SOS CAPITAL LIMITED

Name :	**KYC / AML / CFT Policy**
Classification :	**Confidential**
Prepared By :	**Compliance Division**
Prepared Date :	**December – 2024**
Version :	**1.0**
Approved By :	**Board of Directors**

PURPOSE

Formulation and revision of this policy is in line with requirements of Anti-Money Laundering (AML) Act 2010, Anti-Terrorism Act (ATA) 1997 and applicable SECP [Anti Money Laundering, Combating the Financing of Terrorism and Countering Proliferation Financing) Regulations, 2020 [**"AML/CFT/CPF Regulations"**], SECP Guidelines on Anti-Money Laundering, Countering Financing of Terrorism and Proliferation Financing **(updated April 2020) ["SECP Guidelines on AML/CFT/CPF Regulations"]** and Sanitized Version of NRA 2023 issued on 29th November 2023 [**"NRA 2023"]**.

The SOS Capital required to manage these risks throughout the life cycle of its customers related to channels/products/jurisdictions/services and relationships, starting from onboarding of new business relationships till closure as well as for all walk in or occasional customers.

In addition to the above, the international AML / CFT standards such as Financial Action Task Force (FATF) and Asia Pacific Group (APG) on Money Laundering on Customer Due Diligence, and United Nations (UN) resolutions concerning sanctions are to be followed to prevent the possible use of the Broker as a conduit for money laundering or terrorist financing activities.

To further strengthen the regulatory framework to curb Money Laundering, Terrorist Financing and Proliferation Financing, the SECP has updated AML/CFT/CPF Regulations and its subsequent amendments from time to time, covering the following aspects:

BRIEF ON SECP AML/CFT REGULATIONS:

Regulation	Areas Covered
CHAPTER II RISK ASSESSMENT AND MITIGATION	
Risk Assessment; Risk Mitigation and Applying Risk Based-Approach; New Products, Practices and Techniques' Customer Due Diligence (CDD); Beneficial Ownership of Legal Person and Legal Arrangements; Identification of Beneficiary for Life Insurance or Takaful Polices; Enhanced Due Diligence (EDD); Politically Exposed Persons (PEP); Simplified Due Diligence (SDD); Reliance on Third Parties; Ongoing Monitoring; Reporting of Transactions (STRs/CTRs); and Counter Measures against High Risk Countries.	
Regulation-4 Risk Assessment	Identifying, assessing and understanding Money Laundering (ML)/Terrorism Financing (TF Risks in relation to customers, their jurisdiction or countries, jurisdictions or countries we have operations or dealings in, products, services, transactions and delivery channels we offering. This regulation also prescribes appropriate steps for identifying, assessing and understanding ML/TF Risks.
Regulation-5 Risk Mitigation and Applying Risk Based Approach	Implementation of counter ML and TF measures to ML and TF Risk with respect to size of business, developing and implementing policies, procedures and controls duly approved by the Board, monitoring the implementation, performing enhanced measures to manage and mitigate High Risk if identified, need of independent audit function to test the system.
Regulation-7 New Products, Practices and Technologies	Identification and assessing ML and TF Risk that may arise in relation to New Products and Business Practices, use of new or developing technologies. This Regulation prescribes undertaking risk assessment prior to launch of products, practices and technologies and taking measures to manage and mitigate their risks. The Regulation also covers paying special attention to new products, business practices and new technologies that favor anonymity.

CUSTOMER DUE DILIGENCE (CDD) AND BENEFICIAL OWNERSHIP	
Regulation -8 **Customer Due Diligence**	CDD measures for Identifying and Verifying New and Existing Customers and/or beneficial owners on the basis of documents, data or information obtained from customer and/or from independent sources before, during or after course of establishing a business relationship. CDD measures for understanding and obtaining information on the purpose and intended nature of business relationship. CDD measures also include monitoring of accounts/transactions on ongoing basis to ensure that these being conducted are consistent with our knowledge of customer, his business and risk profile including his source of funds and data/information for taking prompt action in case of material departure from usual and expected activity. This Regulation covers the requirement of documents as per Annexure-I. Prohibitions from establishing business relationship with entities and /or individuals that are DESIGNATED under UNSCR adopted by Govt. of Pakistan, PROSCRIBED under Anti-Terrorism Act, 1997 and associates /facilitators of DESIGNATED / PROSCRIBED entities/individuals. Steps to determine the Person acting on behalf of a Customer including Authority, Identification and Verification of Authorized Person and the Customer. Categorization of customers as High or Low Risk as outcome of CDD. Maintaining list of Customers/Accounts where business relationships were refused or needed to be closed on Negative Verification. Non-satisfactorily CDD measures, account shall be closed or business relationship terminated and considering to warrant STR. Doubt of tipping-off the Customer due to CDD measure, filing STR without CDD process. Govt. entities accounts to be opened on their own names operated by officers on production of Special Resolution or Authority from concerned Admin Dept. or Ministry duly endorsed by MoF or Finance Dept./Division of concerned Govt.

Regulations- 13, 14, 16 & 17 **Beneficial Ownership of Legal Persons and Legal Arrangements.**	Acquisition and usage of information and data from reliable sources for a Legal Person for following CDD measures/purposes: - • Understanding its business nature, ownership and control structure; • Identifying and verifying identity of Natural Person who owns or ultimately has controlling ownership interest in Legal Person. • Where no Natural Persons are identified, identify the Natural Person having Executive Authority or equivalent or similar positions in the Legal Person. Acquisition and usage of information and data from reliable sources for a Legal Arrangement for following CDD measures/purposes: - • For Trusts, identification and verification of identity of the settler, the trustee, the protector, the beneficiaries and Natural Person exercising ultimate ownership and control over the Trust. • For other type, identification and verification of identity of the Natural Person having ultimate ownership and control over such Legal Arrangement.
Regulation – 19 **Ongoing Monitoring including STRs and CTRs**	• Consistency of Transactions and the Knowledge of Customer, its business and risk profile and source of funds (where appropriate). • Obtaining information and examine the background and purpose of all complex and unusual transactions having no apparent economic or visible lawful purpose and background. • Periodic review of information and beneficial owners and ensuring them up to date and relevant, by reviewing existing records, particularly of High-Risk Customer. • Revision of Customers' profiles keeping in view the spirit of KYC/CDD and bases to be documented. • Filing of STR on reasonable grounds for suspension, SOS Capital may consider to retain the customer: o To substantial and document the reasons o Proportionate risk mitigation measures including Enhanced Ongoing monitoring. • Freezing of funds and assets of Designated/Proscribed entity/individual by UNSCR and Anti-Terrorist Act and their associates/facilitators and reporting to Commission. **Suspicious Transaction Reports (STRs) and Currency Transaction Reports (CTRs).** • Guidelines for Reporting of Complex, Unusually Large, and out of pattern Transactions and Currency Transactions.
Regulation 20 **Existing Customers**	• CDD Requirements of Existing Customers on the basis of Materiality and Risk. • Blocking of Account of the customers, if customers fail to provide information / documents within One Month of the Notice. • Activation of In-active / Dormant Account subject to conduct of NADRA Verisys or Bio-metric verification and after obtaining attested copy of customers' valid identity documents.

Regulation – 21 **Enhanced Due Diligence (EDD) &** **Politically Exposed Persons (PEPs) and their Close Associates**	• Requirement of implementing Internal Risk Management Systems, Policies, Procedures and Controls for Customer having High Risk of ML/TF. • Circumstances where Customer presents High Risk of ML/TF also include: o Customers belonging to non-compliant countries with AML Regulations according to FATF. o Body corporate, partnerships, associations and Legal Arrangements including NGOs and NPOs which receive donations. o Legal Person or Arrangement with complex ownership structure. • EDD measures in proportionate to risk posed to business relationship by Customer having High Risk or notified as having High Risk by SECP. • EDD measures include approval from Senior Management, establishing the Source of Wealth and/or Funds or Beneficial Ownership of Funds, enhanced monitoring of business relationship. • Requirement of Internal Risk Management Systems, Policies, Procedures and Controls for determining a Customer as PEP. • EDD Measures include approval from Senior Management, establishing the Source of Wealth and/or Funds or Beneficial Ownership of Funds, enhanced monitoring of business relationship for: - o In case of foreign PEPs; and o In case of domestic PEPs posing High Risk in business relationship in addition to other requirement of these regulations. • EDD Measures are applicable on family members and close associates of all PEPs.
Regulation – 22 **Counter Measures Against High-Risk Countries**	Adoption of counter measures including EDD proportionate to the Risk, to the business relationship and transactions with Customers belonging to High-Risk Countries called by FATF and/or notified by Fed. Govt.
Regulation - 23 **Simplified Due Diligence**	Where Low Risk is identified through risk analysis and adequate checks and controls, SDD or reduced CDD / KYC measures: - • Decision to rate Low Risk a customer to justified in writing. • Low Risk cases may include: o SOS Capital subject to combat ML and TF requirements consistent with FATF recommendations and supervised. o Public Listed companies. o Pension superannuation or similar scheme providing retirement benefits to employees. o Financial products or services. • SDD measures include reducing identification updates, degree of ongoing monitoring and scrutinizing transactions and non-collection of specific information.

Regulation – 24 **Reliance on Third Parties**	• Obtaining of identification information, beneficial ownership and/or business nature. • Provision of copies of identification data and other documents relating CDD requirement without delay. • Third party is regulated and supervised or monitored for. • Confidentiality and non-disclose agreement. • In case of third party of same financial group, CDD and record-keeping requirements and programs against ML and TF. • Ongoing monitoring and ultimate responsibility of AML/CFT obligation.
TFS OBLIGATIONS	
Regulation – 25 **TFS Obligation**	Undertaking TFS obligations under United Nations (Securities Council) Act 1948 and /or Anti-Terrorism Act 1997 and Regulations made there under including: • Develop mechanism, process and procedures for screening and monitoring customer, potential customers and their BOs/Associates to detect any matches or potential matches for designated / proscribed persons. • In case of positive or potential match, SOS Capital shall immediately: i. Freeze relevant funds and assets, block transaction without prior notice; ii. Prohibit from making any funds or other assets, economic resources, or financial and other services and funds; iii. Reject the transaction or attempted transactions or the customer. iv. File a STR to FMU and notify the Commission; v. Implement any other obligation under AML Act 2010, UNSC Act and Anti-Terrorism Act and any other regulations made thee under. • The SOS Capital is prohibited, ongoing basis, for providing financial services to proscribed /designated entities and person or those who are known for their association with such entities and persons.
CHAPTER III **RECORD KEEPING**	
Regulation– 26 **Record Keeping**	Maintenance & Retention of Customer and Transactions related records for minimum period of five (5) years from completion of the transaction. Ensure of timely making available, all CDD and transaction record to Commission, FMU and LEAs, whenever required.
COMPLIANCE PROGRAM	
Regulation – 27 **Compliance Program including screening and training of employees.**	• Mandatory need for appointment of management level Compliance Officer (CO), reportable to the Board or to another equivalent executive position or committee; • Timely access of customers' record and relevant information. • Responsibilities of CO. • Screening procedures for hiring Employees. • Comprehensive Employee due diligence. • Suitable training program for relevant employees on annual basis.

Regulation – 28 Corporate Groups	Group-wise programs against AML/CFT which include the following measures: • Policies and procedures for sharing information for CDD and ML/TF Risks management. • Group-level compliance, audit and/or AML/CFT functions, for customers, accounts and transactions. • Adequate safeguard on confidentiality and use of information.
Regulation – 29 Foreign Branches including Financial Group	• Need for paying attention to foreign branches and subsidiaries which do not or insufficiently comply with FATF recommendations. • In case of difference in AML/CFT requirements in both jurisdictions, apply higher of two standards. • In case of conflict and inability to fully observe High Standards, SOS Capital shall report to Commission.
Regulation – 30 Correspondent Relationship	Measures to performed when forming a correspondent relationship: • Assessing the suitability of respondent FI; • Understanding and documenting the respective AML/CFT responsibilities of FI and respondent FI. • Accessing respondent FI in context of sanctions/embargoes and Advisories about risk; • Approval from Senior Management before providing correspondent service to new FI. • Documentation of the basis of satisfaction. • Not entering or continuing correspondent relationship with Shell FI.

SECP GUIDELINES FOR IMPLEMENTING AML/CFT REGULATIONS:

FIRST VERSION OF SECP GUIDELINES ON ANTI-MONEY LAUNDERING, COUNTERING FINANCING OF TERRORISM, AND PROLIFERATION FINANCING, 2018

In addition to the AML/CFT Regulations, the SECP issued its first Guidelines on September 18, 2018, on Implementation of AML/CFT Framework under the Securities and Exchange Commission of Pakistan (Anti Money Laundering and Countering Financing of Terrorism) Regulations, 2018, to strengthen trade related Anti Money Laundering/Countering Financing of Terrorism (AML/CFT) regime and restrict possible misuse of Brokerage Industries in order to accelerate the level of outreach for achieving the objective of financial inclusion and strengthening the controls related to Money Laundering (ML)/ Terrorist Financing (TF) risks.

SECOND VERSION OF SECP GUIDELINES ON ANTI-MONEY LAUNDERING, COUNTERING FINANCING OF TERRORISM, AND PROLIFERATION FINANCING, 2020

The SECP has revised its Guidelines in line with amendments incorporated in SECP AML/CFT Regulations and review of the latest National Risk Assessment of Pakistan in 2019 ("**NRA 2019**").

a) According to NRA 2019, Regulated Person should have policies and procedures to prevent the misuse of technological development in ML/TF scheme, and to avoid or mitigate all technologies that favor anonymity. NRA 2019 suggested limitations on the use of non-face to face business, or on virtual business to avoid opening up of alternative possibilities for ML/TF and fraud, especially High-Risk industries such as Brokerage.

b) NRA 2019 has determined the risk of corruption and therefore the risk of providing financial services to Politically Exposed Persons ("PEPs") is high. As per NRA 2019, all domestic PEPs must be scrutinized, particularly for their source of funds wealth and assets.

c) Both by international standards and in Pakistan's National Risk Assessment, Non-Profit Organizations ("NPOs") are classified as a High Risk Sector for TF.

d) Conduct Simplified Due Diligence (SDD) in case of lower risks identified by them in line with NRA 2019. Pay particular attention to the level of risk assigned to the relevant sector, type of Customer or activity as mentioned in NRA 2019.

e) Consider guidance material to determine the level of risk involved in relation to Customers, Products/Services, Delivery Channels and Countries/Region provide in NRA 2019.

f) For low risk environment, asses risk by only considering the Likelihood of ML/TF/PF activity involving its identification combined with business experience, and guidance available through SECP, NRA 2019, and FATF.

g) Regulated Person should have appropriate policies, procedures and controls that enable them to manage and mitigate effectively the inherent risks that they may identified, including risk identified in NRA 2019.

NATIONAL RISK ASSESSMENT 2023 [NRA 2023]

SECP provided the findings of the Pakistan's National Risk Assessment 2023 to the readers in a brief form. The purpose of summarized version of NRA 2023 was to provide guidance to the relevant stakeholders so that they can better understand their ML/TF risks and improve their AML/CFT controls. The SOS Capital subject to Pakistan's AML/CFT laws are expected to use the findings of NRA 2023 to update its Internal Risk Assessment Documents / Standard Operating Procedures in accordance with the findings of NRA 2023 and utilize its resources accordingly.

The NRA 2023 incorporated enhanced understanding, resulting in updated risk assessments. The NRA 2023 updates Pakistan's ML/TF risk profile using in-house methodology aligned with international best practices and FATF recommendations. As per the adopted methodology in NRA 2023, 04 rating scales used to assess the risks of ML/TF threats and vulnerabilities included **"Very High", "High", "Medium" and "Low".** It is important to note that low risk doesn't mean that no action is required; rather, as required by law, SOS Capital needs to take sufficient measures and adopt controls related to the low-risk items also.

The following are main features of NRA 2023:

a) Identified twenty-one (21) Predicate Offences and rated them in four (4) ML Threats Rating Scales i.e., Very-High (**VH**), High (**H**), Medium (**M**) and Low(**L**);

b) Identify the Key Sources and Channels used for potential ML Activities;

c) Similarly identified eighty-seven (87) Terrorist Organizations ("**TOs"**) in Pakistan;

d) Considered four (4) TOs as VH risk, eight (8) as H risk, seven (7) as M risk and remaining 689 as L Risk.

e) Identified the Key Sources and Channel may be exploited for TF with their TF Threats Rating Scales i.e., Very-High (**VH**), High (**H**), Medium (**M**) and Low (**L**).

In addition to assessing ML and TF related threats, NRA 2023 also assessed how vulnerable different financial and DNFBP sectors were to ML and TF. While conducting the **Inherent Sectorial Vulnerability Assessment**, Financial Sector, Designated Non-Financial Businesses & Professions (**"DNFBPs"**) and Legal Persons and Legal Arrangements (**"LPLAs"**) were also examined and the following Inherent Vulnerability Relating of the Financial Sectors were revised:

a) Revised NRA 2023 risk Rating from Low to Very High, wherein the Banks are rated Very High from High and Securities Brokers are rated Medium from Low, etc;

b) Identified and revised Risk Rating of Designated Non-Financial Businesses & Professionals ("DNFBP") from low to Very High Risk Rating, wherein, Real Estate Agents were rated as Very High risk and Dealers in Precious Metals & Stones ("DPMS") were maintained at High, Lawyers, Accountants, Trust and Companies Services Providers ("TCSPs") were rated Low from High;

c) Private Limited and Foreign Companies were rated from High risk to Very High risk.

d) Trusts and WAQFS are rated from High risk to Medium risk in NRA 2023.

NRA 2023 provided critical ML/TF risk information to stakeholders, including law enforcement authorities, regulators/ supervisors, their regulated sectors/ entities and other competent authorities, so that they could have a clear understanding of the inherent ML/TF risks and develop and implement the effective preventive measures and controls in line with the risk-based approach on an on-going basis.

AML/CFT POLICIES, PROCEDURES AND CONTROLS

The SOS Capital under the Compliance Program prescribed under the SECP AML/CFT Regulations to develop and implement following internal Policies, Procedures and Controls which are approved by the Board of Directors to enable to effectively manage and mitigate the risk that are identified in the risk assessment of ML/TF/PF or notified by the Commission.

The AML/CFT Policies, Procedures and Controls provide the mechanism to detect and control ML and TF for preventing the abuse of financial products and services.

The SECP Guidelines supplement the AML/CFT Regulations by clarifying and explaining the general requirement of the regulatory framework to help in applying national AML/CFT measures. The AML/CFT Policies, Procedures and Controls define the mechanism for ensuring effective compliance culture for AML/CFT Framework.

SCOPE

This policy applies to each and every business segment and all employees of **SOS Capital Limited** to effectively mitigate the risks of ML / TF/ PF. As the SOS Capital is prone to the risk of being misused by criminal elements for their ulterior motives, this policy will be a guiding document for employees to address the risks stemming from customers or transactions in an effective way of using Risk Based Approach (**"RBA"**).

The management will continuously refine its Customer Due Diligence processes using the RBA, through implementation of system based Risk Rating environment for Customer Risk Profiling. Standard Operating Procedures (SOPs) along with various guidance documents and systems are provided to the branches / field staff from time to time to ensure effective execution of the process to identify & mitigate ML / TF / PF risks. Considering the huge size of undocumented sector in the economy, execution of due diligence process is complex and time consuming. However, for the compliance of regulatory requirements and to contain the customer related risks, the management will make best efforts to conduct proper due diligence of every existing and prospective Customer.

Moreover, the management will handle Terrorism Financing (**"TF"**) as separate risk and will regularly conduct TF risk assessment to identify threats posed by TF and to gauge efficacy of the controls to mitigate the inherent risk in such activities in line with the Pakistan National Risk Assessment on ML/TF 2019 (**"NRA 2019"**) update. Accordingly, existing controls shall be regularly evaluated in the light of prevailing and emerging risks and additional appropriate actions/controls to identify, assess and mitigate the risks; will be implemented.

OBJECTIVES

RISK MANAGEMENT FACTORS:

a) To prevent criminal elements from using the Brokerage House for money laundering activities from any of its branch or channel.

b) To safeguard the Brokerage House from being used as a conduit in Terrorism and Proliferation Financing.

c) Ensuring that only bona fide and legitimate customers are accepted.

RISK MITIGATION MEASURES:

a) To verifying the identity of customers using reliable and independent sources.

b) To ensure that proscribed individuals or entities and their affiliates or associates are not having any trading relationship or being provided any service from the SOS Capital.

c) To conduct Ongoing Monitoring of Customer's accounts and transactions to prevent or / and detect potential ML / TF/Activities.

d) To implement Customer Due Diligence process using Risk Based Approach.

e) To ensure implementation of Targeted Financial Sanctions (TFS) related to Terrorism & Proliferation Financing (TF &PF).

f) To manage reputational, operational, legal and concentration risks etc.

g) To put in place appropriate controls for prevention, detection and reporting of Suspicious Activities in accordance with applicable laws/laid down procedures.

h) To comply with the applicable laws, regulatory requirements and guidelines etc.

ESTABLISHMENT OF DEPARTMENTS/FUNCTIONS AND APPOINTMENT / DESIGNATION OF OFFICERS ESTABLISHMENT OF COMPLIANCE DEPARTMENT / FUNCTIONS AND APPOINTMENT OF COMPLAINCE OFFICER (CO)

a) As required under regulation 29 of the Securities Brokers (Licensing and Operations) Regulations, 2016 (the "Broker Regulations"), the SOS Capital shall, as applicable, either designate or appoint a whole-time Compliance Officer, fulfilling the Fit and Proper criteria specified in the Regulations.

b) The Compliance Officer should be a Senior Management level officer as defined under the Regulation 2(1) (f) of the AML/CFT Regulations and the Regulation 2(1) of the Brokers Regulations.

c) The Compliance Officer shall report directly to the board of directors or chief executive officer or committee.

d) The Compliance Officer as well as any other person appointed to assist him shall have timely access to all customer record and other relevant information, which they may require to discharge their function.

e) The Compliance Officer shall have Job Descriptions / Responsibilities included but limited to the responsibilities described under the Brokers Regulations and Regulation 27(2)(c) of the AML/CFT Regulations as per Job Description annexed as Appendix-A to this document.

f) The function of Compliance Officer cannot be outsourced, only limited functions such as screening or database checks can be performed by another entity, except where the third party is part of a group and is properly supervised by a competent authority.

g) Qualification and experience of Compliance Officer shall preferably be in accordance with the Fit and Proper Criteria prescribed under the Brokers Regulations.

ESTABLISHMENT OF INDEPENDENT INTERNAL AUDIT DEPARTMENT/FUNCTIONS AND APPOINTMENT OF INTERNAL AUDITOR OFFICER/AUDIT OFFICER

a) The SOS Capital shall put in place effective and operationally independent Internal Audit function/department having appropriate trained and competent staff.

b) The Internal Auditor/Internal Audit function shall directly report to the Board of Directors or its Audit Committee as prescribed under the Brokers Regulations.

c) The Internal Audit function shall be headed by a dedicated or designated head of Internal Audit possessing relevant qualification and experience.

d) The Audit Committee, if established by the Board shall be responsible to monitor and review the effectiveness of Internal Audit function/department.

e) Internal Audit Function can be outsourced to third party through the policies and procedures in relation to outsourcing.

f) The SOS Capital shall conduct Due Diligence of Outsourcing Service Provider (OSP) as Fit and Proper to perform the audit activity that is being outsourced.

g) The SOS Capital shall have written Outsourcing Agreement clearly sets out the obligations of both parties.

h) The SOS Capital shall develop a contingency plan and strategy to exit the arrangement in the event that OSP fails to perform the outsourcing activity as agreed.

i) The SOS Capital shall be ultimate responsible for meeting AML/CFT requirements.

j) Internal Audit Officer shall have Job Descriptions / Responsibilities included but limited to the responsibilities described under the Brokers Regulations and the AML/CFT Regulations as per Appendix-B attached to this document

RISK ASSESSMENT AND MITIGATION
RISK ASSESSMENT:

The SOS Capital must assess each Customer's risk to allow for correct application of Enhanced Due Diligence, Standard, Simplified or Special measures for PEPs and other designated categories as per the Regulations. Necessary minimum customer risk rating categories are revised in line with NRA 2023:

a) Very High (VH) Risk Category
b) High (H) Risk Category
c) Medium (M) Risk Category
d) Low (L) Risk Category

RISK MITIGATION MEASURES THROUGH CUSTOMER DUE DILIGENCE (CDD)
CUSTOMER DUE DILIGENCE (CDD) MEASURES:

The SOS Capital will apply the following measures relating to CDD of the Customers:

1. CDD measures for Identifying and Verifying New and Existing Customers and/or beneficial owners on the basis of documents, data or information obtained from customer and/or from independent sources **before, during or after** course of establishing a business relationship.

2. CDD measures for understanding and obtaining information on the purpose and intended nature of business relationship.

3. CDD measures also include monitoring of accounts/transactions on ongoing basis to ensure that these being conducted are consistent with our knowledge of customer, his business and risk profile

including his source of funds and data/information for taking prompt action in case of material departure from usual and expected activity.

4. This Regulation covers the requirement of documents as per **Annexure-I**.
5. Prohibitions from establishing business relationship with entities and /or individuals that are **DESIGNATED** under UNSCR adopted by Govt. of Pakistan, **PROSCRIBED** under Anti-Terrorism Act, 1997 and associates/facilitators of **DESIGNATED / PROSCRIBED** entities/individuals.

6. Steps to determine the person acting on behalf of a customer including authority, identification and verification of authorized person and the customer.

7. Categorization of customers as High or Low Risk as outcome of CDD.

8. Maintaining list of Customers/Accounts where business relationships were refused or needed to be closed on **Negative Verification.**

9. Non-satisfactorily CDD measures, account shall be closed or business relationship terminated and considering to warrant STR.

10. Doubt of tipping-off the Customer due to CDD measure, filing STR without CDD process.

11. Govt. entities accounts to be opened on their own names operated by officers on production of Special Resolution or Authority from concerned Admin Dept. or Ministry duly endorsed by MoF or Finance Dept./Division of concerned Govt.

MEASURE TO MITIGATE THE RISKS ASSOCIATED TO MT, TF AND PF:

The SOS Capital will take the following measures to mitigate the risks associated to Money Laundering (ML), Terrorist Financing (TF) and Proliferation Financing (PF) activities through the customers or potential customers:

CUSTOMER IDENTIFICATION

The SOS Capital will serve only the genuine person(s) and all-out efforts would be made by the management to determine true identity of its customers. Minimum set of documents shall be obtained from various types of customer(s), at the time of opening account, as prescribed in **Annexure-I** to the SECP AML/CFT Regulations.

The Customer relationship is only established on the strength of:

a) In case of Natural Person, valid CNIC / SNIC / Passport / NICOP/ SNICOP/ POC / ARC / POR /Form B / Juvenile Card number;

b) Where the customer is not a Natural Person, the registration/ incorporation number, business registration number or special resolution/authority;

c) In case of government accounts/autonomous entities (as applicable).

d) For **non-face-to-face** customers, the management shall put in place suitable operational procedures to mitigate the risk(s) attached with non-face-to-face prospective customer(s) and establish identity of the client.

Moreover, the management shall not rely on third parties to perform any CDD measures as prescribed by the SECP.

CUSTOMER VERIFICATION

The SOS Capital shall identify the Beneficial Ownership of accounts/ transactions by taking all reasonable measures. Identity(ies) of the customers and Beneficial Owner will be verified using reliable independent sources including receiving copy of Verisys shared by National Clearing Company or any other entity notified as "Third Party" under AML Regulatory framework ("**Notified 3rd Party**"). Verification of the identity of the customers and Beneficial Owners shall be completed before business relations are established. Extra care is essential where the customer is acting on behalf of another person, and reasonable steps must be taken to obtain sufficient identification data to verify the identity of that other person as well. For customers that are Legal Persons or for Legal Arrangements, branches shall take reasonable measures to: -

a) Understand the ownership and control structure of the customer;

b) Determine and verify the natural persons who ultimately own or control the customer. This includes those persons who exercise ultimate effective control over a Legal Person or Arrangement.

c) Identity documents, wherever required as per updated AML/CFT Regulations, shall be invariably verified by utilizing shared copy of Verisys by Notified 3rd Party and Verification of the identity of the customers and Beneficial Owners shall be completed before business relationship is established or a transaction is processed.

d) Bio-Metric Verification of the Customers will be done by through the system within forty-five (45) days from the date establishing business relationship with the Customer or any other time period as extended by the Commission from time to time.

CUSTOMER ACCEPTANCE

The customer will only be accepted once above given formalities have been completed in letter and spirit. Following accounts shall not be opened/maintained, where;

a) Identity, beneficial ownership, or information on purpose and intended nature of business relationship is not clear.

b) Name of the individual customer/organization (including such individuals who are authorized to operate account(s) and the members of governing body/directors/trustees of an entity) appears in the Proscribed/Sanctioned / Specially Designated Nationals (SDNs) entities lists.

c) Proscribed entities and persons or those who are known to be associated with such entities and persons, whether under the proscribed name or with a different name.

d) Anonymous / fictitious (Benami) or numbered accounts.

CDD FOR WALK-IN-CUSTOMERS:

The detail procedures attached as Annexure-E

a) Walk-in-customers shall only be entertained, once due diligence measures for transactions relating to such customers as prescribed by the applicable SECP AML/CFT Regulations /guidelines along with international best practices have been complied with.

b) For walk-in-customers / occasional customers, to establish and validate the true identity of the person(s) executing the transactions either for self or if the person is acting on behalf of some other person(s), complete originator information must be obtained and identities must be invariably verified as directed under the regulations; using reliable, independent source of information, i.e., Biometric Verification or NADRA Verisys in line with SECP directive on use of Biometric Technology.

c) Further, name clearance should also be obtained against sanctioned lists through Central Database (as per **Appendix–D**) for Sanction Screening for walk in customer executing the transaction to ensure that the person is not a proscribed person/entity.

CDD FOR EXISTING CUSTOMERS:

The SOS Capital shall apply CDD requirements to its existing customers on the basis of materiality and risk and shall conduct due diligence on existing relationship at appropriate time taking into account the following:

a) Whether and when CDD measure have previously been undertaken; and
b) Adequacy of data obtained.

The customers who opened accounts with old NICs, the SOS Capital shall ensure the following:

a) Attested copies of identity documents shall be presented in its record;
b) Without identity documents accounts shall be blocked after serving one (1) month prior notice for all withdrawals until all subject regulatory requirements are fulfilled;
c) Upon submission of attested copy of identity document and verification of the same from NADRA Verisys or Biometric Verification, the blockage shall be removed.

The Customers whose accounts are dormant or in-operative, withdrawal shall not be allowed until the account is activated on the request of the Customer on following basis:

a) NADRA Verisys or Biometric Verification has been done; and
b) Attested copy of customer's valid identity document.

TARGETED FINANCIAL SANCTIONS (TFS) MANAGEMENT

In order to comply with the Targeted Financial Sanctions regime, the management will devise effective system and controls to safe guard the bank from being exploited by the terrorists for TF/PF. In this regard, all the relationships (customers/non-customers i.e. walk in customers, shareholders, directors, third party service providers/vendors) will be screened against the prescribed sanctions lists; both local and international before establishment of the relationship. Further, all the relationships will be screened against the sanctioned lists on periodic basis as well.

Undertaking TFS obligations under United Nations (Securities Council) Act 1948 and /or Anti-Terrorism Act 1997 and Regulations made there under including:

a) Develop mechanism, process and procedures for screening and monitoring customer, potential customers and their BOs/Associates to detect any matches or potential matches for designated / proscribed persons.

b) In case of positive or potential match, SOS Capital shall immediately:

i. Freeze relevant funds and assets, block transaction without prior notice;
ii. Prohibit from making any funds or other assets, economic resources, or financial and other services and funds;
iii. Reject the transaction or attempted transactions or the customer.
iv. File a STR to FMU and notify the Commission;
v. Implement any other obligation under AML Act 2010, UNSC Act and Anti-Terrorism Act and any other regulations made thee under.

c) The SOS Capital is prohibited, on an ongoing basis, for providing financial services to proscribed /designated entities and person or those who are known for their association with such entities and persons.

ACCOUNTS AND TRANSACTIONS MONITORING:

The Operations Department shall update expected monthly credit turnover limits in the system and/ or revise CDD profile of customer(s) as per guidelines for ongoing review as required under applicable SECP

AML CFT Regulations/guidelines along with international best practices, while, the basis of revision shall be documented and customers may be consulted, if necessary.

Such limits will be maintained to make sure that all transactions are consistent with the Company's knowledge of the customer, its business and risk profile and are conducted in accordance with the SECP AML / CFT regulations, instructions of Financial Monitoring Unit (FMU) and other applicable local /international bodies.

Financial transactions should be monitored through automated Transaction Monitoring System (TMS) based on predefined scenarios and thresholds.

The management shall pay special attention to every complex, unusually large and out- of-pattern transaction(s), which have no apparent economic or visible lawful purpose. If the SOS Capital suspects or has reasonable grounds to suspect that the funds are the proceeds of criminal activities or have potential to be used for terrorist activities, it shall report its suspicion to Financial Monitoring Unit (FMU) through its GoAML E-portal.

In case of suspicion, the Compliance Officer shall raise Suspicious Transaction Reports in line with the requirement highlighted under AML Act 2010, SECP AML / CFT regulations and SECP Guidelines. Accordingly, the Compliance Officer should devise procedures to meet these requirements.

For customers / clients whose accounts are dormant, we shall not allow debit entries in such accounts (except those allowed under AML/CFT Regulations) until the account holder(s) produce(s) attested copy of his/her CNIC if already not available in the company's record, fulfill all other requirements for activation of the account and the Operation Department is satisfied with CDD of.

The employees are strictly prohibited to disclose the fact to the customer that a Suspicious Transaction Report (STR) / Currency Transaction Report (CTR) or related information has been reported to FMU or any other Law Enforcement Agency (LEA).
Currency Transactions (i.e. CTR) exceeding the prescribed limits as defined in AML Act 2010 and its subsequent amendments from time to time will be reported to FMU through GoAML E-portal.

In order to adopt additional measures to further strengthen the CDD regime, CDD/EDD Assessment up to Top 50 Investors will be conducted by each branch. The branches shall conduct assessment of such accounts regarding compliance of the CDD/EDD requirements and identify deficiencies and make necessary efforts to regularize the deficiencies identified during the assessment process.

ON-GOING MONITORING OF BUSINESS RELATIONSHIPS

In case a customer has no active business, and cannot be reached, or refuses to engage in updating because there is no active business, account should be marked inactive with the instruction that relationship cannot be re-activated without full CDD.

In case due diligence cannot be updated, a formal ending of the relationship should be done by following the legal process for ending a customer relationship under the applicable laws.

SOS Capital shall invest in computer systems for transactions monitoring specifically designed to assist the detection of ML/TF/PF. It is recognized that this may not be necessary in a risk-based approach. In such circumstances, SOS Capital will need to ensure that the alternative systems are in place for conducting ongoing monitoring.

Alternate or manual systems of ongoing monitoring may rely on Compliance Officer generated lists or instructions and regular lists generated from IT system such as:

a) High transaction list for each day;
b) Periodic list of transactions over determined thresholds;

c) Periodic list of new clients and relations closings;
d) Monthly or yearly lists of inactive clients; Ad Hoc reviews, meaning reviews triggered by an event, new information from supervisors and media reports.

SIMPLIFIED DUE DILIGENCE ("SDD") MEASURES:

The detail procedures attached as Annexure F

The SOS Capital may conduct SDD in case of Low Risk identified.

a) To relevant sector;
b) To relevant customer type; and
c) To activity
d) The SOS Capital will use the following SDD Measures:
e) Reducing the frequency of Customer identification update;
f) Reducing the degree of On-going monitoring and scrutinizing transactions, based on reasonable monetary threshold;
g) not collecting specific information or carrying out specific measures to understand the purpose and intended nature of the business relationship, but inferring the purpose and nature from the type of transaction or business relationship established;
h) undertaking verification after establishment of the business relationship;
i) Less stringent steps to verify the Beneficial Owner.
j) Where the SOS Capital decides to take SDD measures w.r.t a customer, it should document the full rationale behind such decision and make available that documentation to the Commission on request.

ENHANCED DUE DILIGENCE MEASURES:

The detail procedures attached as **Annexure-G**

The SOS Capital shall apply Enhanced Due Diligence Measures in the following scenarios:

POLITICALLY EXPOSES PERSONS (PEPS)

Business relationships with SOS Capital holding important public positions may expose SOS Capital to significant reputational and/or legal risk. In addition, PEPs because of their position, may expose SOS Capital and its business partners to a high degree of public expectation and scrutiny.

Family members of a PEP are individuals who are related to a PEP either directly or through marriage. Close associates are individuals who are closely connected to PEP, either socially or professionally. Close associates have in many cases been used to provide a cover for the financial activities of a PEP, and may not be in any way connected to the PEP in an official capacity. The CDD done by SOS Capital on the source of funds or source of wealth of a customer may be the first clear documentation of a close association.

RISK AS PER NRA 2019:

The followings are the Risk Identified through NRA – 2019:

The AML/CFT National Risk Assessment of Pakistan has determined the risk of corruption and therefore the risk of providing financial services to PEPs is high. This means that all domestic PEPs must be scrutinized, particularly for their source of funds wealth and assets.

The SOS Capital shall be obliged to ascertain whether its customer is a PEP. In assessing the ML/TF risks of a PEP, the SOS Capital shall consider factors such as whether the customer who is a PEP:

Has prominent public functions in sectors known to be exposed to corruption;
Has business interests that can cause conflict of interests (with the position held);
Has been mentioned in media related to illicit financial behavior; and
Is from a high risk country.
The PEP red flags that the SOS Capital shall consider include:
The information that is provided by the PEP is inconsistent with other (publicly available) information, such as asset declarations and published official salaries;
A family member of a PEP without own financial means is transacting without declaring the relationship to a PEP, or the origin of the funds transacted;
The PEP is associated with, or owns, or signs for, complex legal structures that are commonly used to hide Beneficial Ownership;
Funds are repeatedly moved to and from countries to which the PEP does not seem to have ties;
A PEP uses multiple bank accounts for no apparent commercial or other reason;

The PEP is from a country that prohibits or restricts certain citizens from holding accounts or owning certain property in a foreign country.

The SOS Capital shall take a Risk-Based Approach in determining whether to consider a customer as a PEP who is no longer a PEP. The factors that SOS Capital should consider include:

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

whether the individual's previous and current function are linked in any way (e.g., formally by appointment of the PEPs successor, or informally by the fact that the PEP continues to deal with the same substantive matters, or through continued strong ties within a party, family or institution).

The SOS Capital in addition to performing normal due diligence measures should also:
have appropriate risk management systems to determine whether the customer is a PEP;
obtain senior management approval for establishing business relationships;
take reasonable measures to establish the source of wealth and source of funds; and
Conduct enhanced ongoing monitoring of the business relationship.

RISK AS PER NRA 2023:

Pakistan conducted its first NRA conducted in 2017 using the World Bank's methodology. A subsequent NRA was undertaken in 2019 by using in-house hybrid methods which was more focused on inherent ML/TF threats and vulnerabilities. Pakistan has made extensive improvements to its AML/CFT regime since 2019, resulting in improved information collection and understanding of its threats and vulnerabilities. The 2023 NRA incorporates this enhanced understanding, resulting in updated risk assessments. The NRA 2023 updates Pakistan's ML/TF risk profile using in-house methodology aligned with international best practices and FATF recommendations. As per the adopted methodology in NRA 2023, 04 rating scales used to assess the risks of ML/TF threats and vulnerabilities included **"Very High", "High", "Medium" and "Low".** It is important to note that low risk doesn't mean that no action is required; rather, as required by law, each stakeholder needs to take sufficient measures and adopt controls related to the low-risk items also.
The followings are the Risk Identified through NRA – 2023:

MONEY LAUNDERING (ML) RELATED THREATS ASSOCIATED WITH PREDICATE OFFENCES:

The NRA 2023 incorporated enhanced understanding, resulting in updated risk assessments. The NRA 2023 updates Pakistan's ML/TF risk profile using in-house methodology aligned with international best practices and FATF recommendations. As per the adopted methodology in NRA 2023, 04 rating scales used to assess the risks of ML/TF threats and vulnerabilities included **"Very High", "High", "Medium" and "Low".** It is important to note that low risk doesn't mean that no action is required; rather, as required by law, SOS Capital needs to take sufficient measures and adopt controls related to the low-risk items also.

The following are main features of NRA 2023 for benefit of the SOS Capital for updating its respective AML/CFT/CPF Policies, Procedures and Controls:

Identified twenty-one (21) Predicate Offences and rated them in four (4) ML Threats Rating Scales i.e., Very-High (VH), High (H), Medium (M) and Low(L);

Identify the Key Sources and Channels used for potential ML Activities

NRA 2023 also identified Major Sources of Illegal Proceeds generated and through Major Channels used to launder that proceeds generated from predicate offences:

Major Sources:

Illegal proceeds generated from committing predicate offences including but not limited to embezzlement, kickbacks/commissions/bribes, extortions, drug trafficking, human trafficking, bonded labor, illegal organ removal, corruption, smuggling, fraud, illegal gambling, smuggling of people and weapons, tax evasion, false tax claims/credits/refunds, Hawala/Hundi or any other predicate offence listed in the Schedule-I of AMLA,2010.

Under-invoicing or over-invoicing as well as underreporting of legal business income/trade-volume/wages/investments, as well as hiding assets or funds in offshore accounts or other undeclared financial irregularities.

Major Channels:
Cash / Cash couriers.
Illegal Money or Value Transfer Services (**"MVTS"**)
Benami Accounts and properties;
Shell Companies
Front Import & Export companies
Offshore Bank Accounts
Trade -based fund transfers
Payment through intermediaries / third parties
Investments in real estate / precious metals & stones / other high value assets;
Investments in stocks / bonds / investments funds;
Crypto currency

TERRORISM AND TERRORISM FINANCING RELATED THREATS:

NRA 2023 identified 87 Terrorist Organizations ("**TOs"**) out which, 78 proscribed are not active rather, most of them most of them are inactive, dismantled or merged into other TOs. A detailed **assessment of TF threats** was carried out during the NRA 2023 process by assessing a total of 87 terrorist organizations (TOs), including 78 proscribed TOs as well as some other non-proscribed and UN-listed entities. Based on the data provided by LEAs and from the intelligence inputs, it was found that 41 terrorist organizations have been active in Pakistan with varying degrees of operations. The rest of the TOs have either been dismantled, merged into other organizations or inactive for long. Based on the assessment, **04 TOs were considered as "very high" risk, 08 as "high" risk, 07 as "medium" risk and the remaining 68 as "low" risk.**

The following are the Key Sources and Channels being used by TOs for TF:

Table 4.2. Key Sources and Channels exploited for TF		
Sr. No.	Sources	NRA 2023
1	Donations	Very High
2	Extortion	Very High
3	Narcotics trafficking	High
5	Cash smuggling	High
4	Misuse of Properties	Medium
6	Kidnapping for ransom	Medium
7	Goods/ Natural resources smuggling	Medium
8	Skin/ Hides collection	Low
Sr. No.	Channels	NRA 2023
1	Cash/ Cash couriers	Very High
2	Illegal MVTS	Very High
3	Banking	High
5	Branchless Banking	High
4	Virtual Currency	Medium
6	Exchange Companies	Medium
7	Securities	Low
8	Insurance	Low
9	NBFCs & *Modaraba*	Low
10	Microfinance	Low
11	Legal persons & legal arrangements	Low

Please note that Pakistan has a large, diverse, and vibrant Non-Profit Organization (NPO) sector and an overall assessment revealed that 6.75% of the NPOs are high-risk whereas 43.64% consists of Medium-risk and 49.61% are Low-risk.

ASSESSMENT OF INHERENT ML/TF VULNERABILITIES BY SECTOR:

In addition to assessing ML and TF related threats, NRA 2023 also assessed how vulnerable different financial and DNFBP sectors were to ML and TF. It is important to understand that vulnerability refers to characteristics, traits or other features that can be exploited by threats or may facilitate their activities. While conducting the **Inherent Sectorial Vulnerability Assessment**, Financial Sector, and Designated Non-Financial Businesses & Professions (DNFBPs) and Legal Persons and Legal Arrangements (LPLAs) were examined.

Financial Sector:

The **inherent Sectorial Vulnerability Assessment** examined ten sub-sectors in the Financial Institutions (FIs) sector. A summary table of vulnerability ratings of financial sectors is given as under;

Table 4.3.1. Inherent Vulnerability Assessment Ratings of the Financial Sectors			
Sector		Supervisor	NRA 2023 Risk Rating
Sr. No.	Financial Sector		
1	Banks	SBP	Very High
2	Microfinance Banks (MFBs)		High
3	Exchange Companies (ECs)		High
4	Development Finance Institutions (DFIs)		Low
5	Securities Market	SECP	Medium
6	NBFCs (Fund Management)		Medium
7	NBFCs (Lending & *Modarbas*)		Medium
8	Life Insurance Companies		Medium
9	Non-Life Insurance Companies		Low
10	Central Directorate of National Savings (CDNS)	National Saving Supervisory Board (NSSB)	Medium

Designated Non-Financial Businesses & Professions (DNFBPs)

Designated Non-Financial Businesses & Professions (DNFBPs) are comprised of real estate agents (including builders/ developers), Dealers of Precious Metals & Stones (DPMS), accountants and lawyers (including trust and company service providers -TCSPs and notaries). All these sub-sectors falling under the Designated Non-Financial Businesses and Professions (DNFBPs) were examined in NRA 2023. These sectors have been assessed based on their unique characteristics, clientele, the offered products and services, their geographic reach, and the channels they operate through. A summary table of vulnerability ratings of DNFBP sectors is given as under;

Table 4.3.2. Inherent Vulnerability Assessment Ratings of the DNFBP Sectors			
Sector		Supervisor	NRA 2023 Risk Rating
Sr. No.	DNFBP Sector		
1	Real Estate Agents	FBR	Very High
2	Dealers in Precious Metals & Stones (DPMS)		High
3	Lawyers, TCSPs and Notaries	PBC/ SECP	Low
4	Accountants	ICAP /ICMA	Low
		FBR	

LEGAL PERSONS AND LEGAL ARRANGEMENTS (LPLAS)

A detailed analysis has also been conducted to assess the inherent vulnerability associated with **Legal Persons and Legal Arrangements (LPLAs)** and their formation. In Pakistan, legal persons are companies, limited liability partnerships (LLPs) and cooperatives while legal arrangements include trusts and *waqfs* (a form of Islamic charitable trust). Companies and LLPs are registered and regulated by the Securities and Exchange Commission of Pakistan at the federal level. In contrast, cooperatives, trusts and *waqfs* are registered and regulated under provincial and territorial laws. A summary table of vulnerability ratings of LPLA sectors is given as under;

Table 4.3.3. Inherent Vulnerability Assessment Ratings of the LPLA Sectors			
Sector		Supervisor	NRA 2023 Risk Rating
Sr. No.	Type of LP/LA		
1	Private Limited Companies	SECP	Very High
2	Public companies		Low
3	Companies Limited by Guarantee		Low
4	Foreign Companies		Very High
5	Limited Liability Partnerships (LLPs)		Medium
6	Cooperatives	As per provincial and territorial laws	Low
7	Trusts		Medium
8	*Waqfs*		Medium

CUSTOMERS FROM HIGH-RISK JURISDICTIONS IDENTIFIED BY FATF:

The management shall also apply Enhance Due Diligence (EDD), proportionate to the risks to business relationships with individuals and entities including Financial Institutions from high-risk foreign jurisdictions as specified by the FATF and as identified by the SOS Capital during its internal TF risk assessment.

NON-PROFIT ORGANIZATIONS ("NPOs") OR NON-GOVERNMENT ORGANIZATIONS ("NGOs")

Both by international standards and in Pakistan's National Risk Assessment, NPOs and NGOs are classified as a High-Risk Sector for TF.

The objective of Enhanced Customer Due Diligence for NPOs/NGOs is to ensure that NPOs/NGOs are not misused by terrorist organizations:
to pose as legitimate entities;
to exploit legitimate entities as conduits for terrorist financing, including for the purpose of escaping asset freezing measures; or

To conceal or obscure the clandestine diversion of funds intended for legitimate purposes, but diverted for terrorist purposes.
The SOS Capital transacts with NPOs/NGOs should understand:
Beneficiaries and Beneficial Owners including certain donors that maintain decision rights;
Flow of funds, in particular the use of funds by an NPO/NGO.

HIGH NET WORTH INDIVIDUALS (HNWI)

High net worth individuals while an attractive customer can expose the SOS Capital to higher risk of financial transactions that may be illicit. There is no standard size of HNWI. SOS Capital knows to whom it is offering its products and services, and can establish criterion for HNWI applicable to their particular business.

The SOS Capital should scrutinize HNWI customers to determine, whether they carry a higher risk of ML/FT and require additional due diligence measures. Such scrutiny must be documented and updated as part of the Risk Assessment.

HIGH-RISK COUNTRIES & HIGHER RISK REGIONS WITHIN A COUNTRY

Certain countries, or regions within countries have a specific higher AML/CFT risk profile. Examples are border regions, large goods transit points such as ports, or regions experiencing social unrest, that can be associated with specific crime patterns such as cash or people smuggling, drug trafficking, violent crimes, fraud and corruption, and consequently pose a higher potential risk to the SOS Capital. Conducting a business relationship with a customer from such a country/region exposes the SOS Capital to risk of channeling illicit money flows.

The SOS Capital should exercise additional caution, and conduct EDD on individuals and/or entities based in high-risk countries / regions. The SOS Capital shall consult publically available information to ensure that they are aware of the high-risk countries/territories. The SOS Capital shall consider among the other sources, sanctions issued by the UN, the FATF high risk and non-cooperative jurisdictions, the FATF and its regional style bodies (FSRBs) and Transparency International Corruption Perception Index (TI CPI).

Complex legal structures may be created in jurisdictions specializing in obscuring the trail to **Beneficial Owners** and allowing easy creation of complex corporate vehicles, so called offshore jurisdictions. SOS Capital engaging with foreign complex legal structures, or with local companies owned by such foreign legal structures, need to educate itself on offshore financial centers and acquire adequate expertise to understand its customers' ownership structure up to the Beneficial Owner and be able to assess documents presented to them.

AFGHAN REFUGEES

Identification and evaluation of the customers or their nominees or authorized persons or directors or sponsors or major shareholders, who are Afghan National or Afghan Refugees.

The SOS Capital shall ensure that before establishing business relationship with people from High Risk jurisdiction areas as identified in AML / CFT regulations, the person is not an Afghan Refugee or a person's nominee or joint holder is not an Afghan Refugee. It is likely hood that Afghan Refugees are involved in various crimes like drug trafficking, kidnapping, money laundering and terrorist activities.

CUSTOMERS RESIDING NEAR TO POROUS BORDERS:

Considering Pakistan's geographical landscape and porous borders, the SOS Capital shall be required to identify and assess vulnerability to both ML and TF, heightening in particular Pakistan's TF risks associated to cash smuggling. Pakistan is bordered by India to the east, Afghanistan to the west, Iran to the southwest, and China in the far northeast. The SOS Capital shall be required to conduct EDD of the Customer having geographical location near to Porous Border to ensure following the EDD procedures before establishing business relationship with such Customer as under:

Identification documents should be verified
Scanning of the Customers and his/her joint holders, nominees from the list of proscribed and designated persons and entities.
Taking verifiable proof of funds;
Only paying and receiving funds from the bank accounts of respective Customers.
Transactions are within the limits set based on source of funds/income of the Customers.
Take management approval before establishing business relationship while marking High Risk factor.
In case of any doubt or non-receipt of information, STR may be considered to file and the funds to be frozen without tip-off.

RISK MANAGEMENT APPLYING RISK BASED APPROACH:

All relationships shall be categorized with respect to their risk levels i.e., High, Medium and Low based on the risk profiling of customer (through e-KYC/CDD application and as guided in SECP AML CFT Regulations and SECP Guidelines and international best practices for making effective decision whether to perform Customer Due Diligence (CDD) or Enhanced Due Diligence (EDD) both at the time of opening and ongoing monitoring of business relationship.

The SOS Capital may endeavor to develop the system based KYC/CDD and Risk Profiling of Customer, through implementation of e-KYC/CDD Application. This application may assist the branches for effective and efficient KYC/CDD management in order to mitigate risk related to Money Laundering/Financing of Terrorism and Proliferation Financing.

The approval for opening of Politically Exposed Person (PEP) and Non-Governmental Organizations (NGOs)/Not-for-Profit Organizations (NPOs) and Charities account will be obtained from Senior Management (Not less than Head of Operations or Business Development) after performing EDD. Further Personal accounts will not be allowed to be used for charity purposes/collection of donations.

Customer KYC / CDD profile will be reviewed and/or updated on the basis of below mentioned predefined frequency, in accordance with the risk profile of the customer:

Very High Risk :	At least Once in a Half Year or on need basis.
High Risk :	At least Once in a Year or on need basis*
Medium Risk :	At Least Once in 2 Years or on need basis*
Low Risk :	At least Once in 3 Years or on need basis*

**In case of any material change in the relationship or deviation from customer profile, CDD will be conducted and customer profile will be updated immediately without lapse of above defined period.*

The Compliance Officer will counter-examine the relationships to ensure that due diligence procedures are adhered to in letter and spirit by the concerned staff in business segments.

While formulating procedures and controls, the management shall take into consideration Money Laundering and Financing of Terrorism threats that may arise from the use of new or developing technologies, especially those having features of anonymity or inconsistency with the spirit of CDD/EDD measures.

IDENTIFICATION OF BENEFICIAL OWNERSHIP OF LEGAL PERSONS OR LEGAL ARRANGEMENT

The SOS Capital shall identify the beneficial owners of Legal Person or Legal Arrangements as per following procedures:

The Beneficial Owner (the "BO") is the natural person at the end of the chain who ultimately owns or controls the customer. The BO is defined under AML/CFT Regulations," beneficial *owner" in relation to a customer of a regulated person means, the natural person who ultimately owns or control a customer or the natural person on whose behalf a transaction is being conducted and includes the person who exercise ultimate effective control over a person or a legal arrangement".*

The Companies Act, 2017 defines "Beneficial Ownership of shareholders or officer of a company" means ownership of securities beneficially owned, held or controlled by any officer or substantial shareholder directly or indirectly, either by him or her;
the wife or husband of an officer of a company, not being herself or himself an officer of the company;
the minor son or daughter of an officer where "son" includes step-son and "daughter" includes step-daughter; and "minor" means a person under the age of eighteen years;
in case of a company, where such officer or **substantial shareholder** is a shareholder, but to the extent of his proportionate shareholding in the company:

Provided that "**control**" in relation to securities means the power to exercise a controlling influence over the voting power attached thereto:

Provided further that in case **the substantial shareholder** is a non-natural person, only those securities will be treated beneficially owned by it, which are held in its name.

***Explanation:* -**For the purpose of this Act **"substantial shareholder"**, in relation to a company, means a person who has an interest in shares of a company-

the nominal value of which is equal to or more than ten per cent (10%) of the issued share capital of the company; or

Which enables the person to exercise or control the exercise of ten (10%) per cent or more of the voting power at a general meeting of the company.

Backward Ownerships means, "Ownership of the Legal Person or Legal Arrangement by another Legal Person or Legal Arrangement, which is also owned by another Legal Person or Legal Arrangement and so on and so forth until ultimate Natural Person(s) is (are) identified. For Example:

<table>
<tr><th>ULTIMATE NATURAL PERSON</th><th>BENEFICIAL OWNERSHIP</th><th>LEGAL PERSON</th><th>BENEFICIAL OWNERSHIP</th><th>LEGAL PERSON</th><th>BENEFICIAL OWNERSHIP</th><th>LEGLA PERSON (CUSTOMER)</th></tr>
<tr><td>Mr. Ahmad</td><td>50%</td><td rowspan="3">ABC Company (Pvt.) Limited</td><td>10%</td><td>XYZ Company</td><td>10%</td><td rowspan="3">Technologies (Pvt.) Limited</td></tr>
<tr><td>Mr. Ali</td><td>25%</td><td>20%</td><td>MNP Limited</td><td>20%</td></tr>
<tr><td>Mr. Sam</td><td>25%</td><td colspan="2">NATURAL PERSONS (Mr. Rizwan-50% & MRS. Rizwan-30%)</td><td>70%</td></tr>
</table>

Forward Ownerships means" the Legal Person or Legal Arrangement which owns another Legal Person or Legal Arrangement, that also owns another Legal Person or Legal Arrangement, until ultimate Natural Person(s) is(are) found, who owns such Legal Person or Legal Arrangement.

<table>
<tr><th>LEGLA PERSON (CUSTOMER</th><th>BENEFICIAL OWNERSHIP</th><th>LEGAL PERSON</th><th>BENEFICIAL OWNERSHIP</th><th>LEGAL PERSON</th><th>BENEFICIAL OWNERSHIP</th><th>ULTIMATE NATURAL PERSON)</th></tr>
<tr><td rowspan="2">Investments Limited</td><td rowspan="2">50%</td><td rowspan="2">ABC Company</td><td rowspan="2">10%</td><td rowspan="2">XYZ Company</td><td>90%</td><td>Mr. Ahmad</td></tr>
<tr><td>10%</td><td>Mr. Ali</td></tr>
</table>

		(Pvt.) Limited	90%	**NATURAL PERSON**		***Mr. Abdullah***
	25%	TRUST	20%	MNP Limited	50%	***Mr. Ali***
					30%	***Mr. Zaman***
					20%	***Mr. Sam***
	25%	**NATURAL PERSON**				***Mr. Bakar***

In this Customer (Legal Person) and its ultimate Beneficial Owners i.e., Natural Persons will be screened for identification and assessment against the lists of Designated/Proscribed Persons/Entities by NACTA and UNSCR through Govt. of Pakistan. The lists of designated / proscribed persons/entities are available on the following links:

https://www.un.org/securitycouncil/content/un-sc-consolidated-list
(https://scsanctions.un.org/search/
https://www.un.org/securitycouncil/sanctions/1267
https://www.un.org/securitycouncil/sanctions/1988
https://www.un.org/securitycouncil/sanctions/1718
https://www.un.org/securitycouncil/content/2231/background
https://nacta.gov.pk/proscribed-organizations-3/
https://nacta.gov.pk/pp/
https://nfs.punjab.gov.pk/

FOR LEGAL PERSONS / LEGAL ARRANGEMENTS:

The SOS Capital will essentially be required to understand the ownership and control structure of the Customer having simple structure based on the following:

Plausibility and records.

Further verification in any case of lack of transparency or doubt, or higher risk.
Register of Ultimate Beneficial Ownership as primary source for verification.

In case of a local Customer having complex structures, foreign entities or foreign owned entities, SOS Capital is required to develop and have the necessary knowledge to correctly identify and verify such clients and their beneficial owners using information and data publicly available on the internet.

The SOS Capital may adopt a Risk-Based Approach to the verification of beneficial ownership of a customer. SOS Capital must identify the beneficial ownership of a customer, regardless of the level of risk associated with that customer. However, the SOS Capital shall take reasonable steps to verify the identity and information depends upon on the risk assessment of the customer.

The SOS Capital should assess different levels of ML/TF risks posed by their customers' beneficial owners.

CUSTOMERS, WHOSE BENEFICIAL OWNERSHIP MUST BE KNOW:

The SOS Capital must identify the BOs of the following Customers:
Politically Exposed Persons;
Customers having links with High-Risk Country or Region.
Students not having regular and known Source of Income;
House-wives not having regular and know Source of Income.
Trusts, Non-Profit Organizations, Non-Government Organizations, etc.
Companies, Corporations and Partnerships having backward and/or forward ownership by another legal person(s).

IN CASE OF SUSPICION REGARDING BO OF THE CUSTOMER:

If the SOS Capital has doubts about the veracity or adequacy of the information provided, it should do the following actions:
not start a business relationship, or provide a financial service;
consider making a suspicious transaction report to FMU;
In case of non-reporting of STR, the SOS Capital may continue business relationship with such Customer provided rationale for its decision is recorded on its EDD form.

BENEFICIAL OWNERSHIP DECLARATION FORM:

The SOS Capital shall gather information relating to Beneficial Ownership from the Customer, who are Legal Person or Legal Arrangement as per declaration given by the Customer on **Appendix-C.**

REVIEW OF NEW PRODUCTS, PRACTICES AND SERVICES INCLUDING NEW TECHNOLOGIES

The management shall identify and assess the ML/FT/PF risks that may arise in relation to expansion of operations in different jurisdictions, the development of new products, services, business practices including delivery mechanism and the use of new or developing technologies for both new and pre-existing products.

CROSS BORDER FUNS TRANSFER

The SOS Capital shall strictly monitor wire transfers (domestic / cross border) regardless of any threshold. Foreign wire transfers are usually used to hide the actual transactions occurred. SOS Capital shall ensure that if any amount is received from cross border, the amount is actually transferred from the client through legal process of funds transfer methods in foreign countries like **SWIFT** not through various financial institutions to layer the transactions.

RECORD KEEPING

The records of identification documents, account opening forms, KYC forms, verification documents and other relevant documents along with records of account files and business correspondence, shall be maintained for a minimum period of ten years after the business relationship is ended.

The management shall also maintain for a minimum period of ten years all necessary records on transactions for both domestic and cross-border from the date of completion of transaction(s). The data relating to Suspicious Transactions and Currency Transactions reported to FMU will be retained for the period of at least ten years from the date of such reporting.

However, records relating to customers, accounts or transactions will be retained for longer period, which involve litigation or is required by court or other competent authority until otherwise instructed by the relevant body. Furthermore, all signature cards and documents indicating signing authorities, and other documents relating to the account or instrument surrendered to SECP / Exchange / any other competent law enforcing agency (duly authorized by law/court), shall be kept record till such time that SECP / Exchange / competent law enforcing agency (duly authorized by law/court) informs in writing that same need no longer to be preserved.

CORRESPONDENT RELATIONSHIP:

The SOS Capital will take appropriate measures when forming a correspondent relationship with any other regulated entity in compliance with regulation 30 of the AML/CFT Regulations, which include the followings:

Assessing the suitability of respondent Regulated Entity;
Understanding and documenting the respective AML/CFT responsibilities of FI and respondent Regulated Entity
Accessing respondent Regulated Entity in context of sanctions/embargoes and Advisories about risk;
Approval from Senior Management before providing correspondent service to new Regulated Entity.

Documentation of the basis of satisfaction.
Not entering or continuing correspondent relationship with Shell Regulated Entity.

The SOS Capital will establish correspondent brokerage relationships with only those foreign brokers that have adequate and effective AML / CFT systems and policies in line with the AML / CFT regulations relating to the country in which foreign broker operate.

The SOS Capital will pay special attention when establishing or continuing correspondent relationship with foreign brokers which are located in geographical locations or governed by jurisdictions that have been identified by FATF for inadequate and poor AML/CFT standards in the fight against money laundering and financing of terrorism.

Before establishing new correspondent brokerage relationship, approval from senior management shall be obtained and proper Due Diligence shall be conducted. Ongoing Due Diligence of respondent/ correspondent broker will be conducted using risk-based approach following the *guidelines given in* below table.

Very High Risk :	At least Once in Half Year or earlier if any happening / event/situation so demands
High Risk :	At least Once in a Year or earlier if any happening / event/situation so demands
Medium Risk :	At Least Once in 2 Years or earlier if any happening / event/situation so demands
Low Risk :	At least Once in 3 Years or earlier if any happening / event/situation so demands

In case of any material change in the relationship or deviation from customer profile, CDD will be conducted and customer profile will be updated immediately without lapse of above defined period. *Material change in relationship in the context of correspondent foreign broker would mean that the conduct of the account is not commensurate with the stated profile of the correspondent or respondent foreign broker and can also be triggered owing to some geo political situation under sanctions regime*

The SOS Capital shall not enter into or continue correspondent brokerage relations with a shell broker/entity and shall take appropriate measures when establishing correspondent brokerage relations, to satisfy themselves that their respondent broker does not permit their accounts to be used by shell companies/entities.

EMPLOYEES DUE DILIGENCE FOR THEIR VERIFICATION AND SCREENING

In line with SECP AML/CFT regulations, the management will implement employee due diligence policy for verification and screening of employees so inducted/hired to ensure that person has a clean history. Further, the Compliance Officer shall perform independent review of Employee Due Diligence process as per HR Manual/Policy.

VENDORS, OUTSOURCING AND SERVICE PROVIDER'S DUE DILIGENCE

The management should ensure that regulatory guidelines as specified in SECP AML/CFT Regulations and Guidelines relating to Outsourcing Arrangements for Compliances, Internal Audit and Operations, if done to outsourcing service providers are implemented.

TRAINING

Suitable Employee Training Program will be put in place by the management on an annual basis to enhance staff capability, to effectively implement the regulatory requirements, the policy & procedural requirements relevant to AML/CFT including alerts analysis, and possible reporting of Suspicious Transactions as well as to understand new developments in ML/TF/PF techniques, methods, and trends. Further, dedicated awareness sessions will be held for the staff to raise the level of understanding on ML/TF/PF risks.

COMPLIANCE PROGRAMS:

COMPLIANCE PROCESS:

The SOS Capital will develop its comprehensive Compliance Program in terms of regulation 27 of the AML/CFT Regulations:

The Compliance Officer will be appointed at management level CO, reportable to Board or to another equivalent executive position or committee;
There will be a screening procedures for hiring Employees.
There will be suitable training program for relevant employees on annual basis.
The Compliance Officer will have timely access of Customers' record and relevant information.

Responsibilities of CO will include:
ensuring that the internal policies, procedures and controls for prevention of ML/TF are approved by the board of directors and are effectively implemented;
monitoring, reviewing and updating AML/CFT/ 22[CPF] policies and procedures;
providing assistance in compliance to other departments and branches;
timely submission of accurate data/ returns as required under the applicable laws;
monitoring and timely reporting of Suspicious and Currency Transactions to FMU; and
such other responsibilities as may deem necessary in order to ensure compliance with these regulations
Comprehensive Employee due diligence.

COMPLIANCE REVIEW:

The Compliance Officer shall perform the periodic review of branches to check their level of compliance with the provisions in the AML/CFT Policy and Procedures according to their scope / framework.

POLICY REVIEW PERIOD

The AML / CFT Policy will be reviewed on as and when required basis but not later than one year.

GROSSARY

AML/CFT	Anti-Money Laundering and Combating the Financing of Terrorism
ARC	Aliens Registration Card
CCO/CO	Chief Compliance Officer/Compliance Officer
CNIC	Computerized National Identity Card
CTR	Currency Transaction Report
FATF	Financial Action Task Force
FMU	Financial monitoring Unit at SBP
EDD	Enhanced Due Diligence
KYC	Know Your Customer
NICOP	National Identity Card For Overseas Pakistanis
NACTA	National Counter Terrorism Authority
POR	Proof of Registration (For Afghan Nationals)
PEP	Politically Exposed Person
POC	Pakistan Origin Card
RBA	Risk Based Approach
SNIC	Smart National Identity Card
SNICOP	Smart National Identity Card for Overseas Pakistanis
SNIC	Smart National Identity Card
STR	Suspicious Transaction Report
TFS	Targeted Financial Sanctions

APPENDIX – A

COMPLIANCE OFFICER

Job Descriptions

Emp.#	Employee's Name	Qualifications	Experiences	Joining/Appointment Date
			`	
Functionally Reporting to:		Administrative Reporting to:		
Board of Director / Risk & Compliance Committee		Chief Executive Officer/Chief Operating Officer		

Under Securities Brokers (Licensing & Operations) Regulations, 2016, the Compliance Officer is responsible: -

- For ensuring compliance with and performing functions pertaining to the segregation and safekeeping of customer assets.
- To immediately report any non-compliance with any requirement for taking immediate steps to ensure compliance with the regulatory regime.
- Where the SOS Capital fails to take steps as reported by the Compliance Officer, to immediately inform the Securities Exchange and the Commission of the non-compliance.
- To prepare monthly compliance reports for submitting to the board of directors/Risk & Compliance Committee.

Under SECP (Anti Money Laundering and Countering Financing of Terrorism) Regulations, 2018, the Compliance Officer is responsible for the areas including, but not limited to-

- Effective compliance with the relevant provisions of these Regulations, the AML Act, the Anti-Money Laundering Rules, 2008, the Anti-Money Laundering Regulations, 2015 and other directions and guidelines issued under the aforementioned regulations and laws, as amended from time to time;
- ensuring that the internal policies, procedures and controls for prevention of ML/TF are approved by the board of directors and are effectively implemented;
- monitoring, reviewing and updating AML/CFT policies and procedures;
- providing assistance in compliance to other departments and branches;
- timely submission of accurate data/ returns as required under the applicable laws;
- monitoring and timely reporting of Suspicious and Currency Transactions to FMU;
- such other responsibilities as the SOS Capital may deem necessary in order to ensure compliance with these regulations; and
- Review and investigate with suspicion, the transactions, which are out of character, inconsistent with the history, pattern, or normal operation of the account or not commensurate with the level of income of a customer and referred to Compliance Officer for possible reporting to FMU under the AML Act.

Reporting to: The Board of Directors or its Equivalent Executive Position or the Committee
Reporting Period: Daily / Monthly / Quarterly
Urgently as and when need arises.

To oversee the compliance function under the Securities and Exchange Commission of Pakistan (Anti Money Laundering and Countering Financing for Terrorism) Regulations, 2020 ("AML/CFT Regulations"), Securities and Exchange Commission of Pakistan Guidelines on Anti-Money Laundering, Countering Financing of Terrorism and Proliferation Financing("SECP Guidelines"), SECP Directive and Circulars issued from time to time, the Company has appointed above said individual as a Compliance Officer ("CO") at the management level as required under the AML/CFT Regulations with the following main Job Descriptions.

The Company ensures that the Compliance Officer and his subordinate staff shall have timely access to all customer records and other relevant information which they may require to discharge their functions.

JOB DESCRIPTIONS:

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

2. If there is any discrepancy in the Account Opening process, the Compliance Officer shall communicate the same to Front Office/Dealer/Sale Person for rectification before start of Business Relation;

3. In compliance with AML/CFT Regulatory framework, the Compliance Officer shall primarily be responsible to the following areas but not limited to:

   a) Effective compliance with relevant provisions of the AML/CFT Regulations, the AML Act, AML Rules, the AML Regulations, and other directions and guidelines issued under the aforementioned regulations and laws, as amended from time to time;
   b) Ensure that internal policies, procedures and controls for prevention of AML/CFT are approved by the Board of Director of the Company and are effectively implemented;
   c) Monitor, review and updated AML/CFT Policies and Procedures of the Company;
   d) Provide assistance in compliance to other departments and branches of the company;
   e) Timely submit accurate date / returns as required under the applicable laws;
   f) Monitor and timely report Suspicious and Current Transactions to FMR; and
   g) May include such other responsibilities assigned by the Company as it deems necessary in order to ensure compliance with the Regulations.

4. The Compliance Officer shall do the Risk Assessment of the Customer as per AML/CFT Risk Assessment Matrix annexed to SECP Guideline on AML/CFT Regulations;

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

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

   b) Activities which should require further enquiry may be recognizable as falling into one or more of the following categories. This list is not meant to be exhaustive, but includes:

      i. any unusual financial activity of the Customer in the context of the Customer's own usual activities;
      ii. any unusual transaction in the course of some usual financial activity;
      iii. any unusually-linked transactions;
      iv. any unusual method of settlement;
      v. any unusual or disadvantageous early redemption of an investment product;
      vi. Any unwillingness to provide the information requested.

6. The Compliance Officer shall be the point of contact with the supervisory authorities including the Commission and the Financial Monitoring Unit (FMU).

7. The Compliance Office will also be responsible to ensure compliance with other Rules and Regulations applicable under Securities Brokers (Licensing and Operations) Regulations, the Securities Act, the Companies Act, circulars/directives issued by the Securities Exchange, Central Depository, Clearing Company and the Securities & Exchange Commission of Pakistan from time to time including the following:
   a) Ensure segregation of clients' assets;
   b) Ensure statutory filings with front line regulators and the SECP;
   c) Ensure timely submission of net worth, net-capital balances and liquid assets statements;
   d) Ensure maintenance of Assets Under Custody in line with limit as net-worth of the company;

e) Ensure timely replies to all queries, letters and notices from the regulators.
f) Ensure timely sending of daily confirmations to the clients through authorized source of communication.
g) Ensure timely sending of periodic statements to the clients as required under the regulations;
h) Another compliance requirement defined by the regulators through letters, notices and directives, etc.
i) Screening procedures when hiring employees to ensure the integrity and conduct, skills and expertise of such employees to carry out the functions effectively;
j) Ongoing employee training program; and
k) An independent audit function to test the system.

Reviewed by: Chief Executive Officer	Dated: __/__/2024	Approved by: Board of Directors	Dated: __/__/2024

APPENDIX – B

INTERNAL AUDITOR

Job Descriptions

Emp.#	Employee's Name	Qualifications	Experiences	Joining/Appointment Date
Functionally Reporting to:		Administrative Reporting to:		
Audit Committee of the Board		Chief Executive Officer/Chief Operating Officer		

Under Securities Brokers (Licensing & Operations) Regulations, 2016, the Internal Auditor/Function is responsible: -

- To ensure that a periodic or annual review of the internal control system;
- For assessment of overall level of compliance of the SOS Capital;
- For reporting directly to the board of directors or its audit committee;
- To monitor the integrity of the financial statements of the company;
- To review the company's internal controls and risk management systems;
- To make recommendations to the board in relation to appointment or removal of the auditor;
- To approve the remuneration and terms of engagement of the auditor;
- To develop and implement policy on engagement of the auditor to supply non-audit services;

Under SECP (Anti Money Laundering and Countering Financing of Terrorism) Regulations, 2018, the Internal Auditor/Function is responsible for the areas including, but not limited to-

- Test the Anti-Money Laundering (AML) and Countering Financing of Terrorism (CFT) system for implementing counter Money Laundering (ML) and Terrorism Financing (TF) measures having regard to ML and TF Risk and size of the business;
- Conduct an AML/CFT audit to independently evaluate the effectiveness of compliance with AML/CFT Policies and Procedures;
- Asses overall governance structure for AML/CFT, including the role, duties and responsibilities of the Compliance Officer/function;
- Asses the ownership taken by management and board of directors (where applicable), in particular Risk Assessment, Risk Based Approach, AML/CFT related internal enquiries, suspicious transaction reports and regulatory compliance;
- Assess the integrity and effectiveness of the AML/CFT systems and controls and the adequacy of internal policies and procedures in addressing identified risks, including:
  - CDD measures including monitoring and updating of customer data;
  - Screening process for TFS, and test its functionality;
  - testing transactions with emphasis on high–risk customers, geographies, products and services;
  - Record keeping and documentation.
- the effectiveness of parameters for automatic alerts and the adequacy of SOS Capital's process of identifying suspicious activity, internal investigations and reporting;

• The adequacy and effectiveness of training programs and employees' knowledge of the laws, regulations, and policies & procedures. **Audit Period:** The frequency of the audit shall be quarterly in normal course of business but at any time if need arises.

Reviewed by: Audit Committee	Dated: __/__/2024	Approved by: Board of Directors	Dated: __/__/2024

APPENDIX - C

Declaration of Beneficial Owner (Individual)

Sub Account No.: _____

Trading Account No.: _____

Name :	
Father/Husband Name :	
Address :	
Residential Status :	
Nationality :	
CNIC Number :	
Mobile/Cell # :	
Telephone # :	
Email :	
Occupation :	
Relationship with Account Holder :	

I, _____ S/o. _____ holder of CNIC _____ hereby certify that _____ is in my relationship and I am supporting him/her to open and maintain Equity Trading Account with SOS Capital Limited.

_____

BENEFICIAL OWNER SIGNATURE

_____

ACCOUNT HOLDER SIGNATURE

Encl.: 01). Attested Copy of CNIC
02). KYC of Beneficial Owner
03). Copies of Income Tax and Wealth Tax Return and/or Evidence for source of Income and Funds
04). Gift Deed, in case of Student, Housewife or dependent.

_____ _____

COMPLIANCE OFFICER CHIEF EXECUTIVE OFFICER

DATED: _____

APPENDIX – D

DATABASE OF LEGAL PERSON OR LEGAL ARRANGEMENT AND THEIR ASSOCIATES FOR CHECKING THEM AGAINST THE LIST OF DESIGNATED/PROSCRIBED PERSONS

The SOS Capital shall build a database having name of the Customers (corporate entities, trusts, NPO, NGO, individuals and authorized persons), such as:
Legal Person / Legal Arrangement having Backward Beneficial Ownerships of Natural Persons:

Legal Person / Legal Arrangement having Forward Beneficial Ownerships of Natural Persons:

The SOS Capital will search the database of its customers which are Legal Persons, Legal Arrangements or Natural Persons whose Beneficial Owners are different on the following scenarios: -

a) When a business relationship with a new Customer will be established;
b) When the lists of Designated / Proscribed will be updated by NACTA, UNSC and any other Law Enforcement Agencies through SECP;
c) When Account of the Customer will be updated regarding its change in its Board of Directors, Trustee, Nominees, Authorized Persons, etc.
d) When, any new Employee will be hired.
e) Periodically screening of all Customers and their Associates including Board members/Trustees, nominees, Authorized persons as notified by the Commission.

APPENDIX – E

PROCEDURES FOR CUSTOMER DUE DILIGENCE (CDD)

In order to know who its Customers are and it shall not keep anonymous accounts or accounts in fictions names, the SOS Capital shall be required to take the following steps to ensure that its customer is who they purport themselves to be:

PROC #	PROCEDURES PERFORMED	YES / NO	REASON, IN CASE "NO"
1	To identify the customers and verify the identity of that customer using reliable and independent documents, data and information obtaining the following: • Name; • Copy of CNIC; • Copy of Utility Bill to confirm residential address; • Date of Birth; • Proof of Income/Wealth Statement (Latest); • Any other information, if needed.		
2	Identify every person who acts on behalf of the customer by verifying the authority of that person to act on behalf of the customer, if any.		
3	Ongoing due diligence on the business relationship and scrutinize transaction undertaken throughout the course of that relationship to ensure that transaction being conducted are consistent with: • Knowledge of the Customer; • Business; • Risk Profiles as assessed through evidences; • Veracity or adequacy of the previously obtained customer identification information.		
4	**In case of suspicion of ML/TF/PF** Seek to identify and verify the identity of the customer and the beneficial owner(s), irrespective of any specified threshold that might otherwise apply;		
5	Filling of Suspicious Transaction Report (STR) with the FMU, in accordance with the requirement under the law.		
6	Monitor transactions to determine whether they are linked and restructured into two or more transactions of smaller values to circumvent the applicable threshold.		
7	Ensure that they understand the purpose and intended nature of the proposed business relationship or transactions		
8	Verify whether that authorized person is properly authorized to act on behalf of the customer while conducting CDD of the authorized persons(s) using the same standards that are applicable to a customer and ascertaining the reason for such authorization and obtain a copy of the authorization document.		
9	Customer's identification procedure and ongoing monitoring standards for Customer not physically present for identification purposes as for those where the client is available for interview.		

10	Where a Customer has not been physically present for identification purposes, practices will generally not be able to determine that the documentary evidence of identity actually relates to the Customers they are dealing with.		

APPENDIX – E – 1

Senior Management's Approval Note for High Risk Clients

The Customer has been marked as High Risk Customer based on the ANY of the following circumstance:

Sr. #	Circumstance	Applicable (Yes/No), name the category, where required.
1	Customer belonging to country or region which is non-compliant with Anti-Money Laundering according to FATF	
2	Customer is Body corporate, partnership, association or legal arrangement including any of the following: a) NGO b) NPO c) Trust, which receives donations d) Company having nominee shareholders e) Business that have Cash-intensive f) Shell Company, especially in case where there is foreign ownership spreaded across jurisdiction;	
3	Legal Person or Legal Arrangement with complex ownership structure	
4	Politically Exposed Person (PEP) or its associates such as: a) Family member; b) Close associates	
5	Customer with Incomplete Documentations	
6	Customer with undisclosed ownership such as a) House-wife b) Student c) Dependents Children d) Dependent Parents	
7	Customer belonging to Higher Risk Regions within a country as per NRA 2019, which has been exposed to ML/TF risks include any of the following: a) Border Regions; b) Large Goods Transit such as ports; c) Region experiencing social unrest; d) Associated with specific crime patterns such as cash or people smuggling, drug trafficking, violent crimes, fraud and corruption,	
8	a) Individual Customer belonging to the following businesses carrying high risks: b) Non-Resident c) Requested/Applied Amount of Investment/business does not match the profile/particulars of customer; d) Designated Non-Financial Business and Professional, such as i. Real Estate Dealer; ii. Dealer in Precious metal and stones; iii. Accountants	

	iv. Lawyer / Notaries	

As the Customer may pose a higher potential risk to the Company, conducting a business relationship with such customer based on applicable High Risk Circumstance as marked above may expose the Company to risk of channeling illicit money flows. Therefore, the Company will exercise additional caution and conduct Enhanced Due Diligence (EDD) on such Customer by doing the following:

a) Consult publically available information;
b) Consider sanction issued by UN;
c) FATF high risk and non-cooperative jurisdictions,
d) FATF and its regional bodies (FSRBs) and Transparency International Corruption Perception Index (TICPI);
e) Educate on Offshore financial centers;
f) Adequate expertise to understand Customer's ownership structure up to Beneficial Owner and to assess documents presented to the Company.

As per circumstance, the Company will conduct EDD for such High Risk Customer, therefore, the Chief Executive Officer/Chief Operating Officer is recommended to allow continuing business relationship with such Customer.

Recommended by: Approved by:

_____ _____

Name Name

Compliance Officer Designation of Approving Authority (CEO/COO)

Dated: _____

APPENDIX – F

PROCEDURES FOR CUSTOMER SIMPLIFIED DUE DILIGENCE MEASURES (SDD)

The SOS Capital conduct Simplified Due Diligence Measures (SDD) in case of Low Risks identified by it.

The SOS Capital however, shall ensure that the low risk it identifies are commensurate with the low risks identified by the country or the Commission. While determining whether to apply SDD

PROC #	PROCEDURES PERFORMED	YES / NO	REASON, IN CASE "NO"
	Where the risks are low and where there is no suspicion on ML/TF/PF,		
	SDD measures on an applicant/customer, it should document the full rationale behind such decision.		
	Reducing the frequency of customer identification updates;		
	Reducing the degree of on-going monitoring and scrutinizing transactions, based on a reasonable monetary threshold; and		
	Approval from the Senior Management to Low Risk with Proper reasons to mark Low Risk.		

Please similar wording for justifying a Customer carrying Low Risk"

In the case of Bank, NBFC (mutual funds), DFI, Investment banks, investment company, etc. then the following may be appropriate justification. please name:

"As the Customer is a (Bank/NBFI/DFI/MF/IB/IC) who is subject to requirement to combat money laundering and terrorist financing consistent with the FATF recommendations and is supervised for compliance with those requirements, therefore, we have rated it as Low-Risk Customer",

If the customer is published listed company then,
"As the Customer is a public listed company that is subject to regulatory disclosure requirements to ensure adequate transparency of beneficial ownership, therefore, we have rated it as a Low-Risk Customer."

In the case of an individual customer;
"As the Customer is doing transaction only for the purpose of long term investment but within his/her know and verifiable sources of income, therefore, we have rated such Customer as Low-Risk Customer."

In case of an individual having a close relationship of the CEO/Director/Senior Management of the Brokerage House;

"As the Customer has known to CEO/Director/Senior Management for a long time and has provided all verifiable documents of his Customer Due Diligence (CDD), therefore, we have rated such Customer has been rated, Low-Risk Customer."

PROCEDURE FOR ENHANCE DUE DILIGENCE:
(Forms Attached as Appendix – F)

To address the assessed ML/TF risk following controls are implemented and methods are used for high risk clients;

KYC/CDD process is performed for each client which includes the following;

- Approval from senior management for enhanced due diligence
- Biometric verification of the customer (Soft/Hard Copy)
- Verification of customer's identity
- Validation of identity documents through NADRA Verisys (Soft/Hard Copy)
- Full name as per identity document;
- Father/Spouse Name as per identity document;
- Mother Maiden Name;
- Identity document number along with date of issuance and expiry;
- Existing residential address (if different from CNIC);
- Contact telephone number(s) and e-mail (as applicable);
- Nationality-Resident/Non-Resident Status
- FATCA/CRS Declaration wherever required;
- Date of birth, place of birth;
- Incorporation or registration number (as applicable);
- Date of incorporation or registration of Legal Person/ Arrangement;
- Registered or business address (as necessary);
- Nature of business, geographies involved and expected type of counter-parties (as applicable);
- Type of account/financial transaction/financial service;
- Profession / Source of Earnings/ Income: Salary, Business, investment income;
- Purpose and intended nature of business relationship;
- Expected monthly turnover (amount and No. of transactions); and
- Normal or expected modes of transactions/ Delivery Channels.
- Verification of customer's mailing and permanent addresses
- Verification of customer's source of income with supporting documents
- Identification of beneficial owner

The photocopies of identity documents shall be validated through NADRA Verisys or Biometric Verification. The SOS Capital shall retain copy of NADRA Verisys or Biometric Verification (hard or digitally) as a proof of obtaining identity from customer.

In case of a salaried person, in addition to CNIC, a copy of his salary slips or service card or certificate or letter on letter head of the employer will be obtained.

In case of expired CNIC, account may be opened on the basis of attested copies of NADRA receipt/token and expired CNIC subject to condition that SOS Capital shall obtain copy of renewed CNIC of such customer within 03 months of the opening of account.

For CNICs which expire during the course of the customer's relationship, SOS Capital shall design/ update their systems which can generate alerts about the expiry of CNICs at least 01 months before actual date of expiry and shall continue to take reasonable measures to immediately obtain copies of renewed CNICs, whenever expired. In this regard, the Company is also permitted to utilize NADRA Verisys 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.

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.

The condition of obtaining photocopies of identity documents of directors of Limited Companies/Corporations is relaxed in case of Government/Semi Government entities, where we should

obtain photocopies of identity documents of only those directors and persons who are authorized to establish and maintain Business Relationship. However, SOS Capital shall validate identity information including CNIC numbers of other directors from certified copies of 'Form-A/Form-B' and verify their particulars through NADRA Verisys. The Verisys reports should be retained on record in lieu of photocopies of identity documents.

Government entities accounts shall not be opened in the personal names of a government official. Any account which is to be operated by an officer of the Federal or Provincial or Local Government in his/her official capacity, shall be opened only on production of a special resolution or authority from the concerned administrative department or ministry duly endorsed by the Ministry of Finance or Finance Department/Division of the concerned Government.

Explanation: - For the purposes of this regulation the expression "Government entities" includes a legal person owned or controlled by a Provincial or Federal Government under Federal, Provincial or local law.

Minimum documents required for CDD shall be in accordance with Annex 1 of SECP (Anti Money Laundering and Countering Financing of Terrorism) Regulations, 2020.

Screening of customers through UN sanctions committee's website, National Counter Terrorism Authority's website and different SROs issued by the Federal Government
Ongoing monitoring of the clients which includes monitoring of their trading activities and their receipts and payments, etc. Enhanced Due Diligence (EDD) process in which more documentary evidences are obtained from the customers to verify their source of income, etc.

APPENDIX – G

PROCEDURES FOR CUSTOMER ENHANCED DUE DILIGENCE (EDD)

In order to know who its Customers are and it shall not keep anonymous accounts or accounts in fictions names, the SOS Capital shall be required to take the following steps to ensure that its customer are who they purport themselves to be:

PROC #	PROCEDURES PERFORMED	YES / NO	REASON, IN CASE "NO"
	• Additional identification about Nature of Business Relationship.		
	• Ongoing Monitoring of High Risk Client on Regular Interval. • Pattern of Transaction • Internal Control Procedures applied on consistency of the transaction and monitoring of abnormal behavior in the activity of the client. • Volume of Transaction		
	• High Risk Business Relationship • Occupation details • Volume of Assets • Information about source of funds • Proof of Income / Wealth Statement • Information on the source of funds		
	• The reasons for intended or performed transactions.		
	• Selection and Control Procedures applied while selection of clients and transactions.		

	• Monitor transactions to determine whether they are linked and restructured into two or more transactions of smaller values to circumvent the applicable threshold.		
	• Filling of Suspicious Transaction Report (STR) with the FMU, in accordance with the requirement under the law.		
	• The approval of senior management to commence or continue the business relationship.		

APPENDIX – G – 1

Enhanced Due Diligence Form

1. Name: _____
2. CNIC/ Passport#: _____ Account #: _____
3. Cash Transfer Amount and Mode: _____
4. Purpose and reason of cash transfer: _____
5. Frequency of funds transfer in a month: _____
6. Country(s) of funds transfer: _____
7. Customer's source of fund: _____
8. Customer's occupation: _____
09. Name of employer/ business title: _____
10. Annual income of the customer: _____
11. Has the customer ever met the counterparty in person (i.e., Face to face): Yes No
12. Have you ever or you are related to or associated with any individual, holding or had held a senior position in public office with the Government: Yes / No
13. If response to question 12 is "Yes" please mention the position of Public office:
14. Please add any relevant additional information which can assist as a due diligence:

_____
Customer Signature

Date: _____

APPENDIX – G – 2

Customer's Name: _____ CDC-Sub A/c: _____ Trading ID: _____
CUSTOMER'S RISK PROFILE:

Monthly Income in Rs.	Annual Income in Rs.	Last Update	Source (Documents)

Periodic Review From <<Date> to <<Date>>											
Amount in Rupee			Securities Value in Rupee			Profit / Loss Realized but not received	Customer Worth in Rs.	Trading Limit Allowed A	Risk Tolerance (%age) B	Average Trading Exposure C	Exceeds A+B-C
Total Receipt	Total Payment	Available	Total In	Total Out	Available						

In Compliance with relevant Regulations of the SECP (AML/CFT) Regulation 2018:

Regulation Reference	Description
6. Customer Due Diligence (3)(C)	Monitoring of accounts/transactions on ongoing basis to ensure that the transactions being conducted are consistent with the regulated person knowledge of the customer, the customer's business and risk profile, including, the source of funds and, updating records and data/ information to take prompt action when there is material departure from usual and expected activity through regular matching with information already available.
13. Ongoing Monitoring (1)	All business relations with customers shall be monitored on an ongoing basis to ensure that the transactions are consistent with the regulated person' knowledge of the customer, its business and risk profile and where appropriate, the sources of funds.
14. Reporting of Transaction (4)	The transactions, which are out of character, are inconsistent with the history, pattern, or normal operation of the account or are not commensurate with the level of income of a customer shall be viewed with suspicion, be properly investigated and referred to Compliance Officer for possible reporting to FMU under the AML Act.

Request to Client for Evidence:

Based on the Clause _____, you are requested to provide us addition Source of Revenue as your Average Trading Activity is not in line with the Sources of Funds provided by you as mentioned above.
Additional Source of Document, if received:

Date: _____ Amount in Rs. _____ Source Document: _____
Reported by:
Compliance Officer: _____Signature_____

Chief Executive Officer/
Chief Operating Officer: _____Signature_____

PROCEDURE FOR ACCOUNT OPENING, KYC CDD/EDD/AML PROCEDURES AND OTHER PROCESSES:

SUMMARY

This procedure defines the methods used to identify and (where applicable) the standard Account Opening, KYC/AML Procedures and Processes at the Company's premises and services offered. This procedure includes methods:

- To define the methods for identifying the standard Account Opening, KYC/AML Procedures and Processes at the Company's premises and services offered (what they are)
- Customer Identification (Customer visits, Biometric, NACTA Screening, NADRA Verisys)
- Risk Assessment (KYC, SDD, CDD, EDD, Receipt and Payment Monitoring, Trade monitoring, Risk profiling based on customer type, product and service, geography and transaction channels like (profession, residential status, PEP, high net worth, customer type, beneficial owner identification, high risk jurisdiction like cross border, transactions types)
- Simplified Due Diligence
- Customer Due Diligence
- Enhanced Due Diligence
- On-going Monitoring
- Filing CTR/STR to FMU
- Customer database maintenance
- Periodic Reporting to Customers
- Account Closing
- SECP compliance relevant to AML/CFT
- PSX, NCCPL, CDC Reporting

The Compliance Officer is responsible for implementation and risk management of this procedure.

APPLICATION:

This procedure applies to all departments that are interlinked, deals with the Company at all Company's facilities.

This procedure not only applies to typical services, but also deliverables from services, such as reports, schedules, etc.

DEFINITIONS:

Service

"Service" includes any of the following:

- Any the action of helping or doing work for someone
- Perform routine, maintenance or repair work
- Employee as a servant entered into his service agreement.

ACCOUNT OPENING PROCESS

CUSTOMER IDENTIFICATION PROCESS

KYC PROCESS:

RISK ASSESSMENT PROCESS:

Risk Assessment (KYC, SDD, CDD, EDD, Receipt and Payment Monitoring, Trade monitoring, Risk profiling based on profession, residential status, PEP, high net worth, customer type, beneficial owner identification, high risk jurisdiction like cross boarder) are prohibited as a matter of corporate policy.

CUSTOMER DUE DILIGENCE PROCESS:

he success of our business is dependent on the trust and confidence we earn from our employees, customers and shareholders. We gain credibility by adhering to our commitments, displaying honesty and integrity and reaching company goals solely through honorable conduct. It is easy to say what we must do, but the proof is in our actions. Ultimately, we will be judged on what we do.

The Company shall take steps to know who their customers are. The Company shall not keep anonymous accounts or accounts in fictitious names. The Company shall take steps to ensure that their customers are who they purport themselves to be. The Company shall conduct CDD, which comprises of identification and verification of customers including beneficial owners (such that it is satisfied that it knows who the beneficial owner is), understanding the intended nature and purpose of the relationship, and ownership and control structure of the customer.

CLIENT SCREENING PROCESS:

CUSTOMER DUE DILIGENCE
(Forms attached as Appendix – D)

The Company shall take steps to know who their customers are. The Company shall not keep anonymous accounts or accounts in fictitious names. The Company shall take steps to ensure that their customers are who they purport themselves to be. The Company shall conduct CDD, which comprises of identification and verification of customers including beneficial owners (such that it is satisfied that it knows who the beneficial owner is), understanding the intended nature and purpose of the relationship, risk assessment in compliance of NRA 2019 jurisdictions like Iran & Korea, beneficial ownership and control structure of the customer.

SOS Capital shall conduct ongoing due diligence on the business relationship and scrutinize transactions undertaken throughout the course of that relationship to ensure that the transactions being conducted are consistent with the SOS Capital's knowledge of the customer, its business and risk profile (Annex 3), including, where necessary, the source of funds, funds received by foreign or non-resident clients. The Company shall conduct CDD when establishing a business relationship if: (1) there is a suspicion of ML/TF, Annex 4 gives some examples of potentially suspicious activities or "red flags" for ML/TF. Although these may not be exhaustive in nature, it may help The Company recognize possible ML/TF schemes and may warrant additional scrutiny, when encountered. The mere presence of a red flag is not by itself evidence of criminal activity. Closer scrutiny will assist in determining whether the activity is unusual or suspicious or one for which there does not appear to be a reasonable business or legal purpose; or (2) there are doubts as to the veracity or adequacy of the previously obtained customer identification information.

In case of suspicion of ML/TF, SOS Capital should: (1) Seek to identify and verify the identity of the customer and the beneficial owner(s), irrespective of any specified threshold that might otherwise apply; and (2) File a Suspicious Transaction Reporting ("STR") with the FMU, in accordance with the requirements under the Law.

The Company shall monitor transactions to determine whether they are linked. Transactions could be deliberately restructured into two or more transactions of smaller values to circumvent the applicable threshold.

The Company shall verify the identification of a customer using reliable independent source documents, data or information including verification of CNICs from Verisys. Similarly, The Company shall identify and verify the customer's beneficial owner(s) to ensure that the company understands who the ultimate beneficial owner is.

The Company shall ensure that they understand the purpose and intended nature of the proposed business relationship or transaction. The Company shall assess and ensure that the nature and purpose are in line with its expectation and use the information as a basis for ongoing monitoring.

The Regulations require The Company to identify and verify the identity of any person that is purporting to act on behalf of the customer ("authorized person"). The SOS Capital should also verify whether that authorized person is properly authorized to act on behalf of the customer. The Company shall conduct CDD on the authorized person(s) using the same standards that are applicable to a customer. Additionally, The Company shall ascertain the reason for such authorization and obtain a copy of the authorization document.

The Company may differentiate the extent of CDD measures, depending on the type and level of risk for the various risk factors. For example, in a particular situation, they could apply normal CDD for customer acceptance measures, but enhanced CDD for ongoing monitoring, or vice versa. Similarly, allowing a high-risk customer to acquire a low risk Page 13 of 40 product or service on the basis of a verification standard that is appropriate to that low risk product or service, can lead to a requirement for further verification requirements, particularly if the customer wishes subsequently to acquire a higher risk product or service.

When performing CDD measures in relation to customers that are legal persons or legal arrangements, The Company should identify and verify the identity of the customer, and understand the nature of its business, and its ownership and control structure.

ENHANCED DUE DILIGENCE:
The Company should examine, as far as reasonably possible, the background and purpose of all complex, unusual large transactions, and all unusual patterns of transactions, that have no apparent economic or lawful purpose with high risk assessment;

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.

Where the risks of ML/TF are higher, or in cases of unusual or suspicious activity, The Company should conduct enhanced CDD measures, consistent with the risks identified. In particular, The Company should increase the degree and nature of monitoring of the business relationship, in order to determine whether those transactions or activities appear unusual or suspicious.

Examples of enhanced CDD measures that could be applied for high-risk business relationships include:

a) Obtaining additional information on the applicant/customer (e.g. occupation, volume of assets, information available through public databases, internet, etc.).

b) Updating more regularly the identification data of applicant/customer and beneficial owner.
c) Obtaining additional information on the intended nature of the business relationship.

d) Obtaining additional information on the source of funds or source of wealth of the applicant/customer.

e) Obtaining additional information on the reasons for intended or performed transactions.

f) Obtaining the approval of senior management to commence or continue the business relationship.

g) 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.

In case of accounts where the accountholder has instructed the SOS Capital not to issue any correspondence to the accountholder's address. Such accounts do carry additional risk to the Company, and they should exercise due caution as a result. It is recommended on a best practice basis that evidence of identity of the

accountholder should be obtained by the SOS Capital. "Hold Mail" accounts should be regularly monitored and reviewed and the SOS Capital should take necessary steps to obtain the identity of the account holder where such evidence is not already in the SOS Capital file.

High-Risk Countries& Jurisdictions:

Certain countries are associated with crimes such as drug trafficking, fraud and corruption, and consequently pose a higher potential risk to the company. Conducting a business relationship with an applicant/customer from such a country exposes the SOS Capital to reputational risk and legal risk.

The Company should exercise additional caution and conduct enhanced due diligence on individuals and/or entities based in high-risk countries.
Caution should also be exercised in respect of the acceptance of certified documentation from individuals/entities based in high-risk countries/territories and appropriate verification checks undertaken on such individuals/entities to ensure their legitimacy and reliability.

The Company are advised to consult publicly available information to ensure that they are aware of the high-risk countries/territories. While assessing risk of a country, The Company are encouraged to consider among the other sources, sanctions issued by the UN, the FATF high risk and non-cooperative jurisdictions, the FATF and its regional style bodies (FSRBs) and Transparency international corruption perception index.

Useful websites include: FATF website at www.fatf-gafi.org and Transparency International, www.transparency.org for information on countries vulnerable to corruption.

ON-GOING MONITORING
Once the identification procedures have been completed and the business relationship is established, the RP 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 Company shall conduct ongoing monitoring of their business relationship with their customers. Ongoing monitoring helps The Company to keep the due diligence information up-to-date, and review and adjust the risk profiles of the customers, where necessary.

The Company shall conduct on-going due diligence which includes scrutinizing the transactions undertaken throughout the course of the business relationship with a customer.

SOS Capital should develop and apply written policies and procedures for taking reasonable measures to ensure that documents, data or information collected during the identification process are kept up-to-date and relevant by undertaking routine reviews of existing records.

The Company shall consider updating customer CDD records as a part its periodic reviews (within the timeframes set by the SOS Capital based on the level of risk posed by the customer) or on the occurrence of a triggering event, whichever is earlier. Examples of triggering events include:

a) Material changes to the customer risk profile or changes to the way that the account usually operates;
b) Where it comes to the attention of the SOS Capital that it lacks sufficient or significant information on that particular customer;
c) Where a significant transaction takes place;
d) Where there is a significant change in customer documentation standards;
e) Significant changes in the business relationship.

Examples of the above circumstances include:

a) New products or services being entered into,
b) A significant increase in a customer's salary being deposited,
c) The stated turnover or activity of a corporate customer increases,
d) (A person has just been designated as a PEP,

e) The nature, volume or size of transactions changes.

The Company should 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: (1) transaction type (2) frequency (3) amount (4) geographical origin/destination (5) account signatories

However, if SOS Capital has a suspicion of ML/TF or becomes aware at any time that it lacks sufficient information about an existing customer, it should take steps to ensure that all relevant information is obtained as quickly as possible

It is recognized that the most effective method of monitoring of accounts is achieved through a combination of computerized and human manual solutions. A corporate compliance culture, and properly trained, vigilant staff through their day-to-day dealing with customers, will form an effective monitoring mechanism.

Whilst some The Company may wish to invest in expert computer systems specifically designed to assist the detection of fraud and ML/TF, it is recognized that this may not be a practical option for many The Company for the reasons of cost, the nature of their business, or difficulties of systems integration. In such circumstances The Company will need to ensure they have alternative systems in place for conducting on-going monitoring.

FILING CTR/STR TO FMU
After suspicion filing STR/CTR to FMU through its online portal

CUSTOMER DATABASE MAINTENANCE
Maintenance of proper KYC database of all active clients for their activity monitoring.

PERIODIC REPORTING TO CUSTOMERS
Forwarding quarterly client balance statement through email/physically

ACCOUNT CLOSING
Account closing after obtaining customer request and settling his/her all assets and liabilities outstanding with the house.

SECP COMPLIANCE RELEVANT TO AML/CFT:
Reporting of Suspicious Transactions / Currency Transaction Report:

A suspicious activity will often be one that is inconsistent with a customer's known, legitimate activities or with the normal business for that type of account. Where a transaction is inconsistent in amount, origin, destination, or type with a customer's known, legitimate business or personal activities, the transaction will be considered unusual, and Company will put the case "on enquiry". The Company will also pay special attention to all complex, unusual large transactions, and all unusual patterns of transactions, which have no apparent economic or visible lawful purpose.

Where the enquiries conducted by the Company do not provide a satisfactory explanation of the transaction, it may be concluded that there are grounds for suspicion requiring disclosure and escalate matters to the CO.

Enquiries regarding complex, unusual large transactions, and unusual patterns of transactions, their background, and their result will be properly documented, and made available to the relevant authorities upon request. Activities which will require further enquiry may be recognizable as falling into one or more of the following categories. This list is not meant to be exhaustive, but includes:

a) any unusual financial activity of the customer in the context of the customer's own usual activities;
b) any unusual transaction in the course of some usual financial activity;
c) any unusually-linked transactions;
d) any unusual method of settlement;

e) Any unwillingness to provide the information requested.

Where cash transactions are being proposed by customers, and such requests are not in accordance with the customer's known reasonable practice, the Company will need to approach such situations with caution and make further relevant enquiries. Company will set its own parameters at Rs. 25,000 for the identification and further investigation of cash transactions.

Where the Company will be unable to satisfy that any cash transaction is reasonable it will be considered as suspicious. The Company will also be obligated to file Currency

Transaction Report ("CTR"), to FMU for a cash based transaction involving payment, receipt, or transfer of Rs. 2 million and above.

If the Company decides that a disclosure should be made, the law require the Company to report STR without delay to the FMU, in standard form as prescribed under AML Regulations 2015. The STR prescribed reporting form can be found on FMU website through the link.
http://www.fmu.gov.pk/docs/AMLRegulations2015.pdf.

The process for identifying, investigating and reporting suspicious transactions to the FMU is clearly specified in the Company's KYC/CDD SOPs and communicated to all personnel through regular training. The Company will also be required to report total number of STRs filed to the Commission on a bi-annual basis within seven days of close of each half year. The CO will ensure prompt reporting in this regard. The Company will evolve a vigilance system for the purpose of control and oversight, which requires maintenance of a register of all reports made to the FMU. Such registers will be maintained and updated by CO and will contain details of:

a) the date of the report;
b) the person who made the report;
c) the person(s) to whom the report was forwarded; and
d) Reference by which supporting evidence is identifiable.

The Company as a matter of policy will turn away business where an applicant or a customer is hesitant/fails to provide adequate documentation (including the identity of any beneficial owners or controllers), consideration will be given to filing an STR to the FMU.

For existing customers, once suspicion has been raised in relation to an account or relationship, in addition to reporting the suspicious activity, the Company will ensure that appropriate action is taken to adequately mitigate the risk of the Company being used for criminal activities. This will include a review of either the risk classification of the customer or account or of the entire relationship itself. In such cases an escalation will be made to the Chief Executive Officer to determine how to handle the relationship, taking into account any other relevant factors, such as cooperation with law enforcement agencies or the FMU.