

**ANTI-MONEY LAUNDERING & COUNTERING
FINANCING OF TERRORISM**

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

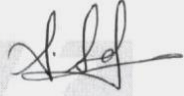
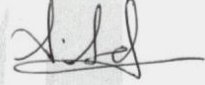
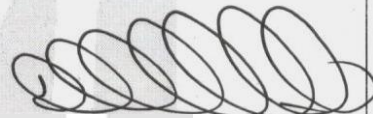
Description	Name / Designation	Signature
Drafted by	Compliance Manager	
Review and finalization by	Compliance Manager	
Approved by	Chief Executive Officer	
First Amendment	N/A	N/A
Second Amendment	N/A	N/A

Table of Contents

GLOSSARY	4
ABOUT DJM SECURITIES PRIVATE LIMITED	5
BACK GROUND	5
GOALS & OBJECTIVES	6
SCOPE.....	6
REGULATORY OVERSIGHT & COMPLIANCE RISK.....	7
AML/CFT & KYC/CDD POLICIES AND PROCEDURES	8
MONITORING AND REPORTING OF SUSPICIOUS TRANSACTION / ACTIVITIES.....	13
ACCOUNTABILITIES AND RESPONSIBILITIES	14
INTERNAL AUDIT.....	14
ANNEXURE – A.....	15
Warning Signs/ Red Flags.....	15
ANNEXURE – B.....	16
LIST OF REQUIRED DOCUMENTS FROM DIFFERENT TYPES OF CUSTOMERS	16
RISK PROFILING OF CUSTOMER.....	20
KNOW YOUR CLIENT (KYC) APPLICATION FORM.....	23

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

ABOUT DJM SECURITIES PRIVATE LIMITED

DJM Securities (Private) Limited was established in June 17, 2002 under the Companies Ordinance of 1984 to provide specialized financial services to both the institutional and private sector in the area of both local and international equity and future markets. **DJM Securities (Private) Limited** is a TREC Holders: Pakistan Stock Exchange Limited and brings, through its team of highly experienced, trained and qualified management, a personal and pro-active style of advisory services with a view to both educate and serve the ever evolving needs of our clients

BACK GROUND

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 **ANTIMONEY 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.

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

SCOPE

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) Customer Identification
- b) Risk assessment of customer
- c) Circumstances where Enhanced Due Diligence is required
- d) On-going due Diligence
- e) Circumstances where simplified Due Diligence can be adopted
- f) Compliance function
- g) Data retention
- h) Training and employee screening

a) 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

b) 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.

c) Enhanced Due Diligence

Once a customer has been categorized as HIGH RISK, it is necessary to have Enhanced Due Diligence (EDD) when dealing with such a customer. Activities and transactions of HIGH-RISK customers shall be monitored, and any unusual transactions shall be reported in suspicious transaction report.

- When dealing with high-risk customers, including Politically Exposed Persons (PEP's), senior management' approval shall be obtained to establish business relationships with such customers. The same shall also apply in case of an existing customer which will be classified as high-risk pursuant to these policies or which will be subsequently classified as a result of ongoing due diligence. Further, reasonable measures shall be taken to establish the source of wealth and source of funds.
- If it is not possible to comply with the above requirements, the account will not be opened, and business relationship shall be terminated, suspicious. Also, transaction report shall be submitted.
- When it will be not possible to identify and verify the identity of the customer and the beneficial owner or will be not possible to obtain adequate information regarding the purpose and intended nature of the customer relationship, account shall not be opened, customer relationship shall not be commenced or in the case of an existing customer relationship shall be terminated and filing of a Suspicious Transaction Report shall be considered.

d) 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.

e) 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.

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.

f) Compliance Function

- A compliance function shall be established with suitable individual resource and MIS reporting capabilities, enabling it to efficiently monitor the customers' transactions and make timely reports.
- The Head of Compliance function shall have skills and experience necessary for satisfactory performance. Head of Compliance shall be independent and report directly to the Board of Directors.
- The Compliance function shall ensure compliance with the requirements of these policies as well as other regulatory requirements related under the applicable legal framework. A record shall be maintained of all non-compliance identified and reported to the BoD and must be available for the inspection of SECP as and when required.

g) 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.

h) 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.



MONITORING AND REPORTING OF SUSPICIOUS TRANSACTION / 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.

1. NON COMPLIANCE

Failure to abide by the Policy set by “DJML” to prevent money laundering and terrorist financing will be treated as a disciplinary issue. Any deliberate breach will be viewed as severe misconduct. Such cases will be referred to HR for onward initiation of disciplinary action that could lead to termination of employment and could also result in criminal prosecution and imprisonment for the concerned staff member.

2. RECORD RETENTION

It is a Policy of DJML:

- To retain identification and transaction documentation for the minimum period as required by applicable Laws and Regulations.
- To retain records of all suspicious activity reports made by Compliance department to Regulators for an indefinite period unless advised by the Regulator otherwise.
- To be able to retrieve, records that are required by law enforcement agencies as part of their investigations.

To keep records of KYC&CDD, AML/CFT training provided to the employees, nature of the training and the names of staff who received such training.

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.

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-MoneyLaundering 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.

<p>4.</p>	<p>Limited Companies/ Corporations</p>	<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 b. account specifying the person(s) authorized to c. open and operate the account; d. Memorandum and Articles of Association; e. Certificate of Incorporation; f. Certificate of Commencement of Business, wherever applicable; g. List of Directors on 'Form-A/Form-B' issued under Companies Act, 2017, as applicable; and h. Form-29, wherever applicable. ii. Photocopies of identity documents as per Sr. No. 1 above of all the directors and persons authorized to open and operate the account;
<p>5.</p>	<p>Branch Office or Liaison Office of Foreign Companies</p>	<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.
<p>6.</p>	<p>Trust, Clubs, Societies and Associations etc.</p>	<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.

<p>7.</p>	<p>NGOs/NPOs/Charities</p>	<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.
<p>8.</p>	<p>Agents</p>	<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.
<p>9.</p>	<p>Executors and Administrators</p>	<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.
<p>10.</p>	<p>Minor Accounts</p>	<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 / Transactions 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	
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		

To Be Implemented Starting 01-April-2019 *

KNOW YOUR CLIENT (KYC) APPLICATION FORM

<http://djtrade.com/wp-content/uploads/2019/03/KNOW-YOUR-CLIENT-KYC-APPLICATION-FORM.pdf>



*Subject to SECP Approval