Punjab Skills Development Fund

Anti-Money Laundering and Countering the Financing of Terrorism Policy

Approval Date:	January 28, 2020
Effective Date:	January 28, 2020
Version Number:	1
Last Review Date:	-
Next Review Date:	-
Policy Owner:	Board of Directors
Approval Authority Signature:	

Contents

1. Purpose

The policy has been generated to ensure that:

- Every person covered under the policy comply with all applicable Anti-Money Laundering and Countering the Finance of Terrorism (AML/CFT) rules & regulations of Pakistan and other jurisdictions in which its stakeholders operates.
- No customer or transactions involved in ML/TF should be acceptable
- AML activities are embedded throughout the programme cycle, from design through implementation, delivery and review with controls routinely reviewed to ensure they remain effective;
- PSDF systems and processes are fit for purpose with adequate controls that adhere to legislative and policy requirements including support of PSDF's zero tolerance approach;
- PSDF should establish an appropriate framework to prevent ML/TF and conduct the following measures:
    - Risk assessment of ML/TF
    - Customer Due Diligence such as KYC for preventing ML/TF
    - Suspicious activity reporting and implementing applicable measures

2. Policy Statement

Punjab Skills Development Fund (PSDF), herein after referred to as "the Fund", is committed to full compliance with all applicable laws and regulations regarding anti-money laundering procedures. The Fund has adopted and will enforce the provisions set forth in Anti-Money Laundering/Countering the Financing of Terrorism (AML/CFT) Guidelines for Non-Profit Organization in order to prevent and detect money laundering, terrorist financing and other illegal activities.

If the Fund, its personnel and/or premises are being used for money laundering or other illegal activities, PSDF can be subject to potentially serious civil and/or criminal penalties. Therefore, it is imperative that every member, officer, and employee is familiar with and complies with the policies and procedures set forth in this Compliance Manual.

Anti-money laundering and Counter Terrorist Finance policy ("the Policy") is designed to assist all stakeholders in adhering to the Fund's policy and procedures.

3. Scope

The Policy applies to the Fund, its Directors, officers, senior management and employees, whether contractual or temporary, and requires all such persons to comply with the relevant applicable AML/CFT rules and regulations at all time.

The laws and regulations applicable on the PSDF include, but are not limited to, the following:

- AML/ CFT Guidelines for Non-Profit Organization (NPOs)
- Anti-Money Laundering Act, 2010;
- Anti-Terrorism Act, 1997;
- Companies Act, 2017;
- Associations with Charitable and Not for Profit Objects Regulations, 2018;

- Income Tax Ordinance, 2001;
- Prevention of Electronic Crimes Act, 2016.

4. Definitions

4.1 **"Money Laundering",** also referred to as "ML", is the movement of cash or other assets generated from illegal activities through legitimate financial institutions or businesses to conceal the source of the funds or make it appear that the source of funds is, in fact, legitimate. A closely related issue is the channelling of funds to support illegal activities (e.g. terrorism).

Types of Money Laundering Transaction

Money Laundering Transactions may include, but are not limited to, the following:

- Giving advice to a potential or existing client, employee or officer on how to structure a transaction to avoid reporting and/or record keeping requirements;
- Engaging in any activity designed with an intention to hide the nature, location, source, ownership or control of proceeds of criminal activity;
- Engaging in any activity while wilfully or recklessly disregarding the source of the funds or the nature of the Clients transaction;
- Dealing in funds to facilitate criminal activity; or
- Dealing in the proceeds of criminal activity.

Money laundering may also involve the proceeds of drug dealings, terrorist activities, arms dealings, mail fraud, bank fraud, wire fraud or securities fraud, among other activities.

- **"Terrorist financing",** or "TF", generally refers to carrying out transactions involving funds that may or may not be owned by terrorist, or that have been, or are intended to be, and used to assist the commission of terrorism;
- **"Beneficiary",** for the purpose of the Policy, means Trainees to whom training is being provided though PSDF;
- **"Contractors",** for the purpose of this Policy, means current or potential prospective, Training Service Providers (TSPs), vendors, suppliers, Partners or any other Contractor;
- **"Relevant Person",** for the purpose of this Policy, means employees/ officers of PSDF who is hiring the Contractor, or whose request the Contract is being carried out by the PSDF;
- **"AML/CFT"** means "anti-money laundering / countering the financing of terrorism";
- **"CDD"** means "Client Due Diligence". This includes "SDD", which means "Simplified Due Diligence" and "EDD", which means "Enhanced Due Diligence";
- **"ERM Framework"** means Enterprise-wide Risk Management Framework, developed by the Audit Risk and Compliance Department (ARC Dept.) of the PSDF for effective management of the risks involved in all PSDF's activities;
- **"Financial Action Task Force (FATF)"** is an intergovernmental organization founded in 1989 on the initiative of the G7 Countries with an objective to develop and promote policies and protocols at both national and international level to protect the global financial system against money laundering, terrorist financing and other related matters;
- **"CEO"** means "Chief Executive Officer" of the PSDF;
- **"Compliance Officer"** means an independent person responsible to ensure effective compliance with the relevant provisions of the AML Act & Regulations and other directions and guidelines issued under the aforementioned regulations and laws, as amended from time to time by the Regulator;

- **"Guidelines"** means Anti-Money Laundering/Countering the Financing of Terrorism (AML/CFT) Guidelines for Non-Profit Organizations (NPOs);
- **"Business Relationship"** means provision of any service by an organization. It may include sponsor, vendor, partnership or outsourcing relationship;
- **"Commission",** under this policy, means Securities Exchange Commission of Pakistan.

5. General Controls to Prevent Money Laundering/Terrorist Finance

PSDF should establish and maintain a sound system to prevent, detect & report money laundering. It is the responsibility of the PSDF management to ensure that adequate systems are in place to prevent and report Money Laundering. General controls that may be used to prevent money laundering may be as follows:

- To put in place the Policy and to ensure continuing compliance with the Policy and the Rules & Regulations. Guidance should be given to employees in respect of the understanding and interpretation of the Policy by the Fund.
- To appoint a CO. Provide training to the CO to enable him to understanding his roles and responsibilities and to perform his duties properly.
- To establish / enhance record keeping systems for all transactions & the verification of client's' identity;
- To establish internal suspicion reporting procedures (Annexure III);
- To educate and train all staff, including the CO, with the main requirements of the applicable AML/CFT Rules & Regulations.

6. Specific Controls to Prevent Money Laundering/ Terrorism Financing

6.1 The Three Lines of Defence

PSDF should establish the following mechanisms for countering Money Laundering & Terror Financing:

- The First line of defence is the employees and officers. Every officer and employee of PSDF should know and carry out the AML/CFT due diligence procedures stated in the Policy. Clear guidance in writing should be communicated to all employees in order to further elaborate the process. Every employee should be familiar with the Internal suspicion reporting procedures (Annexure III) for detecting, monitoring & reporting suspicious transactions;
- The CEO should be responsible for ensuring that there are robust governance, risk management and internal control arrangements across the whole organisation. The CEO should be supported by the Board, in ensuring that policies and procedures are put in place and are communicated to the employees.
- Second line activities are associated with oversight of the management activity through Compliance Officer (CO).
- The Board should appoint a suitably qualified and experienced person as CO, independent from the management, who is fit and proper to meet the criteria of position and authority and ability to oversee the effectiveness of PSDF's AML/CFT policy, compliance with applicable laws & regulations and directives, implementation of compliance program and provide guidance in day to day operations relating to AML/ CFT policies and procedures. The CO must have the authority & ability to oversee the effectiveness of AML/CFT systems, compliance with applicable laws and legislation and provide guidance with day-to-day operations of the Policy and the related procedures.

- The primary responsibilities of the CO are listed in Annexure IV.

- ARC Dept. shall be the third line of defence which shall conduct periodically independent AML/CFT regulatory compliance audits and reviews as per its management plan under the ERM framework. Such audits should be based on the nature, size, complexity and risks identified during the risk assessments. The report of the ARC Dept. should be sent to Board Audit and Finance Committee for review and presented to the Board on periodic basis.

- The objective of these audits and reviews shall be to evaluate the effectiveness and adequacy of internal policies and procedures including compliance with AML/CFT and overall adequacy, integrity and effectiveness of systems.

7. Client Identification

PSDF's anti-money laundering policies and procedures are intended to ensure that, prior to establishing any business relationship all reasonable and practical measures are taken to confirm the client identities. In case PSDF appoints a third party for Client Identification, PSDF should verify that the third party, such as an accounting firm, a bank and other financial intermediary, or any other third party adheres to the same standards.

PSDF's Client Identification Procedures are based on the premise that PSDF will sign a new contract or renew the old one only after:

- PSDF has confirmed the Contractor's identity and that the Contractor is acting as a principal and not for the benefit of any third party, unless specific disclosure to that effect is made; or

- If the Contractor is acting on behalf of others, PSDF has confirmed the identities of the underlying third parties.

    - A contractor 'Know Your Customer' (KYC) Checklist is used (Annexure I). The Checklist should be filled by the Relevant Person at the initial stage, prior to establishing the business relationship. Employees are encouraged to provide the CO with any revision they consider appropriate. The filled KYC Checklist should be forwarded to CO by the Relevant Person for risk assessment.

    - The CO shall retain copies of all documents reviewed or checklists completed in connection with its KYC Procedures in accordance with PSDF's record retention practice, however not less than 5 years.

7.1 Risk Assessment

- The CO should be responsible for the risk assessment process. The CO shall, before determining the level of overall risk and the appropriate level and type of mitigation to be applied, take into account all the relevant risk factors, such as geography, products and services, delivery channels, types of customers, or jurisdictions within which or its customers do business.

- The risk in the Client relationship should be assessed through identification of the risk factors. Client relationships should be classified with respect to their ML/TF risk categories i.e. High and Low to be determined through customer risk profiling performed through KYC to take informed decision regarding whether to initiate Simplified or Enhanced Due Diligence. .

- PSDF ARC Dept. should monitor and evaluate the implementation of mitigating controls and make improvements where necessary; Risk assessment should be an ongoing process (Preferably every 12-18 months) and the risks-based approach should be documented.

- All TSP should be subject to EDD, irrespective of the results of KYC.

- In the case of some very high-risk situations, which are outside the PSDF's risk tolerance, PSDF may decide not to accept the contract or may exit from an existing relationship. In addition, the effectiveness of the risk mitigation procedures and controls, and identify areas for improvement, where needed.

7.2 Risk Factors

Risk should be assessed according to the factors identified by the Fund. Examples and factors of low risk level of ML/FT in the specific case are listed in Annexure V.

In making the assessment, relevant persons must bear in mind that the presence of one or more risk factors may not always indicate that there is a low risk of money laundering and terrorist financing in a particular situation.

Factors that may indicate high risk of ML/FT that require for an increased scrutiny for AML/CFT purposes are listed in Annexure VI.

7.3 Simplified Due Diligence Procedures

PSDF may conduct Simplified Due Diligence (SDD) in case level of risk assigned to the Contractor in the KYC Checklist in low. Where PSDF decides to take SDD measures on a Contractor, it should document the full rationale behind such decision and make available that documentation to the Commission on request.

Where the CO is satisfied that the contractor falls under SDD criteria, then the only requirement is to verify Contractor's identification using the KYC Checklist (Annexure I).

A CO must not continue to apply SDD measures:

- if it doubts the veracity or accuracy of any documents or information previously obtained for the purposes of identification or verification;

- if its risk assessment changes and it no longer considers that there is a low degree of risk of money laundering and terrorist financing;

- if it suspects money laundering or terrorist financing.

7.4 Enhanced Client due Diligence Procedures for High Risk Contractors

Where the CO has assessed High risk from the KYC Checklist, CO should undertake Enhanced Due Diligence Procedures in order to mitigate the risk (Annexure II)

The CO may differentiate the extent of EDD procedures, depending on the type and level of risk for the various risk factors. The enhanced due diligence procedures undertaken with respect to 'high risk' Contractors must be thoroughly documented in writing, along with the results of the procedures and the basis of the conclusion reached.

7.5 Approval of Contracts with High Risk Contractors

When EDD measures has been applied due to higher risk assessed in a certain business relationship, such business relationship should not be established unless prior approval has been obtained from the CEO.

7.6 Know Your Donors or Sponsors

- Before receiving funds from a sponsor, CO must establish that the Sponsor is not placed on the United Nations' list of persons who are linked to terrorist financing or against whom a ban, sanction or embargo subsists.

- CO shall undertake best efforts to document the identity of their significant sponsor. CO must collect and maintain record or correct and complete identification particulars of major sponsors.

- CO shall conduct, on a risk-based approach, a reasonable search of public information, including information available on the Internet, to determine whether the donor or their key employees, board members or other senior managerial staff are suspected of being involved in activities relating to terrorism, including terrorist financing.

7.7 Politically Exposed Persons (PEPs)

- Business relationships with persons holding important public positions and with individuals or companies associated to them may expose PSDF to high reputational and/or legal risk. The risk occurs when public power is abused by such persons for either their own personal benefit and/or benefit of others through illegal activities such as the receipt of bribes or fraud.

- PSDF is encouraged to be vigilant in relation to PEPs from all jurisdictions, who are seeking to establish business relationships. PSDF should, in relation to PEPs, in addition to performing normal EDD measures conduct ongoing monitoring of the business relationship with PEPs.

7.8 Customer's Record Retention

- Copies of all documents should be retained for at least five (5) years according to the PSDF retention practice. This should include copies of documents reviewed in connection with KYC Checklist and enhanced due diligence procedures.

- PSDF should maintain, for at least 5 years after termination, all necessary records on transactions to be able to be able to comply swiftly with information requests from the competent authorities. Such record should be sufficient to permit the reconstruction of individual transactions, to provide, if necessary, evidence for prosecution of criminal activity.

7.9 Review of Existing Client Base

- The CO shall coordinate a periodic review of the PSDF's existing Client list, and ensure the adequacy of due diligence performed on existing clients

- In addition, PSDF's policies, procedures and controls should provide for the detection of suspicious activity, and if detected may require further review to determine whether the activity is suspicious.

7.10 On-going Monitoring & Business Relationships

- All business relationships should be monitored on an on-going basis in order to make sure that the transactions are in accordance with the PSDF's knowledge of the Contractors, its business and risk profile and its sources of funds.

- PSDF shall be vigilant for any significant changes or inconsistencies in the pattern of transactions. Inconsistency is measured against the stated original purpose of the accounts. Possible areas to monitor could be transaction type, frequency, amount, geographical origin/destination, account signatories, parties behind the contract, change is requirements of the Contractor.

8. Confidentiality

Management, employees and others working on behalf of PSDF must ensure that neither the Contractors nor another unauthorised party receives knowledge that a report as referred to a competent authority or that an investigation due to suspected money laundering has been initiated. Furthermore, the same parties should not inform the Contractor, or indicate to the contractor, by any means that the transaction is the object of an investigation following a report from another party, so that they become aware of such an investigation.

9. Responsibility of PSDF towards its employees

PSDF shall ensure that information as to what employee reported a customer's suspicious transaction is kept secret and the employee's name shall not be disclosed, for instance, in reports to the Relevant Authority unless there is a critical reason for so doing.

In such case, the Fund must also take necessary measures to protect those employees involved in the report on the customer's transaction against threats or hostile actions by Contractors following such reports.

10. Internal Controls

PSDF is expected to have systems and controls that are comprehensive and proportionate to the nature, scale and complexity of their activities and the ML/TF risks that are identified.

10.1 Audit, Risk and Compliance Department

PSDF should, on a regular basis, conduct an AML/CFT audit to independently evaluate the effectiveness of compliance with AML/CFT policies and procedures. The frequency of the audit should be commensurate with PSDF's nature, size, complexity, and risks identified during the risk assessments.

10.2 Outsourcing

PSDF shall conduct the due diligence on the proposed Contractor to whom it intends to outsource as appropriate and ensure that the Contractor is fit and proper to perform the activity that is being outsourced.

PSDF shall ensure that the outsourcing agreement requires Contractors to file a STR with the FMU in case of suspicions arising in the course of performing the outsourced activity.

10.3 Employee Screening

PSDF should maintain adequate policies and procedures to screen prospective and existing employees. The extent of employee screening should be proportionate to the potential risk associated with ML/TF in relation to the business in general, and to the particular risks associated with the individual positions.

10.4 Anti-Money Laundering Employee Training Program

To ensure the continued adherence to PSDF's anti-money laundering policies and procedures, , all employees are expected to be fully aware of PSDF's anti-money laundering policies and procedures and to reconfirm their awareness of the contents of this Compliance Manual by signing the acknowledgement form annually, or more frequently, as required by the CO.

11. Review

The Chief Internal Auditor and the CO shall be responsible for keeping this document updated from time to time. This policy in its entirety shall be reviewed at least annually and updated, if necessary, and approved by the Board of Directors.

12. Effective Date

The AML/CFT Policy will be effective from the date of its approval by the Board of Directors i.e. January 28, 2020.

Annexes

Annexure I- Know Your Customer (KYC) Checklist

For Individual Contractor

Regional Office: _____

D	D	M	M	Y	Y	Y	Y

Business Relationship: _____

Name: (in block letter as per CNIC)

Address:

Date of Birth:

D	D	M	M	Y	Y

Gender: ☐ **Male** ☐ **Female** ☐ **Others**

VERIFICATIONS

ID Document Type
(Please fill only relevant ID details)

☐ CNIC# ☐ NICOP # ☐ Passport #

Issuance date:

D	D	M	M	Y	Y

Expiry date:

D	D	M	M	Y	Y

Source of Income: ☐ ☐ Salaried Individual

Non-Salaried, please specify the source of income:

_____

_____

Other Details (Please write in block letters)

Father's/ Spouse Name		**Country Of residence**	
Mother's Name		**Telephone Number**	
NTN of the Contractor		**Email Address**	

Nationality	☐ Pakistan ☐ Others, please specify_____	**Fax Number (if any)**	
Marital Status	☐ Single ☐ Married	**Any present or past affiliation with the Government**	
Occupation			

BENEFICIAL OWNERSHIP (Natural person(s) who ultimately owns or controls the Individual Contractor or on whose behalf, the contract is being executed. Please provide below details if beneficiary is other than the singing party).

Name	Identity Document (CNIC/SNIC/NICOP/PASSPORT)	Document No.	Issuance Date (DD/MM/YYYY)	Expiry Date (DD/MM/YYYY)

I hereby declare that the details furnished above are true and correct to the best of my knowledge and belief and I undertake to inform you of any changes therein, immediately. In case any of the above information is found to be false or untrue or misleading or misrepresenting, I am aware that I may be held liable for it.

Declaration from the Contractor:

_____ Date (DD/MM/YYYY)	_____ Contractor's Signature/ Thumb Impression

FOR OFFICE USE ONLY – Relevant Person

Copies of required documents mentioned in below annexure obtained?

☐ Yes ☐ No _____

Signature of the relevant person:

Name of the relevant person:

FOR OFFICE USE ONLY – Compliance Officer

PROFILE OF CONTRACTOR

☐ Politically Exposed Person ☐ Company Registered u/s 42 ☐ Forex dealer, real estate agent or travel agent

☐ Banks, financial institutions ☐ Others (please specify)

Copies of identity documents obtained? ☐ Yes ☐ No

For salaried person, in addition to identity documents, a copy of his/her service card or letter on letter head of employer obtained? ☐ Yes ☐ No

Verisys" identity verification of customer & beneficial ☐ Yes ☐ No _____ (Comments in case of No)

UN Sanctions ☐ Yes ☐ No _____ (Comments in case of No)

NACTA ☐ Yes ☐ No _____ (Comments in case of No)

CDD/KYC Category ☐ High Risk ☐ Low Risk

Brief comment on the basis of the risk assessment:

I certify that all information and documentation required as per AML/CFT Regulations have been obtained and identity verifications and sanction screening from relevant websites has been performed and found satisfactory.

Compliance Officer's Signature

For Corporate Contractors

Regional Office: _____

D	D	M	M	Y	Y	Y	Y

Business Relationship:

_____

Company/Organization Name: (in block letter as per Certificate of Incorporation/ Registration with Registrar of Firms, License issued by SECP, etc.)	
Company/Organization address:	
Company/Organization's National Tax Number (NTN):	
Contact Number:	

CUSTOMER CATEGORY

☐ Sole proprietor	☐ AOP/Partnership	☐ Private Limited Company
☐ Public Listed Company	☐ Public Unlisted Company	☐ Public Sector Company
☐ Government	☐ Autonomous body	☐ NGO, Trust, Welfare/Cooperative Society
☐ Multinational Company	☐ Others (Please specify) _____	

INDUSTRY TYPE/LINE OF BUSINESS

☐ Bank	☐ Power & Energy/Oil & Gas Real Estate	☐ Trading/Manufacturing
☐ Services	☐	☐ Others (Please specify) _____

IDENTITY INFORMATION OF ALL DIRECTORS/PARTNERS/TRUSTEES, ETC.

Name	Identity Document (CNIC/SNIC/NICOP/PASSPORT)	Document No.	Issuance Date (DD/MM/YYYY)	Expiry Date (DD/MM/YYYY)

BENEFICIAL OWNERSHIP (Natural or legal person(s) who ultimately own or control the Company/Organization)

_____

Name	Identity Document (CNIC/SNIC/NICOP/PASSPORT)	Document No.	Issuance Date (DD/MM/YYYY)	Expiry Date (DD/MM/YYYY)

Declaration from the Contractor:

I hereby declare that the details furnished above are true and correct to the best of my knowledge and belief and I undertake to inform you of any changes therein, immediately. In case any of the above information is found to be false or untrue or misleading or misrepresenting, I am aware that I may be held liable for it.

Date (DD/MM/YYYY)	Contractor's Signature/ Thumb Impression

FOR OFFICE USE ONLY – Relevant Person

Copies of required documents mentioned in below annexure obtained?

☐ Yes ☐ No, in case of No, please specify _____

Signature of the relevant person:

Name of the relevant person:

FOR OFFICE USE ONLY – Compliance Officer

"Verisys" identity verification of Directors/partners/trustees,	☐ Yes	☐ No _____ (Comments in case of No)
etc. & beneficial owner(s) mentioned above	☐ Yes	☐ No_____ (Comments in case of No)
NACTA screening	☐ Yes	☐ No_____ (Comments in case of No)
NTN verification	☐ Yes	☐ No_____ (Comments in case of No)

CUSTOMER RISK CATEGORY

CDD/KYC Risk Category	☐ High Risk	☐ Low Risk

Brief comment on the basis of the risk assessment:

I certify that all information and documentation required as per **AML/CFT Regulations** have been obtained and identity verifications and sanction screening from relevant websites has been performed and found satisfactory.

Compliance Officer's Signature

Annexure: Documents required for KYC Checklist

Customer Type	Documents required	Documents obtained	
		YES	NO
Sole proprietorship	Copies of ID documents (CNIC, SNIC, NICOP, Passport, etc.)		
	Copy of registration certificate		
	Copy of certificate or proof of membership of trade bodies (if applicable)		
	Declaration of sole proprietorship on business letter head		
Partnership	Copies of ID documents of all partners		
	Copy of Partnership deed		
	Copy of Registration Certificate with Registrar of firms. In case the unregistered partnership, this shall be mentioned above in customer category		
	Authority letter from all partners, in original, authorizing the person(s) to execute the contracts		
Companies/Corporations	Copies of ID documents of all Directors		
	Copy of Board of Directors (BoD) resolution specifying the person(s) authorized to sign insurance contracts		
	Memorandum and Articles of Association		
	Certificate of Incorporation		
	Certificate of Commencement of Business (for public companies)		
	Copy of 'Form-A/Form-B, & Form 29		
Multinational/Foreign Companies and/or Branch/Liaison office of Foreign Company	Copies of ID documents of all Directors/country managers, etc. along with particulars of all such persons on Company's letterhead		
	Authority letter from principal office authorizing the person(s) to execute insurance contracts		
	A copy of permission letter from relevant authority		
NGOs/NPOs/Charities, Trust, Clubs, Societies and Associations, etc.	Copy of certificate of registration/incorporation, instrument of Trust, etc.		
	Copy of by-laws/rules & regulations		
	Resolution of the Governing Body/Board of Trustees/Executive Committee, etc. authorizing person(s) to execute contracts		
	Copies of ID documents of the authorized person(s) above and of the members of Governing Body/Board of Trustees /Executive Committee, etc.		
	Other documents as deemed necessary including annual accounts/ financial statements which may help to ascertain the detail of activities, sources and usage of funds in order to assess the risk profile of the organization		
Agents	Copy of 'Power of Attorney' or 'Agency Agreement'		
	Copy of ID document of the agent and principal		
	If the agent or the principal is not a natural person, then the documents would be obtained on the basis of above customer category.		
Executor & Administrator	Copies of ID documents of executor/administrator		
	Copy of letter of administration of probate		

Annexure II- Enhanced Due Diligence Procedures

Enhanced Client Identification Procedures for 'high risk' Contractor includes, but are not limited to, the following:

- Assessing the Contractor's business reputation through review of financial or professional references, generally available media reports or by other means;
- Considering the source of the Contractor and Principal's wealth, including the economic activities that generated the wealth and the source of the particular funds;
- Reviewing generally available public information, such as media reports, to determine whether the contractor has been the subject of any criminal or civil enforcement action based on violations of anti-money laundering laws or regulations or any investigation, indictment, conviction or civil enforcement action relating to financing of terrorists;
- Conducting visits and a face-to-face meeting with the Contractors' management to discuss/confirm the proposed trainings;
- Identifying & verifying the Contractor's beneficial owner (s) to ensure that PSDF understands who the ultimate beneficial owner is;
- Assessing and ensuring that the nature and purpose are in line with its expectations and use the information as a basis for ongoing monitoring;
- In case of TSP, obtaining assurance from the Banks that the TSP has opened a separate bank account for execution of PSDF's training contract.

Annexure III- Internal suspicion reporting procedures

Internal suspicion reporting procedures are described below:

1. **Reporting to the Compliance Officer**

   All suspicious transactions attempt to conclude such transactions or suspicious behaviour by customers should be reported to the CO immediately. This may include:

   - Information provided by the Contractor which is considered not to be credible;
   - Transactions are unusual, very extensive or complicated, having regard to the customer's normal activities.

2. **Reporting to the Board**

   The CO shall be responsible for having all the circumstances of such Contractors carefully examined and the results of this examination reported to the Board depending on the severity of the circumstances. On the other hand, if there are not deemed to be grounds for such a report, the outcome of the report by the CO shall be preserved.

3. **Reporting to the Relevant Authorities**

   In case transactions with the parties including donors appear unusual or suspicious, regardless of the amount involved and whether or not made in cash, the Board consider issuing suspicious transaction report (STR). In addition, transactions which give rise to a reasonable ground of suspicion that they may involve financing of activities relating to terrorism, shall also be reported to the Financial Monitoring Unit (FMU) at http://www.fmu.gov.pk/contactus.html.

Annexure IV- Primary Responsibilities of the CO

The Primary responsibilities of CO includes but are not limited to, the following;

- Effective compliance with the relevant provisions of AML/CFT Regulations, the AML Act & Rules, and other directions and guidelines issued and 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;
- Reports directly and periodically to the 'Board of Directors';
- monitoring, reviewing and updating AML/CFT policies and procedures;
- providing assistance in compliance to other departments of PSDF;
- Responds promptly to requests for information by the SECP/LAW enforcement agency;
- has sufficient resources (including time and staff) and access to all information necessary to perform the AML/CFT compliance function;
- ensures regular audits of the AML/CFT activities;
- CO should provide necessary training and orientation, in collaboration with the HR Department, to the employees in respect of the Policy and the procedures and their responsibilities in respect of the Policy. CO should inform the potential risks and its implication on PSDF and on them as well. CO should also inform the employees about all the laws and regulations applicable on them and on PSDF. CO should maintain records evidencing such training;
- Receiving and reviewing any reports of suspicious activity from Employees and determining whether any suspicious activity as reported by an Employee warrants reporting to senior management of the Firm
- Coordination of enhanced due diligence procedures regarding Clients; and Responding to both internal and external inquiries regarding PSDF's anti- money laundering policies and procedures
- maintains various logs, as necessary, which should include logs with respect to declined business, politically exposed person ("PEPs"), and requests from SECP, FMU and Law Enforcement Agencies particularly in relation to investigations; and
- Such other responsibilities as may deem necessary in order to ensure compliance with AML/CFT regulations.

Annexure V- Factors indicating Low Risk Level of ML/FT

The factors indicating low risk of ML/CT includes, among other things:

1. contractor risk factors, including but not limited to, where the contractor:

    - is an individual resident in a geographical area of lower risk;
    - is a credit institution or a financial institution;
    - is a company whose securities are listed on a stock exchange.

2. product, service, transaction or delivery channel risk factors, including whether the product or service is:

    - a life insurance policy for which the premium is low or a pension scheme which does not provide for an early surrender option, and cannot be used as collateral;
    - a pension or similar scheme which satisfies the following conditions:
        - the scheme provides retirement benefits to employees;
        - contributions to the scheme are made by way of deductions from wages; and
        - the scheme rules do not permit the assignment of a member's interest under the scheme;
    - a product where the risks of money laundering and terrorist financing are managed by other factors such as purse limits or transparency of ownership;

3. geographical risk factors, including whether the country where the customer is resident, established or registered or in which it operates is:

    - an European Economy Area (EEA) state;
    - a third country which has effective systems to counter money laundering and terrorist financing;
    - a third country identified by credible sources as having a low level of corruption or other criminal activity, such as terrorism, money laundering, and the production;
    - a third country which, on the basis of credible sources, such as evaluations, detailed assessment reports or published follow-up reports published by the Financial Action Task Force, the International Monetary Fund, the World Bank, the Organisation for Economic Co-operation and Development or other international bodies or nongovernmental organisations;
    - has requirements to counter money laundering and terrorist financing that are consistent with the revised Recommendations published by the Financial Action Task Force in February 2012 and updated in October 2016; and
    - effectively implements those Recommendations.

Annexure VI- Factors indicating High Risk Level of ML/FT

Factors indicating high risk of ML/FT in a Contractor includes, but are not limited to, the following:

a. A Political Figure, any member of a Political Figure's immediate family, and any close associate of a Political Figure;

b. Any Contractor who gives the CO any reason to believe that its funds originate from, or are routed through, an account maintained at an "offshore bank" or a bank organized or chartered under the laws of a Non-Cooperative Jurisdiction;

c. Any Contractor who gives the CO any reason to believe that the source of its funds may not be legitimate or may aid terrorist activities;

d. Donation received from unidentifiable or suspicious source or though unusual payment mechanism or any other factor that would increase the risk in sponsors organizations;

e. Fake or suspicious identity documents of the beneficiaries or employees identified or beneficiaries or employees with identical characteristics and addresses or multiple identical or similar names and signatures;

f. The contract with partners is vague or lacks adequate financial or technical details or the structure or nature of the proposed project makes it difficult to identify the partner and verify their identity and details or the partners of the contract are PEPs or are otherwise exposed to higher risk;

g. Contractors belonging to countries which are noncompliant with anti- money laundering regulations according to FATF;

h. Legal persons or arrangements with complex ownership structures;

i. Other factors as indicated in the Guidelines.