,000,001 - Rs. 2,500,000 <input type="checkbox"/> Rs. 100,001 - Rs. 250,000 <input type="checkbox"/> Rs. 500,001 - Rs. 1,000,000 <input type="checkbox"/> Above Rs 2,500,000			
2. Source of Income:			
3. Shareholder's / Unit Holder's Category: INDIVIDUAL			
4. (a) Occupation: <small>(Please tick (✓) the appropriate box)</small>	<input type="checkbox"/> Agriculturist	<input type="checkbox"/> Business	<input type="checkbox"/> House wife
	<input type="checkbox"/> Retired Person	<input type="checkbox"/> Student	<input type="checkbox"/> Business Executive
	<input type="checkbox"/> Professional	<input type="checkbox"/> Service	<input type="checkbox"/> Govt./Public Sector
			<input type="checkbox"/> Household <input type="checkbox"/> Industrialist <input type="checkbox"/> Others (Specify)
(b) Name of Employer / Business: <small>(Exclude name of employer/owner/company)</small>		(c) Job Title / Designation:	(d) Department:
(e) Address of Employer / Business:			

KYC/CDD

D. BANK DETAILS***		
Bank Name:	IBAN No.:	
E. DECLARATION		
I hereby confirm that all the information furnished above is true and correct to the best of my knowledge and belief and I understand that in case any of the above information is found to be untrue or false or misleading or misrepresenting, I shall be held liable for it.		
Signature of the Applicant	Date	Signature of the Applicant as per CNIC/SMC/NICOP/ARC/POC/Passport No. (Only applicable if Applicant signature is different)
FOR OFFICE USE ONLY		
Authorized Signatory	Date	Seal/Stamp of the Authorized Intermediary

* Optional

** For NICOP/ARC/POC/Passport, Email is mandatory and Mobile Number is Optional. Whereas for CNIC/SMC, Mobile Number is Mandatory and Email is Optional, In case of SMC where country of stay is not Pakistan, email will be mandatory.

*** IBAN shall be mandatory for all customers subject to any exception available under applicable laws, rules, reg.

Terms & Conditions of the KYC Application Form:

- All terms herein shall, unless expressly stated otherwise, have the same meaning as ascribed to them in the Centralized KYC Organization Regulations.
- The information provided in KYC application form and/or CRF shall be in addition to and not in derogation of the requirements prescribed under Anti-Money Laundering and Countering Financing of Terrorism Regulations, 2018.
- All correspondence shall be sent by CKO at the mailing address and/or email address of the Customer, as stated on the KYC Application Form.
- Neither the CKO nor its directors, officers, employees or agents shall be liable for losses, damages, liabilities, costs or expenses suffered or incurred by the Customer as a result of providing its KYC information to Authorized Intermediaries or the CKO due to any reasons whatsoever including its unauthorized disclosure.
- The Customer undertakes to indemnify the CKO against any losses, damages, liabilities, costs or expenses suffered or incurred by CKO, including any legal costs and claims by third parties, as a result of any inaccuracy, misrepresentation, misstatement or incorrect details in the information supplied by the Customer or any omission in such information or any other contravention or violation of the Centralized KYC Organization Regulations.
- The Customer agrees that in the event that he does not abide by the timelines prescribed in the Centralized KYC Organization Regulations for submission of information and confirmation to the NCCPL, the NCCPL shall be authorized to take action as prescribed in the Centralized KYC Organization Regulations. The Customer undertakes that it shall hold CKO harmless and that CKO shall not be liable for any losses, damages, liabilities, costs or expenses suffered or incurred by the Customer as a result of such actions.
- The Customer agrees that CKO may hold, store and process its KYC information on the KYC Information System and KYC Database in connection with its KYC functions under the Centralized KYC Organization Regulations. The Customer also agrees that CKO may disclose its KYC information as permitted under the CKO Regulations and such other disclosures as may be reasonably necessary for compliance with any other laws or regulatory requirements.
- The Customer acknowledges that KYC Information System and KYC Database, including but not limited to all the information contained therein is the legal property of CKO.
- The Authorized Intermediaries agree to pay CKO the fees and charges as prescribed by CKO from time to time in respect of its KYC functions.
- CKO has absolute discretion to amend or supplement any of the terms and conditions at anytime and will endeavor to give prior notice of fifteen days wherever feasible for such changes.
- The Customer agrees and affirms that it shall be bound by and acts in accordance with the provisions of the Centralized KYC Organization Regulations.
- These terms and conditions shall be governed by the laws of Pakistan.