A Group Company
of the Bank of Punjab

PUNJAB CAPITAL SECURITIES

(PRIVATE) LIMITED

ANTI MONEY LAUNDERING, COUNTERING FINANCING OF TERRORISM AND COUNTERING PROLIFERATION FINANCING

POLICY, PROCEDURES AND CONTROLS

1. INTRODUCTION

Definition of Money Laundering (ML)

Money laundering involves the placement of illegally obtained money into legitimate financial systems so that monetary proceeds derived from criminal activity are transformed into funds with an apparently legal source.

Countering Financing Terrorism (CFT)

Terrorist financing refers to the processing of funds to sponsors involved in or those who facilitate terrorist activity. Terrorist individuals/ groups/ organization derive income from a variety of sources, often combining both lawful and unlawful funding, and where the agents involved do not always know the illegitimate end of that income.

Proliferation Financing (PF)

Proliferation financing is the act of providing funds or financial services which are used, in whole or in part, for the manufacture, acquisition, possession, development, export, transshipment, brokering, transport, transfer, stockpiling or use of nuclear, chemical or biological weapons and their means of delivery and related materials (including both technologies and dual-use goods used for non-legitimate purposes), in contravention of national laws or, where applicable, international obligations.

With respect to entities, any involvement, whether it is to instigate, assist, conceal, or ignore the source, nature, location, ownership or control of money laundering and terrorism financing activities, can lead to both civil and criminal proceedings against both the individual and the entity involved.

For detailed types of Money laundering (ML) transactions refer as below however ML transactions may include but not limited to:

a. Advising a potential or existing client on how to structure a transaction to avoid reporting and/or record keeping requirements;
b. Engaging in any activity while willfully or recklessly disregarding the source of the funds or the nature of the Clients transaction;
c. Engaging in any activity designed to hide the nature, location, source, ownership or control of proceeds of criminal activity;
d. Dealing in funds to facilitate criminal activity; and
e. dealing in the proceeds of criminal activity

Terror Financing (TF) transactions refer following mention two types may include but not limited to:

i. Financial Support - In the form of donations, community solicitation and other fundraising initiatives. Financial support may come from states and large organizations, or from individuals.

ii. Revenue Generating Activities - Income is often derived from criminal activities such as kidnapping, extortion, smuggling or fraud. Income may also be derived from legitimate economic activities such as diamond trading or real estate investment.

Virtual Assets/ Virtual Currencies/ Virtual Assets Service Providers (VASPs)

Virtual currency is a type of unregulated digital currency. It is not issued or controlled by a central bank. Examples of virtual currencies include Bitcoin, Litecoin, and XRP. Digital currencies are stored in and transacted through designated software, applications, and networks in digital form.

Purpose and Scope

Anti-Money Laundering and Countering the Financing of Terrorism ("AML/CFT") regime requires financial institutions to understand their Money Laundering ("ML"), Terrorist Financing ("TF") and Proliferation Financing ("PF") risks, adopt and effectively implement an appropriate risk-based ML/TF/PF control framework. By aligning Pakistan's AML and CTF control framework with FATF recommendations, Pakistan's integration into the global financial system will be facilitated. This is an essential contribution that all RPs can make to the lawfulness, transparency, and long-term solid growth of Pakistan's financial sector supported by strong a capital market and the economy as a whole.

Securities and Exchange Commission of Pakistan ("SECP"), in order to maintain the integrity of its regulated financial sector that includes the brokers, insurers, NBFCs and Modarabas notified the Securities and Exchange Commission of Pakistan AML/CFT Regulations, 2018 ("the Regulations"). The SECP AML/CFT Regulations require SECP Regulated Persons (RPs) to establish policies, systems and internal controls to detect and combat ML and TF for preventing the abuse of their financial products and services.

These Guidelines supplement the Regulations and the AML/CFT regime by clarifying and explaining the general requirements of the regulatory framework to help RPs in applying national AML/CFT measures. The Guidelines are based on Pakistan' AML/CFT legislation and reflect, so far as applicable, the 40 Recommendations and guidance papers issued by the Financial Action Task Force ("FATF") and relevant international best practices.

Applicable Regulations

An effective Anti-Money Laundering and Countering the Financing of Terrorism("AML/CFT") regime requires financial institutions to adopt and effectively implement Appropriate ML and TF control processes and procedures, not only as a principle of good Governance but also as an essential tool to avoid involvement in ML and TF. AML and CFT Regime Is governed under Anti-Money Laundering Act, 2010 ("AML Act"), Anti-Money Laundering Rules, 2008 ("AML Rules") made under the Anti-Money Laundering Ordinance, 2007 ("AML Ordinance"), Securities and Exchange Commission of Pakistan (Anti Money Laundering and Countering Financing of Terrorism)

Regulations, 2018 ("SECP AML/CFT Regulations") made under the Securities and Exchange Commission of Pakistan Act, 1997 ("SECP Act"), upon recommendation of Financial Monitoring

Unit ("FMU") established under AML Act, Guidelines on SECP AML/CFT Regulations issued by SECP in September 2018 and Pakistan National Risk Assessment (PNRA) Report on Money Laundering and Terrorist Financing issued in September 2019.

PCS Compliance Statement

Money laundering (ML) and Countering Financing Terrorism (CFT) and Proliferation financing is conducting or attempting to conduct a financial transaction knowing that the transaction is designed in whole or in part to conceal or disguise the nature, location, source, ownership, or control of the proceeds of specified unlawful activity. PCS will take all necessary steps to comply with applicable AML and CTF laws and regulations. PCS will maintain an AML & CTF program in accordance with the applicable laws and regulations. The program is reasonably designed to prevent PCS's services from being used to facilitate money laundering and the financing of terrorist activities and or illegal activities.

PCS is committed to full compliance with all applicable laws and regulations regarding AML & CTF procedures. If PCS, its personnel and/or premises are inadvertently used for ML/CTF or other illegal activities, PCS can be subject to potentially serious civil and/or criminal penalties. Therefore, it is imperative that every officer, director, and employee (each, an "Employee") is familiar with and complies with the policies, procedures and controls set forth in this Compliance Manual.

This Compliance Statement is designed to assist all clients in adhering to PCS's policy, procedures and controls, which if followed thoroughly, are designed to protect themselves, PCS, its Employees, its facilities and its activities from money laundering and terrorism financing or other illegal activities.

Objectives of Procedures and Controls

Objectives of this document include the following:

a) Comply with all AML and CTF Rules, Regulations and guidelines issued by SECP of the jurisdictions it operates in;
b) Procedures & controls to verify customer identification and retain necessary identifying and transactional information;
c) A designated Compliance officer to coordinate compliance with the program and/ or policies;
d) Require all Employees to prevent, detect and report to the Compliance Officer all potential instances in which PCS or its employees, its facilities or its activities have been or are about to be used for money laundering, terrorist financing and other illegal activity;
e) Suspicious activity reporting procedures and document retention guidelines for any suspicious activity reports and supporting documentation;

f) Training and education of appropriate Employees concerning their responsibilities under the program, including suspicious activity reporting; and
g) Independent review to monitor and maintain an adequate program and/or controls.

2. OBLIGATION OF PCS IN ESTABLISHING AN EFFECTIVE ANTI MONEY LAUNDERING AND COUNTER FINANCING TERRORISM GOVERNANCE AND COMPLIANCE

a. PCS understands its obligation of establishing an effective AML/CFT procedures and controls to discourage criminals for using its platform for ML or TF purposes, therefore, PCS develops a comprehensive AML/CFT procedures and controls with strict compliance program to comply with the relevant and applicable laws and obligations.
b. PCS Board of Directors and senior management is fully engaged in the decision making on AML/CFT policies, procedures and control which are addressing on the risk based approach. They are fully aware of the level of ML/TF risks and take a view on it to encounter these risks effectively.
c. PCS must give due priority to establishing and maintaining an effective AML/CFT compliance culture and must adequately train its staff to identify suspicious activities and adhere with the internal reporting requirements for compliance with the Regulations.
d. PCS has established written internal procedures and control that alarm on any suspicious activity. All staff members are aware of the reporting chain and the procedures to be followed. These procedures and controls will be periodically updated to handle any suspicious activity and/ or for updating new regulatory requirements/changes.
e. PCS is appointed a Compliance Officer at the management level who is working independently and ensures the compliance frameworks developed by PCS and regulatory requirements.
f. PCS is ensuring that any suspicious transaction report must be made by employees to the Compliance officer and the Compliance officer develops a professional opinion regarding to transaction(s) which may lead to opportunities for money laundering and/or terrorism financing.
g. The Compliance officer is responsible for ensuring that employees are responsive to their reporting obligations and defined procedures and controlled be follows when making a suspicious transaction report.
h. The Company shall update/amend the Policies, Procedures and Controls in line with the changes/amendments in SECP AM/CFT Regulations with the approval of the Board or Equivalent and communicate in writing to all relevant employees; and
i. The Company shall provide amendments in the Policies, Procedures and Controls separately attached to amendment Policies, Procedure and Controls showing impact of such changes on AML/CFT Regime.
j. PCS shall access and analyze as a combination of the likelihood that the risk will occur and the impact of cost or damages if the risk occur. The impact of cost or damage may consist of:
    i. Financial loss to the PCS from the crime;
    ii. Monitory penalty from regulatory authorities; and
    iii. Reputational damages to the business or the entity itself.

3. PROGRAM AND SYSTEMS TO PREVENT ML AND TF

a. PCS will establish and maintain appropriate procedures and controls to prevent, detect and report ML/TF to which it is exposed. These are as:

- To identify and assess ML/TF risks relating to persons, countries and activities which should include checks against all applicable UN Security Council Sanctions List; https://www.un.org/sc/suborg/en/sanctions/un-sc-consolidated-list.
- PCS closely monitor client's network, exposure, receipt of funds, trading patterns, and withdrawal of funds to assess risk involved;
- PCS internal policies, procedures and controls are well equip to combat ML/TF, including appropriate risk management arrangements;
- PCS enhance customer due diligence and others measures;
- PCS define customer related record keeping controls;
- An audit function to test the AML/CFT system;
- PCS adopt a screening procedures to ensure high standards when hiring employees;
- PCS arrange employee-training program internally as well as externally when deems.

b. The Compliance Officer is responsible to ensure that appropriate systems are in place to prevent and report ML/TF and PCS is in compliance with the applicable legislative and regulatory obligations.

AML Compliance Officer Designation and Duties

The Company has designated Head of Compliance who shall report directly, and periodically to the Board of Directors ("Board") or to another equivalent executive position or committee of the Company.

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

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

4. THE THREE LINES OF DEFENSE

a. PCS establish the following three lines of defense to combat ML/TF;

Front Office: PCS trading and settlement staff are trained and knowledge to carry out the AML/CFT due diligence in accordance with related policies and procedures relating to client(s).

Compliance function: The Compliance officer monitors and implement with regulatory frameworks to prevent ML/TF at employee level to organization level.

Audit function: The Compliance officer performs internal control and audit function to compliant with defined procedure and controls

b. PCS's policies and procedures are available in writing that communicated to all employees. These procedures have the clear description for employees of their obligations and instructions as well as guidance for detecting, monitoring and reporting suspicious transactions with the regulatory frameworks.

c. The Compliance Officer have the authority and ability to observe the effectiveness of PCS's AML/CFT policy, procedures and controls, compliant with applicable AML/CFT regulatory frameworks and provide guidance in day-to-day operations of the AML/CFT policies, procedures and controls.

d. PCS will be appointed such a person as the Compliance Officer who is fit and proper to assume the role and who:

- He/she has sufficient skills and experience to develop and maintain systems and controls (including documented policies and procedures);
- He/ She reports directly and periodically to the Board of Directors or equivalent on AML/CFT systems and controls.
- He has sufficient resources, including time and support staff.
- He has access to all information necessary to perform the AML/CFT compliance function.
- He will ensure regular audits of the AML/CFT program.
- He has to maintains various logs, as necessary, which should include logs with respect to declined business, politically exposed person ("PEPs"), and requests from Commission, FMU and Law Enforcement Agencies ("LEAs") particularly in relation to investigations; and
- He must respond promptly to requests for information by the SECP/Law enforcement agency.

e. The Compliance officer must periodically conduct AML/CFT audits on an Institution-wide basis and be proactive in following up their findings and recommendations. As a general rule, the processes used in auditing should be consistent with internal audit's broader audit mandate, subject to any prescribed auditing requirements applicable to AML/CFT measures.

5. RISK ASSESSMENT AND APPLYING A RISK BASED APPROACH

Before undertaking an ML/TF/PF risk assessment, PCS must consider the following guidance material to determine the level of risk involved in relation to customers, products/services, delivery channels and countries/regions:

(a) Latest National Risk Assessment;
(b) Sector Risk Assessment guidance by the SECP;
(c) Any applicable guidance by relevant authorities (such as FMU, SBP, MoFA, NACTA etc.);
(d) Information and guidance published by international organizations such as the FATF, APG;
(e) RPs business experience in relation to certain risks.

i. PCS shall also follow the methodology for Internal Risk Assessment as required by PNRA Report. The concepts as defined by PNRA report, i.e. threat, vulnerabilities, inherent risk, consequences and likelihood of ML/TF and remedial measures / controls will be taken into consideration. The vulnerabilities will be assessed by considering the products and services offered, the customers, the geographical reach and delivery channels available.

The PCS adopted SECP AML/CFT Regulations which is shifting its emphasis from one-size-fits-all approach to Risk Based Approach ('RBA'), and PCS carryout ML/TF risk assessment and apply RBA to prevent or mitigate ML and TF.

ii. PCS, before determining what is 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 it or its customers do business. As is the case for PCS overall risk management, PCS senior is understand the nature and level of the risks that they are exposed to and ensure that systems and processes are in place to identify, assess, monitor, manage and mitigate ML/TF risks.

iii. The RBA enables PCS to ensure that AML/CFT measures are commensurate to the risks identified and allocated in the most efficient ways. PCS develops an appropriate RBA for its level to organization, structure and business activities:

1) Identify ML/TF risks relevant to organization, structure and business activities;
2) Assess ML/TF risks in relation to:

   a. PCS customers (including beneficial owners);

   b. Country or geographic area in which PCS customers reside or operate and where the PCS operates;

   c. Products, services and transactions that the PCS offers; and

   d. PCS delivery channels.

2) The Compliance officer design and implement policies, procedures and controls that are approved by PCS Board of Directors to manage and mitigate the ML/TF risks identified and assessed;

4) The Compliance officer monitors and evaluates the implementation of mitigating controls and improves systems where necessary;

5) The Compliance officer keep customers risk assessments current through ongoing reviews and, when necessary, updates;

6) The Compliance officer document the RBA including implementation and monitoring procedures and updates to the RBA; and

7) The Compliance officer adopts appropriate mechanisms to provide risk assessment information to the Commission.

iv. Under the RBA, where there are higher risks, the Compliance officer is required to take enhanced measures to manage and mitigate those risks; and correspondingly, where the risks are lower, simplified measures may be permitted. However, simplified measures are not permitted whenever there is a suspicion activity/ transaction of ML/TF. In the case of some very high-risk situation(s) which are outside the PCS risk tolerance, the PCS may decide not to open such account, or to exit from the relationship.

v. PCS in view of the fact that the nature of the TF differs from that of ML, the risk assessment also includes an analysis of the vulnerabilities of TF. Since the funds used for TF may emanate from legal sources, the nature of the sources may vary when the source of the TF originate from criminal activities, the risk assessment related to ML is also applicable to TF.

vi. PCS overlaps its CFT measures with AML measures. These may cover, for example, risk assessment, CDD checks, transaction monitoring, and escalation of suspicions and liaison relationships with the PSX, SECP and FMU.

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

a. Identifying the area of the business operations susceptible to ML/TF
b. Conducting an analysis in order to assess the likelihood and impact of ML/TF;
c. Managing the risks; and
d. Regular monitoring and review of those risks.

2) **ML/TF Risk Assessment**

There are three levels of risk assessment, which review ML/TF risks from different perspectives. Together, the three assessments inform RPs of potential risks to help combat ML/TF. The three risk assessments inform each other and combined provide a picture of the ML/TF risks Pakistan faces. The three levels of risk assessments are:

3) **National Risk Assessment (NRA)**
The NRA reviews ML/TF issues affecting the whole of Pakistan. It is based on information from suspicious transaction reports (STRs) and proceeds of crime asset recovery data. Information from government organizations, both domestic and international, also contribute to the NRA, and it provides a comprehensive overview of threats and crime trends. SECP encourages RPs to use the NRA to stay informed about emerging threats and trends.

4) Sector Risk Assessment (SRA)
SECP produce a risk assessment for the sectors it regulates aiming to improve RPs' understanding of the ML/TF sector risks, and to inform them of the risk indicators, trends and emerging issues. The SRA is reviewed from time to time to check how ML/TF risks affect the regulated sectors.

5) Risk assessments by RPs
PCS must carry out a risk assessment of ML/TF in their business. taking into account guidance material from SECP and the Financial Monitoring Unit. The entity risk assessment is part of SECP anti-money laundering and countering financing of terrorism guidance materials.

PCS shall regularly create and maintain an updated document that describes its current assessment of its ML/TF/PF risk in light of the latest National Risk Assessment. This document will be formally approved by the management and board of directors of the RP and must provide a list of proposed actions needed to address any deficiencies in risk mitigates, controls processes and procedures identified by the assessment. In addition, the document must include a view on the AML/CFT risks with respect to its customers, products, delivery channels, geography and the quality of the RPs risk mitigates, such as controls processes and procedures involving more detailed steps.

The ML/TF/PF risk assessment is not a one-time exercise and is required to be carried out annually and as required under SECP SRO 920(1)2020 on TFS Obligation and reporting. https://www.secp.gov.pk/laws/directives/.
For guidance to prepare Internal AML/CFT Risk Assessment, please refer to Section 13 - Risk Assessment and Applying a Risk Based Approach.

a) Identification, Assessment and Understanding Risks

PCS's AML and CTF policies and procedures are intended to ensure that, prior to establishing any relation with the client all reasonable and practical measures are taken to confirm the Clients' identities. Further, PCS will verify that any third party, upon whom the PCS relies for Client identification, adheres to the same standards.

The Compliance Officer may determine to apply enhanced measures for reasons other than those discussed below. Employees are encouraged to provide the Compliance Officer with any revisions in the KYC they consider appropriate.

Copies of all documents reviewed or checklists completed in connection with the Client Identification Procedures shall be kept in accordance with PCS's Client Records Retention

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

i. PCS understand, identify and assess the inherent ML/TF risks posed by its customer base, products and services offered, delivery channels and the jurisdictions within which it or its customers do business, and any other relevant risk category. The risk assessment policies and procedures adopted by PCS to appropriate size, nature and complexity.

ii. ML/TF risks may be measured using a number of risk categories and for each category applying various factors to assess the extent of the risk for determining the overall risk classification (e.g. high, medium high, medium or low). PCS make determination as to the risk weights to be given to the individual risk factors or combination of risk factors. When weighing risk factors, PCS will take into consideration the relevance of different risk factors in the context of a particular customer relationship.

iii. PCS may enhance ML/TF risks that can be encountered by the PCS need to be assessed analyzed as a combination of the likelihood that the risks will occur and the impact of cost or damages if the risks occur. This impact can consist of financial loss to the PCS from the crime, monitory penalties from regulatory authorities or the process of enhanced mitigation measures. It may include reputational damages to the business or the PCS itself. The analysis of certain risk categories and their combination is specific for PCS so that the conclusion on the total risk level must be based on the relevant information available.

iv. For the analysis, PCS will identify the likelihood that these types or categories of risk will be misused for ML and/or for TF purposes. This likelihood is for instance high, if it can occur several times per year, medium if it can occur once per year and low if it is unlikely, but not possible. In assessing the impact, PCS can, for instance, look at the financial damage by the crime itself or from regulatory sanctions or reputational damages that can be caused. The impact can vary from minor if PCS is only short-term or there are low-cost consequences, to very major, when PCS found to be very costly inducing long-term consequences that affect the proper functioning of the PCS.

v. The following is an example of a risk probability likelihood matrix with 5 risk ratings as an example. PCS can customize their own as applicable to their operation with more details, if preferable.

vi. PCS documents risk assessment that able to demonstrate allocation of compliance resources. An effective risk assessment is an ongoing process. Risk levels may change as new markets are entered, as high-risk customers open or close accounts, or as the services, policies, and procedures change. The PCS will be therefore updates its risk assessment every 12 to 18 months to take account of these changes. The Compliance officer adhere risk assessment information to the Commission, if required.

vii. For a high risk environment, the PCS should assess risk likelihood in terms of threat and vulnerability. For example, PCS may consider customers from porous border areas as the threat, and accounts dealing with cash payments as the vulnerability. Depending on the risk assessment method PCS use, the inherent risk rating for this scenario would be high. PCS may then want to assess the impact of this event on the business and the wider AML/CFT environment.

Probability and Likelihood Risk Rating Matrix

					Consequences				
				Customers	Few or isolated instances of reportable suspicious activity.	Minimal instances of reportable suspicious activity.	Single or a few instances of suspicious activity.	Single or multiple instances of suspicious activity.	Excessive, uncontrollable and manageable instances of suspicious activity.
				Countries	Few or isolated instances of technical exceptions related the organizations operational infrastructure.	Minor compromise of information sensitive to the operations of internal or departmental units.	Compromise of information sensitive to the organization's use of its operations.	Systemic compromise of information sensitive to the organization's use of its operations.	Porous and uncontrollable comprise of the organization's operations management.
				Products	Minimal losses.	Some losses.	Significant losses.	Extensive damage or losses.	Serious damages and losses.
				Services	Freedom to operated is primarily unaffected. Self assessment and improvements should suffice.	Scrutiny by the Executive, internal communication or internal audit to prevent short term or low cost consequences.	Persistent concerns, scrutiny required. Medium term consequences with some costs.	Persistent intense long term, high cost consequences affecting operations.	Significant losses to the organization's 'Brand' significantly affects its growth and abilities.
				Delivery Channels	Minimal impact on non-core operations. Technical exceptions can be addressed by routine day-to-day operations.	Some impact on the organization's capability in terms of delays and management's performance of controls.	Impact on the organization resulting in reduced performance.	Breakdown of key activities leading to reduction in service and performance.	Protracted unavailability of individuals with critical skills. Critical failure(s) preventing core activities from being performed. Survival of the entity is at risk.
					1	2	3	4	5
	Chance	Probability	Frequency		Insignificant	Minor	Moderate	Major	Significant
Likelihood	Is expected to occur in most circumstances	>95%	Occurs many times a year	E Almost Certain	M	H	H	VH	VH
	Will probably occur in most circumstances	>65%	Probably occurs several times a year	D Likely	L	M	H	H	VH
	Might occur at some time	>35%	Probably occurs once a year	C Possible	L	L	M	H	H
	Could occur at some time	<35%	Unlikely to occur but not impossible	B Unlikely	VL	L	L	M	H
	May occur in exceptional circumstances	<5%	Rare and unusual probability to occur	A Rare	VL	VL	L	L	M

Very High	Immediate action required by the Executive with detailed planning, allocation of resources and regular monitoring.
High	Senior management's attention required
Medium	Management's responsibility must be specified
Low	Minor and managed by routine supervisory procedures
Very Low	Managed by routine procedure

RISK MATRIX

PCS may use above risk matrix as a method of assessing risk in order to identify the types or categories of customers that are in the low-risk category, those that carry somewhat higher, but still acceptable risk, and those that carry a high or unacceptable risk of money laundering and terrorism financing. In classifying the risk, PCS, taking into account its specificities, may also define additional levels of ML/TF risk.

EXAMPLES OF RISK CLASSIFICATION FACTORS

Below are some examples that can be helpful indicators of risk factors/indicators that may be considered while assessing the ML/TF risks for different risk categories relating to types of customers, countries or geographic areas, and particular brokerage services, transactions or delivery channels.

High-Risk Classification Factors

(1) **Customer risk factors:** PCS describe all types or categories of customers that provide business to and should make an estimate of the likelihood that these types or categories of customers that will related to high risk jurisdiction in light of National Risk Assessment 2019, will misuse the PCS for ML or TF, and the consequent impact if indeed that occurs. Risk factors that may be relevant when considering the risk associated with a customer or a customer's beneficial owner's business include:

(a) The business relationship is conducted in unusual circumstances - significant unexplained geographic distance between the PCS and the customer;

(b) Non-resident customers.

(c) Legal persons or arrangements, non-governmental organizations. (NGOs) / not-for-profit organizations (NPOs) and trusts / charities;

(d) Companies that have nominee shareholders.

(e) Business that is cash-intensive, money market dealers and precious metal dealer.

(f) The ownership structure of the customer appears unusual or excessively complex given the nature of the customer's business such as having many layers of shares registered in the name of other legal persons – Trustee, Partners, Administers/ Executors;

(g) Politically exposed persons – are individuals who are or have been entrusted with prominent public functions for example senior politicians, senior government, judicial or military officials, senior executives of state owned corporations, important political party officials. Business relationships with family members or close associates of PEPs involve reputational risks similar to those with PEPs themselves.

- The customer(s) belonging to countries where CDD / KYC and anti-money laundering regulations are lax or if funds originate or go to those countries that are exist in FATF gray list countries in the light of NRA 2019.
- The customer(s) with links to offshore tax havens;
- The high net worth customers with no clearly identifiable source of income;
- Any customer(s) with any reason to believe that has been refused brokerage services by another brokerage house;
- The customer(s) are establishing business relationship or transactions with counterparts from or in countries not sufficiently applying FATF recommendations;

h) Shell companies, especially in cases where there is foreign ownership which is spread across jurisdictions;

i) Business that is related to real state agents, Builders and banks recognized as very high risk factor as per NRA- 2023.

- trusts and other legal arrangements which enable a separation of legal ownership and beneficial ownership of assets.
- Requested/applied quantum of business does not match with the profile/particulars of client
- updating more regularly the identification data of applicant/customer and beneficial owner
- Internal Risk Assessment of PCS includes Risk assessment of Virtual Assets/ Virtual Currencies/ Virtual Assets Service Providers (VASPs).

PCS strictly refused to open any account of person who involved at any stage in money laundering and terrorist financing or funding.

Non-Cooperative Jurisdiction means any foreign country that has been designated as non-cooperative with international AML and ATF principles or procedures by an intergovernmental group or organization, such as the Financial Action Task Force on Money Laundering ("FATF")

(2) **Country or geographic risk factors:** Countries or geographical risk may arise because of the location of a customer, the origin of a destination of transactions of the customer, but also because of the business activities of the PCS itself, its location and the location of its geographical units. Country or geographical risk, combined with other risk categories, provides useful information on potential exposure to ML/TF. Following factors that may indicate a high risk:

(a) Countries identified by credible sources, such as mutual evaluation or detailed assessment reports or published follow-up reports by international bodies such as the FATF, and NRA 2019 as not having adequate AML/CFT systems.

(b) Countries subject to sanctions, embargos or similar measures issued by, for example, the United Nations.

(c) Countries identified by credible sources as having significant levels of corruption or other criminal activity.

(d) Foreign countries or local geographic areas identified by NRA 2019 as providing funding or support for terrorist activities, or that have designated terrorist organizations operating within their country.

(e) People of which geographical area were found mostly involved in suspected Virtual Assets and Virtual Currency and Virtual Asset Service Provider transactions

or which geographical areas are considered most vulnerable by PCS in relation to VAs/ VCs and VASPs as per internal risk rating.

(3) Product, service, transaction or delivery channel risk factors:

PCS adopt a comprehensive ML/TF risk assessment must take into account the potential risks arising from the services, and transactions that the PCS offers to its customers and the way these services are delivered. In identifying the risks of products, services, and transactions, the following factors should be considered:

(a) Anonymous transactions (which may include cash) refer to SECP circular 10 of 2016.

(b) Non-face-to-face business relationships or transactions.

(c) Online payments received from unknown or un-associated third parties.

(d) International transactions, or involve high volumes of currency (or currency equivalent) transactions

(e) Products that involve large receipt in cash; refer to PSX Rule Book and

(f) Controls developed specific to highly vulnerable products in connection to Virtual Assets and Virtual Currency and Virtual Asset Service Provider were found adequate.

MEDIUM RISK CLASSIFICATION FACTORS

As per NRA -2023 life insurance and NBFC's recognized as medium risk factor.

LOW RISK CLASSIFICATION FACTORS

(1) **Customer risk factors:** A customer that satisfies the requirements under regulation 11 (2) (a) and (b) of the SECP AML/CFT Regulations and identified in NRA 2019.

(2) **Product, service, transaction or delivery channel risk factors:** satisfy the requirement under regulation 11(2) (c) to (g) of the SECP AML/CFT Regulations and AML/CFT policies identified in NRA 2019.

(3) Profession that is related to Lawyers, Law firms, Chartered Accountants firm, non-life insurance sector recognized as low risk as per NRA 2023

(3) **Country risk factors:**

a) Countries identified by credible sources, such as mutual evaluation or detailed assessment reports, as having effective AML/CFT systems.

(b) Countries identified by credible sources as having a low level of corruption or other criminal activity.

In making a risk assessment, PCS may, when appropriate, also take into account possible variations in ML/TF risk between different regions or areas within a country.

AML AND CTF COMPLIANCE OFFICER

Employee(s) shall immediately notify the Compliance Officer if he/she suspects or has any reason to suspect that any potentially suspicious activity has occurred or will occur if a transaction is completed. Compliance Officer will judge, and thereby assess which suspicious matter should be reported to the Regulatory Authority i.e. PSX, SECP, FMU (Financial Monitoring Unit).

Note: The obligation to report does not depend on the amount involved or the seriousness of the offence. There are no the Minims concessions.

The Compliance Officer shall ensure:

a. Compliance with applicable Rules and Regulations and this Policy, Procedures and controls on continuous basis;
b. Receive and review any report(s) of suspicious activity from Employees and/ or observed review of system and controls;
c. Determine whether any suspicious activity as reported by an Employee warrants reporting to the senior management and or the Regulatory Authority i.e. PSX, SECP and FMU (Financial Monitoring Unit);
d. Conduct Employee training programs for appropriate employees and maintain records evidencing such training;
e. Responding to both internal and external queries regarding this document.

B) RISK MANAGEMENT

Risk Tolerance

i. Risk tolerance is the amount of risk that the PCS is willing and able to accept. PCS risk tolerance impacts its decisions about risk mitigation measures and controls. For example, if PCS determines that the risks associated with a particular type of customer exceed its risk tolerance, it may decide not to accept or maintain that particular type of customer(s). Conversely, if the risks associated with a particular type of customer are within the bounds of PCS risk tolerance, PCS must ensure that the risk mitigation measures applies are commensurate with the risks associated with that type of customer(s).

ii. PCS will establish its risk tolerance. Such parameters will be done by senior management and the Board. In establishing the risk tolerance, PCS will consider whether it has sufficient capacity and expertise to effectively manage the risks that it decides to accept and the consequences such as legal, regulatory, financial and reputational, of an AML/CFT compliance failure.

iii. PCS decides not to tolerance a high-risk and refuse to establish business relations and/or terminate existing relations.

Risk Mitigation

i. PCS adopted appropriate policies, procedures and controls that enable to manage and mitigate effectively the inherent risks that they have identified, including the national risks. The Compliance Officer monitors the implementation of those controls and enhance(s) them, if necessary. The policies, controls and procedures will be approved by senior management, and the measures taken to manage and mitigate the risks(whether high, medium High, medium or low) should be consistent with legal and regulatory requirements.

ii. The nature and extent of AML/CFT controls will depend on a number of aspects as prescribe in NRA 2019 may be following:

1) The nature, scale and complexity of PCS business activities

2) Diversity, including geographical diversity of PCS operations proximity to porous border areas and areas with terrorist activity/threat

3) PCS, customer, product and activity profile

4) Volume and size of transactions

5) Extent of reliance or dealing through third parties or intermediaries.

iii. Some of the risk mitigation measures that PCS may consider include:

1) The Compliance Officer determining the scope of the identification and verification requirements or ongoing monitoring based on the risks posed by particular customers;

2) Setting transaction limits for higher-risk customers or products;

3) Requiring CEO/director approval for higher-risk transactions, including those involving PEPs;

4) Determining the circumstances under which they may refuse to take on or terminate/cease high risk customers/products or services;

5) Determining the circumstances requiring senior management approval (e.g. high risk or large transactions, when establishing relationship with high risk customers such as PEPs).

Evaluating Residual Risk and Comparing with the Risk Tolerance

Subsequent to establishing the risk mitigation measures, PCS will evaluate residual risk, the risk remaining after taking into consideration the risk mitigation measures and controls. Residual risks should be in line with the RP's overall risk tolerance.

Where PCS finds that the level of residual risk exceeds its risk tolerance or that its risk mitigation measures do not adequately mitigate high-risks, PCS will enhance the risk mitigation measures that are in place.

6. MONITORING AML/CFT SYSTEMS AND CONTROLS

i. PCS controls are in place to monitor the risks identified and assessed as they may change or evolve over time due to certain changes in risk factors, which may include changes in customer conduct, development of new technologies, new embargoes and new sanctions. PCS will update controls as appropriate to suit the change in risks.

ii. Additionally, PCS will assess the effectiveness of risk mitigation procedures and controls, and identify areas for improvement, where needed. For this purpose, PCS will need to consider monitoring certain aspects which include:

1) The ability to identify changes in a customer profile or transaction activity/behavior which come to light in the normal course of business;

2) The potential for abuse of services by reviewing ways in which different services may be used for ML/TF purposes, and how these ways may change, supported by typologies/law enforcement feedback etc.;

3) The adequacy of employee training and awareness;

4) The adequacy of internal coordination mechanisms i.e. between AML/CFT compliance and other functions/areas;

5) The compliance arrangements;

6) The performance of third parties who were relied on for CDD purposes;

7) Changes in relevant laws or regulatory requirements; and

8) Changes in the risk profile of countries to which the RPs or its customers are exposed to.

DOCUMENTATION AND REPORTING

i. PCS will be documented its RBA. Documentation of relevant policies, procedures and controls review results and responses will enable PCS to demonstrate to the Commission:

1) Risk assessment relating to ML/TF procedures and controls, in the light of National Risk Assessment 2019;

2) Implementation of procedures and controls, including due diligence requirements, in light of its national risk assessment;

3) Monitoring and, as necessary, improves the effectiveness of procedures and controls; and

4) Reporting to BOD on the results of ML/TF risk assessed and implementation status of ML/TF risk management systems and control processes.

ii. PCS believe that the ML/TF risk assessment is not a one-time exercise and therefore, we must ensure that ML/TF risk management processes are kept under regular review which is at least annually. Further, Senior Management/ CEO should review the program's adequacy

when the reporting entity adds new services, opens or closes accounts with high-risk customers.

iii. PCS will be able to demonstrate to the Commission:

- Adequacy of its assessment, management and mitigation of ML/TF risks;
- Customer acceptance policy;
- Procedures and policies concerning customer identification and verification;
- Ongoing monitoring and procedures for reporting suspicious transactions; and all types of measure taken in the context of AML/CFT, during the SECP's on-site inspection. PCS will maintain ***Control Assessment Template*** within the period as required by the Commission from time to time.

1.1 Transaction Monitoring of High Risk Customer

For a high risk environment, the PCS should assess risk likelihood in terms of threat and vulnerability. PCS may consider customers from porous border areas and high risk jurisdiction (local and foreign) as per NRA -2019 as the threat, and accounts dealing with cash payments as the vulnerability and any scenario in relation to VAs/ VCs and VASPs.. Depending on the risk assessment method PCS use, the inherent risk rating for this scenario would be high. PCS may then want to assess the impact of this event on the business and the wider AML/CFT environment.

1. NEW PRODUCTS AND TECHNOLOGIES

i. PCS will place systems to identify and assess ML/TF risks that may arise in relation to the development of new products and new business practices, including new delivery mechanisms, and the use of new or developing technologies for both new and pre-existing products such as:

- Electronic verification of documentation;
- Data and transaction screening systems.

ii. PCS will undertake a risk assessment prior to the launch or use of such products, practices and technologies; and take appropriate measures to manage and mitigate the risks.

iii. PCS will be adopted policies and procedures to prevent the misuse of technological development in ML/TF schemes, particularly those technologies that favor anonymity.

For example, securities trading and investment business on the Internet, add a new dimension to PCS activities. The unregulated nature of the Internet is attractive to criminals, opening up alternative possibilities for ML/TF, and fraud. It is not appropriate that PCS offer on-line live account opening allowing full immediate operation of the account in a way which would dispense with or bypass normal identification procedures. However, initial application forms could be completed on-line and then followed up with appropriate identification checks. The account, in common with accounts opened through more traditional methods, should not be put into full operation until the relevant account opening provisions have been satisfied.

iv. PCS will maintain adequate systems to ensure that systems and procedures are kept up to date with such developments and the potential new risks and impact theymay have on the services offered by PCS. Risks identified must be fed into PCS's business risk assessment.

In coordination with compliance function should have systems in place to identify and assess ML/TF/PF risks that may arise from new and pre-existing product such as:

(a) New products, markets or sales channels;
(b) New internal organization or new offices and departments;
(c) New data and transaction screening systems and verification of documentation:
(d) the use of virtual or digital currencies and assets;

2. CROSS-BORDER CORRESPONDENT RELATIONSHIP

i For time being PCS have not any cross-border correspondent relationships provision to services by one institution to another institution (the respondent institution). Correspondent institutions that process or execute transactions for their customer's (i.e. respondent institution's), if PCS enter in to any such arrangement customers may present high ML/TF risk and as such may require EDD.

ii. If in case PCS will transact cross-border, then PCS will manage its risks effectively, entering into a written agreement with the respondent institution before entering into the correspondent relationship.

iv. In addition to setting out the responsibilities of each institution, the agreement could include details on how the PCS will monitor the relationship to ascertain how effectively the respondent institution is applying CDD measures to its customers, and implementing AML/CFT controls in the light of NRA 2019.

iv. Correspondent Institutions are encouraged to maintain an ongoing and open dialogue with the respondent institutions to discuss the emerging risks, strengthening AML/CFT controls, and help the respondent institutions in understanding the correspondent institutions' AML/CFT policies and expectations of the correspondent relationship.

3. CUSTOMER DUE DILIGENCE

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

ii. PCS will 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 PCS's knowledge of the customer, its ***Business and Risk Profile***, including, where necessary, the source of funds. PCS will

conduct CDD when establishing a business relationship if:

- There is a suspicion ***WARNING SIGNS*** gives some examples of potentially suspicious activities or ***RED FLAGS*** for ML/TF. Although these may not be exhaustive in nature, it may help PCS to 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

- There are doubts as to the veracity or adequacy of the previously obtained customer identification information.

iii. In case of suspicion of ML/TF, PCS will:

- 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
- File a Suspicious Transaction Reporting ("STR") with the FMU, in accordance with the requirements under the Law.

iv. PCS will 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.

v. PCS will verify the identification of a customer using reliable independent source documents, data or information including verification of CNICs from NADRA Verisys/Biometric and from UIN database and POR in case of Afghan refugees, FBR NTN & active taxpayer list. Similarly, PCS will identify and verify the customer's beneficial owner(s) to ensure that understands who the ultimate beneficial owner is.

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

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

viii. PCS will 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 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.

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

x. The purpose of the requirements set out regarding the identification and verification of the applicant and the beneficial owner is twofold: first, to prevent the unlawful use of legal persons and arrangements, by gaining a sufficient understanding of the applicant to be able to properly assess the potential ML/TF risks associated with the business relationship; and second, to take appropriate steps to mitigate the risks. In this context, PCS will identify the customer and verify its identity.

xi. If, PCS has any reason to believe that an applicant has been refused to open account/ closed his/her account by another broker due to concerns over illicit activities of the customer, not accepting the customer in accordance with its own risk assessments and procedures.

For customers whose accounts are dormant or in-operative, withdrawals will not be allowed until the account is activated on the request of the customer. For activation, the regulated person shall conduct NADRA Verisys or biometric verification of the customer and obtain attested copy of customer's valid identity document (if already not available) and fulfil the regulatory requirements

Dormant or in-operative account means the account in which no transaction or activity or financial service has been extended by the regulated person from last three (3) years;

Securities transactions In the securities industry, intermediaries may be required to perform transactions very rapidly according to the market conditions at the time the customer is contacting them and the performance of the transaction may be required before verification of identity is completed.

a) Timing of Verification

PCS will undertake verification prior to entry into the business relationship or conducting a transaction. However, as provided in the Regulations broker may complete verification after the establishment of the business relationship.

b) Existing Customers

The Compliance Officer has to require to apply CDD measures to existing customers on the basis of materiality and risk, and to conduct due diligence on such existing relationships at appropriate times, taking into account whether and when CDD measures have previously been undertaken and the adequacy of data obtained.

c) **Identification of Customers that are not physically present**

CO shall apply equally effective Customers identification procedures and ongoing monitoring standards for Customers not physically present for identification purposes as for those where the client is available for interview.

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.

Consequently, there are increased risks and practices must carry out at least one of the following measures to mitigate the risks posed:

further verifying the Customer's identity on the basis of documents, data or information referred in Annexure-1 to AML/CFT Regulations, but not previously used for the purposes of verifying the client's identity;

taking supplementary measures to verify the information relating to the client that has been obtained by the practice.

ii. The Compliance officer ensure that CDD requirements entails a suspicion of ML/TF or becomes aware at any time that it lacks sufficient information about an existing customer, its hould take steps to ensure that all relevant information is obtained as quickly as possible.

iii. PCS is entitled to rely on the identification and verification steps that it has already undertaken, unless it has doubts about the veracity of that information. Examples of situations that might lead to PCS such doubts could be where there is a suspicion of money laundering in relation to that customer, or where there is a material change in the way that the customer's account is operated, which is not consistent with the customer's business profile.

iv. When PCS is unable to complete and comply with CDD requirements as specified in the Regulations, PCS will not open the account, commence a business relationship, or perform the transaction. If the business relationship has already been established, PCS terminate the relationship. Additionally, PCS will consider making a STR to the FMU.

c) Tipping-off & Reporting

i. The Law is prohibiting tipping-off. However, a risk exists that customers could be unintentionally tipped off when the RP is seeking to complete its CDD obligations or obtain additional information in case of suspicion of ML/TF. The applicant/customer's awareness of a possible STR or investigation could compromise future efforts to investigate the suspected ML/TF operation.

ii. Therefore, PCS form a suspicion of ML/TF while conducting CDD or ongoing CDD, they should take into account the risk of tipping-off when performing the CDD process. If, the Compliance officer reasonably believes that performing the CDD or on-going process will tip-off the applicant/customer, it may choose not to pursue that process, and should file a STR. RPs should ensure that their employees are aware of, and sensitive to, these issues when conducting CDD or ongoing CDD.

d) No Simplified Due Diligence for Higher-Risk Scenarios

PCS will not adopt simplified due diligence measures where the ML/TF risks are high.
The Compliance Officer has to identify risks and have regard to the risk analysis in determining the level of due diligence.

4. ON-GOING MONITORING OF BUSINESS RELATIONSHIPS

i. Once the identification procedures have been completed and the business relationship is established, PCS 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. PCS will conduct ongoing monitoring of their business relationship with their customers. Ongoing monitoring helps to keep the due diligence information up-to-date, and review and adjust the risk profiles of the customers, where necessary.

ii. PCS will conduct on-going /enhance due diligence which includes scrutinizing the transactions undertaken throughout the course of the business relationship with a high risk customer as per SECP Regulation 19 (Ongoing Monitoring) requires a regulated person to conduct ongoing due diligence on the business relationship by undertaking reviews of existing records and ensuring that documents data or information collected for CDD purposes is up to date.

iii. PCS will 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.

iv. The Compliance officer will consider updating customer CDD records as a part its periodic reviews on the occurrence of a triggering event; triggering events include:

- Material changes to the customer risk profile or changes to the way that the account usually operates;

- When, the compliance officer notice to bring to notice that lacks sufficient or significant information on that particular customer;

- scrutinizing transactions undertaken throughout the course of the relationship to ensure that the transactions being conducted are consistent with the regulated person's knowledge of the customer, their business and risk profile, including where necessary, the source of funds

    - Where a significant transaction takes place;
    - Where there is a significant change in customer documentation standards;
    - Significant changes in the business relationship as:

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

vi. The Compliance officer is to 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

vii. However, if the Compliance Officer 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

viii. 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.

ix. PCS 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 reasons of cost, the nature of business, or difficulties of systems integration. In such circumstances, the Compliance Officer has to ensure that alternative controls in place for conducting on-going monitoring. In case a customer has no active business with the PCS, 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.

5. FREQUENCY FOR UPDATING CUSTOMER DUE DILIGENCE

PCS will carry out the due diligence of existing customers using the risk rating assigned to each customer at the time of customer on boarding as under:

1- CDD information of customers categorized as “High Risk” shall be reviewed/updated each year.

2- CDD information of customers categorized as “Medium Risk” shall be reviewed/updated at least once in every three years while CDD information of customer categorized as “Low Risk” shall be reviewed/updated at least once in every five years.

Moreover, CDD information of customers shall be updated immediately whenever material information regarding the customers becomes known or there is a suspicion of money laundering or terrorist financing or there are doubts about the veracity or adequacy of previously obtained data.

6. SIMPLIFIED DUE DILIGENCE MEASURES (“SDD”)

i. The Compliance Officer conducts SDD in case of lower risks identified. However, the Compliance Officer will ensure that the low risks customer’s identifies are commensurate with the low risks identified by the country or the Commission. While

determining whether to apply SDD, the Compliance Officer will pay particular attention to the level of risk assigned to the relevant sector, type of customer or activity. The simplified measures should be commensurate with the low risk factors.

ii. SDD is not acceptable in higher-risk scenarios where there is an increased risk, or suspicion that the applicant is engaged in ML/TF, or the applicant is acting on behalf of a person that is engaged in ML/TF.

iii. Where the risks are low and where there is no suspicion of ML/TF, the law allows PCS to rely on third parties for verifying the identity of the applicants and beneficial owners. PCS verifying the identity through UIN database, FBR NTN and Active Taxpayer list

iv. Where the Compliance Officer decides to take SDD measures on an applicant/customer, it should document the full rationale behind such decision and make available that documentation to the Commission on request.

Standard CDD is likely to apply to most of the customers. It involves the collection of identity information of the customer, any beneficial owner of the customer, or any person acting on behalf of the customer. It also includes the verification of that information. For beneficial owners the verification is according to the level of risk involved.

Reliance on Third Parties (Regulation 24)

i Identifying the customer and verifying that customer's identity using reliable, independent source documents, data or information;

ii Identifying the beneficial owner, and taking reasonable measures to verify the identity of the beneficial owner, such that the financial institution is satisfied that it knows who the beneficial owner is. For legal persons and arrangements this should include financial institutions understanding the ownership and control structure of the customer;

iii Understanding and, as appropriate, obtaining information on the purpose and intended nature of the business relationship: (a) remain liable for any failure to apply such indicated CDD measures;

Provided that the regulated person shall -

(a) remain liable for any failure to apply the indicated CDD measures (i) to (iii) above;

(b) immediately obtain from the Third Party the required information concerning the indicated CDD measures (i) to (iii) above;

(c) take steps to satisfy itself that copies of identification data and other relevant documentation relating to CDD requirements will be made available from the third party upon request without delay; and

(d) satisfy itself that the Third Party is supervised by an AML/CFT regulatory authority or an equivalent foreign authority and has measures in place for compliance with AML Act obligation of CDD and record keeping.";

iv. Where a regulated person relies on a third party that is part of the same corporate group, the regulated person may deem the requirements of subsection 24(1) to be met if: (3) In addition to subsection 24(1), when determining in which country a third party may be based, the regulated person shall have regard to available information on the level of country risk

v. RP shall ultimately remain responsible for its AML/CFT obligations, including generating STRs and shall carry out ongoing monitoring of such customer itself.

7. ENHANCED CDD MEASURES ("EDD")

i. The Compliance Officer will 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.

ii. Where the risks of ML/TF are higher, or in cases of unusual or suspicious activity, the Compliance Officer conduct enhanced CDD measures, consistent with the risks identified. In particular, RPs 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.

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

- Obtaining additional information on the applicant/customer (e.g. occupation, volume of assets, information available through public databases, internet, etc.). Updating more regularly the identification data of applicant/customer and beneficial owner.

- Obtaining additional information on the intended nature of the business relationship.

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

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

- Obtaining the approval of Senior Management /CEO to commence or continue the business relationship.

- 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.

vi. In case of accounts where the accountholder has instructed PCS not to issue any correspondence to other joint accountholder's address. Such accounts do carry additional risk to PCS and the Compliance Officer will exercise due caution as a result. It is

recommended on a best practice basis that evidence of identity of the accountholder's address should be obtained by the Welcome. "Hold Mail" accounts should be regularly monitored and reviewed and the Compliance Officer will take necessary steps to obtain the identity of the account holder where such evidence is not already in the PCS file.

vii. If Customer Due Diligence Measures are Not Completed.

Where a Securities Broker is unable to complete and comply with COD requirements as specified in the Regulations

For New Customers:

It shall not open the account,

commence a business relationship; or

perform the transaction..

For Existing Customers:

The Securities Broker shall terminate the relationship.

Additionally, the Securities Broker shall consider making a STR to the FMU.

a) High-Risk Countries

i. Certain countries are associated with crimes such as drug trafficking, fraud, corruption and gray list countries in the light of NRA 2019 and high risk non-cooperative jurisdictions identified as high risk by FATF and consequently pose a higher potential risk to PCS. The Compliance Officer has to refuse for conducting a business relationship.

ii. The Compliance Officer is advised to consult publicly available information to ensure that customers are belonging to high-risk countries/territories. While assessing risk of a country, the Compliance Officer is 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.

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

8. POLITICALLY EXPOSED PERSONS (PEPS)

Domestic PEPs

Individuals who are, or have been entrusted domestically with prominent public functions, for example heads of state or of government, senior politicians, senior government officer or employees with position of influence, judicial or military officers .

Foreign PEPs

Individuals who are, or have been entrusted with prominent public functions by a foreign country, for example heads of state or government, senior politicians, senior government, judicial or military officials, senior executives of state owned corporations, important political party officials.

International organization PEPs

Persons who are, or have been entrusted with a prominent function by an international organization, refers to members of senior management or individuals who have been entrusted with equivalent functions i.e. directors, deputy directors, and members of the board or equivalent functions.

i. Business relationships with individuals holding important public positions and with persons or companies clearly related to them may expose as PEP's to PCS for significant reputational and/or legal risk. The risk occurs when such persons abuse their public powers for either their own personal benefit and/or the benefit of others through illegal activities such as the receipt of bribes or fraud. Such persons, commonly referred to as 'politically exposed persons(PEPs) and defined in the Regulations, inter-alia, heads of state, ministers, influential public officials, judges and military commanders and includes their family members and close associates.

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

iii. Close associates to PEPs are individuals who are closely connected to PEP, either socially or professionally.

iv. Provision of financial services to corrupt PEPs exposes, PCS to reputational risk and costly information requests and seizure orders from law enforcement or judicial authorities. In addition, public confidence in the ethical standards of the whole financial system can be undermined.

v. PCS are encouraged to be vigilant in relation to PEPs from all jurisdictions, who are seeking to establish business relationships. PCS in relation to PEPs, in addition to performing normal due diligence measures:

- PCS deploy appropriate risk management systems to determine whether the customer is a politically exposed person;

- Senior Management/ CEO approval is required for establishing business relationships with such customers;

- The Compliance Officer has to take reasonable measures to establish the source of wealth and source of funds; and conduct enhanced monitoring of the business relationship.

vi. The Compliance Officer has to obtain Senior Management/ CEO approval to continue a business relationship once a customer or beneficial owner is found to be, or subsequently becomes, a PEP.

vii. The Compliance Officer has to take a risk based approach to determine the nature and extent of EDD where the ML/TF risks are high. In assessing the ML/TF risks of a PEP, the Compliance Officer has to consider factors such as whether the customer who is a PEP:

- Is from a high risk country;
- 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).

viii. The other red flags that the Compliance Officer has to consider include (in addition to the above and the red flags that they consider for other applicants):

- The information that is provided by the PEP is inconsistent with other (publicly available) information, such as asset declarations and published official salaries;
- Funds are repeatedly moved to and from countries to which the PEP does not seem to have ties;
- A PEP uses multiple bank accounts for no apparent commercial or other reason;
- The PEP is from a country that prohibits or restricts certain citizens from holding accounts or owning certain property in a foreign country.

ix. The Compliance Officer will be followed a risk based approach in determining whether to continue to consider a customer as a PEP who is no longer a PEP. The Compliance Officer may to consider factors included as:

- 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).

Red Flags /Warning Signs

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

Red flags that signal possible money laundering or terrorist financing, Proliferation Financing and Red flag indicating of LPLAs may include, but are not limited to:

AML/CFT and PF Red Flags /Warning Signs

1. Customers who are unknown to the broker and verification of identity / incorporation proves difficult;
2. Customers who wish to deal on a large scale but are completely unknown to the broker;
3. Customers who wish to invest or settle using cash;
4. Customers who use a cheque that has been drawn on an account other than their own;
5. Customers who change the settlement details at the last moment;
6. Customers who insist on entering into financial commitments that appear to be considerably beyond their means;
7. Customers who accept relatively uneconomic terms, when with a little effort they could have a much better deal;
8. Customers who have no obvious reason for using the services of the broker (e.g.: customers with distant addresses who could find the same service nearer their home base; customers whose requirements are not in the normal pattern of the service provider's business which could be more easily serviced elsewhere);
9. Customers who refuse to explain why they wish to make an investment that has no obvious purpose;
10. Customers who are introduced by an overseas agent based in a country noted for drug trafficking or distribution.
11. Customer trades frequently, selling at a loss
12. Customers who constantly pay-in or deposit cash to cover requests for bankers drafts, money transfers or other negotiable and readily marketable money instruments;
13. Customers who wish to maintain a number of trustee or customers' accounts which do not appear consistent with the type of business, including transactions which involve nominee names;
14. Any transaction involving an undisclosed party;
15. transfer of the benefit of an asset to an apparently unrelated third party, or assignment of such benefit as collateral;
16. Significant variation in the pattern of investment without reasonable or acceptable explanation
17. Transactions appear to be undertaken in a structured, sequential manner in order to avoid transaction monitoring/ reporting thresholds.
18. Transactions involve penny/microcap stocks.
19. Customer requests a securities provider to execute and/or clear a buy order and sell order for the same security or similar or correlated securities (and/or on behalf of the same beneficial owner), in close chronology.

20. Transfers are made to the same person from different individuals or to different persons from the same individual with no reasonable explanation.
21. Unusually large aggregate wire transfers or high volume or frequency of transactions are made with no logical or apparent reason.
22. Customer invests in securities suddenly in large volumes, deviating from previous transactional activity.
23. Customer conducts mirror trades.
24. Customer closes securities transaction before maturity, absent volatile market conditions or other logical or apparent reason.

Proliferation Financing Warning Signs/Red Alerts

1. RPs should take note of the following circumstances where customers and transactions are more vulnerable to be involved in proliferation financing activities relating to both DPRK and Iran sanctions regimes:
2. customers and transactions associated with countries subject to sanctions;
3. instruments that could particularly be used to finance prohibited transactions, such as certain trade financing products and services;
4. customers involved with and/or transactions related to items, materials, equipment, goods and technology prohibited by UNSCRs;
5. reasonableness of invoiced goods against market value, inconsistency or discrepancies in trade-related documentation.

Red flag indicating misuse of LPLAs

1. Using LP or LAs as a front entity with little underlying operations for laundering illicit finance.
2. Use of complex ownership and control structures to obscure beneficial ownership
3. Mismatched business profile with unusual transaction behavior or activity
4. Large cash deposits and withdrawals with dubious underlying operations
5. Using non-profit operations as a front end to seek donations for terrorist activities
6. Structuring of transactions with mismatch between transactions and nature of business
7. Entity unable to provide a satisfactory explanation regarding the pass-through nature of the transactions and reasons for fund transfers between companies with seemingly unrelated business profile.
8. High turn-over of funds within a relatively short period of time without any plausible explanations.
9. Unclear relationships between ‘connected or associated’ companies and/or persons
10. Frequent/multiple transaction involving entities with the same beneficial owner which did not make economic sense
11. Deliberate avoidance of formal banking service without legitimate reasons

12. Use of influential names (indicating linkage with NPOs, highly trending terminologies or government linked entities) where the actual operations cannot be directly validated.
13. Co-mingling of business and personal funds
14. Unable to establish relationship between the beneficial owner and authorized signatory of the company.
15. Lack of or frequent failure to comply with disclosure requirements for public interest entity
16. There is adverse information relating to the entity and/or its management.
17. The investments are not in line with the net worth of the client.
18. The underlying investments of the PIF and their value, where known, are unusual in nature or not substantiated.
19. Inconsistencies in the information relating to purpose of the entity and source of funding
20. LP or LAs using financial services based on the name of entity whose license or registration has already been revoked or cancelled by the concerned authorities
21. LP or LA having no physical operational presence or employees

In particular, RPs should be alert to the following non-exhaustive list of factors that are relevant to the DPRK sanctions regime:

1. significant withdrawals or deposits of bulk cash that could potentially be used to evade targeted financial sanctions and activity-based financial prohibitions;
2. opening of banking accounts by DPRK diplomatic personnel, who have been limited to one account each under relevant UNSCRs (including number of bank accounts being held, holding of joint accounts with their family members);
3. clearing of funds, granting of export credits or guarantees to persons or entities that are associated with trading transactions relating to the DPRK;
4. providing insurance or re-insurance services to maritime vessels owned, controlled or operated, including through illicit means, by the DPRK or classification services to vessels which there are reasonable grounds to believe were involved in activities, or the transport of items, prohibited by UNSCRs concerning the DPRK, unless the Security Council 1718 Committee determines otherwise on a case-by-case basis;
5. direct or indirect supply, sale or transfer to the DPRK of any new or used vessels or providing insurance or re-insurance services to vessels owned, controlled, or operated, including through illicit means, by the DPRK, except as approved in advance by the Security Council 1718 Committee on a case-by-case basis; or
6. the leasing, chartering or provision of crew services to the DPRK without exception, unless the Security Council 1718 Committee approves on a case-by-case basis in advance;38 or
7. using real property that DPRK owns or leases in Pakistan for any purpose other than diplomatic or consular

High Net worth Individuals (HNWI)

1. High net worth individuals while an attractive customer for PCS, can expose PCS to higher risk of financial transactions that may be illicit. As per PCS policy standard size of HNWI is 10 million. PCS knows to whom it is offering its products and services, and can establish criterion for HNWI applicable to their particular business.
2. PCS will 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 of the PCS.

Beneficial Ownership (BO)

The Beneficial Owner is the natural person at the end of the chain who ultimately owns or controls the customer. The definition of BO in the Regulations is as below:

"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".

For the beneficial ownership in the context of natural person, where a natural person seeks to open an account in his/her own name, the PCS should inquire whether such person is acting on his own behalf. However, in relation to student, senior citizens and housewife accounts (where doubt exists that the apparent account holder is acting on his own behalf) the PCS may obtain a self-declaration for source and beneficial ownership of funds from the customer and perform further due diligence measures accordingly.

For legal persons or arrangements, it is essential to understand the ownership and control structure of the customer. This may be done based on plausibility and records. In any case of lack of transparency or doubt, or higher risk, verification is needed. For legal persons, the primary source for verification of ultimate beneficial ownership is the Register of Ultimate Beneficial Ownership.

For complex structures, foreign entities or foreign owned entities, PCS are 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.

Non-Profit Organizations (NPOs)

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

2. The objective of Enhanced Customer Due Diligence for NPOs is to ensure that NPOs are not misused by terrorist organizations: (i) to pose as legitimate entities; (ii) to exploit legitimate entities as conduits for terrorist financing, including for the purpose of escaping asset freezing measures; or (iii) to conceal obscure the clandestine diversion of

funds intended for legitimate purposes, but diverted for terrorist purposes.

3. RP who transact with NPOs should understand:
   a. Beneficiaries and Beneficial Owners including certain donors that maintain decision rights;
   b. Flow of funds, in particular the use of funds by an NPO.

15. RECORD-KEEPING PROCEDURES

i. The Compliance Officer has to ensure that all information obtained in the context of CDD is recorded. This includes both;

The AMLA Section 2 defines record as follows:

(xxxii) "record" includes the records maintained in the form of books or stored in a computer or any electronic device, or such other form as may be prescribed.

The AMLA Section 7C states the general record keeping requirements:
Every reporting entity shall maintain a record of all transactions for a period of at least five years following the completion of the transaction, and records of account files, business correspondence, documents, of all records obtained through CDD and the results of any analysis undertaken for a period of at least five years following the termination of the business relationship.
Further, Section 7(4) requires the record to be maintained for a period of 10 years for submitted STRs and CTRs after reporting of the transaction:

"Every reporting entity shall keep and maintain all record related to Suspicious Transaction Reports and CTRs filed by it for a period of at least ten years after reporting of transaction under sub-sections (1), (2) and (3)."

- The Compliance Officer has to record the documents as provided by the customers and verifying the identity of the customer or the beneficial owner, and

- Transcription into of the relevant CDD information contained in such documents or obtained by other means in customer file.

ii. PCS will maintain, for at least 05 years after termination, all necessary records on transactions to be able to comply swiftly with information requests from the competent authorities. Such records should be sufficient to permit the reconstruction of individual transactions, so as to provide, if necessary, evidence for prosecution of criminal activity.

iii. Where there has been a report of a suspicious activity or PCS will aware of a continuing investigation or litigation into ML/TF relating to a customer or a transaction, records relating to the transaction or the customer should be retained until confirmation is received that the matter has been concluded.

iv. PCS will also keep records of identification data obtained through the customer due diligence process, account files and business correspondence that would be useful to an investigation for a period of 05 years after the business relationship has ended. This includes records pertaining to enquiries about complex, unusual large transactions, and unusual patterns of transactions. Identification data and transaction records should be made available to relevant competent authorities upon request.

vi. Beneficial ownership information must be maintained for at least 5 years after the date on which the customer (a legal entity) is dissolved or otherwise ceases to exist, or five years after the date on which the customer ceases to be a customer of PCS.

vi. Records relating to verification of identity will generally comprise:

- A description of the nature of all the evidence received relating to the identity of the verification subject; and

- The evidence itself or a copy of it or, if that is not readily available, information reasonably sufficient to obtain such a copy.

vii. Records relating to transactions will generally comprise:

- Details of personal identity, including the names and addresses, of:
  - The customer;
  - The beneficial owner of the account or product; and
  - Any counter-party

- Details of securities and investments transacted including:
  - The nature of such securities/investments;
  - Valuation(s) and price(s);
  - Memoranda of purchase and sale;
  - Source(s) and volume of funds and securities;
  - Destination(s) of funds and securities;
  - Memoranda of instruction(s) and authority(ies);
  - Book entries;
  - Custody of title documentation;
  - The nature of the transaction;
  - The date of the transaction;
  - The form (e.g. cash, cheque) in which funds are offered and paid out.

16. REPORTING OF SUSPICIOUS TRANSACTIONS / CURRENCY TRANSACTION

REPORT

i. 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 must be considered unusual, and the Compliance Officer has to put "on enquiry". The Compliance Officer has to pay special attention to all complex, unusual large transactions, and all unusual patterns of transactions, which have no apparent economic or visible lawful purpose.

ii. Where the enquiries conducted by the Compliance Officer has to do not provide a satisfactory explanation of the transaction, it may be concluded that there are grounds for suspicion requiring PCS disclose and escalate matters to the AML/CFT.

iii. Enquiries regarding complex, unusual large transactions, and unusual patterns of transactions, their background, and their result should be properly documented, and made available to the relevant authorities upon request. 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:

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

iv. Where cash transactions are being proposed by the customer(s), and such requests are not in accordance with the customer's known reasonable practice, the Compliance Officer will need to approach such situations with caution and make further relevant enquiries. Depending on the type of business and the nature of customer portfolio (low/medium/medium high and high risks), PCS will informed PSX immediately of cash transactions as per PSX regulations.

v. PCS informed PSX if, any client wants to make his/her payment through cash exceeding Rs.25,000/- to PSX through NCHS system keep the reporting record by the Compliance Officer.

vi. If, the Compliance Officer decides that a disclosure should be made, the law requires the PCS 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.

vii. The process for identifying, investigating and reporting suspicious transactions to the FMU should be clearly specified in the reporting entity's policies and procedures and

communicated to all personnel through regular training.

viii. PCS is required to report total number of STRs filed to the Commission on bi-annual basis within seven days of close of each half year. The Compliance Officer will ensure prompt reporting in this regard.

ix. The Compliance Officer has to require the maintain of a register of all reports made to the FMU. Such registers should contain details of:

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

x. The Compliance Officer will ensure, when an applicant or a customer is hesitant/fails to provide adequate documentation (including the identity of any beneficial owners or controllers), consideration should be given to filing a STR. Also, where an attempted transaction gives rise to knowledge or suspicion of ML/TF, that attempted transaction should be reported to the FMU.

xi. Once suspicion has been raised in relation to an account or relationship, in addition to reporting the suspicious activity, the Compliance Officer will ensure that appropriate action is taken to adequately mitigate the risk of PCS being used for criminal activities. This may include a review of either the risk classification of the customer or account or of the entire relationship itself. Appropriate action may necessitate escalation to the BOD to determine how to handle the relationship, taking into account any other relevant factors, such as cooperation with law enforcement agencies or the FMU.

In order to ensure quality reporting, the reason(s) for suspicion should be supported with proper analysis and should contain following elements:

(a) Information on the person/entity conducting the suspicious transaction/activity;
(b) Details of the transaction, such as the pattern of transactions, type of products or services and the amount involved;
(c) Description of the suspicious transaction or its circumstances
(d) Tax profile of person/entity (if available)
(e) If the reported subject (e.g. client/customer) has been the subject of a previous STR then the reference number with date should be provided.
(f) Information regarding the counterparties, etc.
(g) Any other relevant information that may assist the FMU in identifying potential offences and individuals or entities involved.

There are two types of suspicious reports which can be submitted by the RP to FMU.

(a) **STR- A** is to be reported on parties (Person, Account or Entity) involved in any suspicious activity, which does not involve transaction (s) or transmission of funds, However, STR-F should be filed in case where the transactions have been conducted.

(b) **STR- F** is to be reported on parties (Person, Account or Entity) for reporting of transactions and/or financial activity in which funds are involved and appears to be suspicious. An activity/event in which funds transmitted from one party to another must be reported as STR-F.

The link of the goAML registration guide is provided as follows: http://www.fmu.gov.pk/docs/RegistrationGuideFMU.pdf. The link of the goAML reporting guide is provided as follows: http://www.fmu.gov.pk/docs/Financial-Monitoring-Unit-FMU-goAML-Web-Users-Guide-Updated-2020.pdf.

As per Gazette notification SRO 73 (I)/2015 dated 21-01-2015, the minimum amount for reporting a CTR to FMU is two million rupees. Accordingly, all cash-based transactions of two million rupees or above involving payment, receipt, or transfer are to be reported to FMU as CTR. Aggregation of cash transactions during the day for the purpose of reporting a CTR is not required. However, if there is a suspicion that the customer is structuring the transaction into several broken cash transactions to evade reporting of CTR, the same may be reported in the form of an STR.

Similar to STR reporting to the FMU, all CTR reporting is via the FMU's online goAML system – refer: https://goamlweb.fmu.gov.pk/PRD/Home.

17. SANCTIONS COMPLIANCE

i. Sanctions are prohibitions and restrictions put in place with the aim of maintaining or restoring international peace and security. They generally target specific individuals or entities; or particular sectors, industries or interests. They may be aimed at certain people and targets in a particular country or territory, or some organization or element within them. There are also sanctions that target those persons and organizations involved in terrorism. The types of sanctions that may be imposed include:

- Targeted sanctions focused on named persons or entities, generally freezing assets and prohibiting making any assets available to them, directly or indirectly;
- Economic sanctions that prohibit doing business with, or making funds or economic resources available to, designated persons, businesses or other entities, directly or indirectly;
- Currency or exchange control;
- Arms embargoes, which would normally encompass all types of military and paramilitary equipment;
- Prohibiting investment, financial or technical assistance in general or for particular industry sectors or territories, including those related to military or paramilitary equipment or activity;
- Import and export embargoes involving specific types of goods (e.g. oil products), or their movement using aircraft or vessels, including facilitating such trade by means of financial or technical assistance, brokering, providing insurance etc.; and
- Visa and travel bans.

ii. The Regulations require, PCS not to establish business relationship with the individuals/entities and their associates that are either, sanctioned under United Nations Security Council (UNSC) Resolutions adopted by Pakistan or proscribed under the Anti-Terrorism Act, 1997.

iii. The UNSC Sanctions Committee, maintains the consolidated list of individuals and entities subject to the sanctions covering assets freeze, travel ban and arms embargo set out in the UNSC Resolution 1267 (1999) and other subsequent resolutions, concerning ISIL (Daésh)/ Al-Qaida and Taliban and their associated individuals.

iv. Government of Pakistan publishes Statutory Regulatory Orders (SROs) under the United Nations (Security Council) Act, 1948 in the official Gazettes to give effect to the decisions of the UNSC Sanctions Committee and implement UNSC sanction measures in Pakistan. The regularly updated consolidated list is available at the UN sanctions committee's website, at following link;

www.un.org/sc/committees/1267/aq_sanctions_list.shtml

https://www.un.org/securitycouncil/content/un-sc-consolidated-list

http://mofa.gov.pk/unsc-sanctions/

https://nfs.punjab.gov.pk/

http://www.secdiv.gov.pk/page/sro-unscr-sanctions

https://www.un.org/sc/suborg/en/sanctions/1988/materials

https://www.un.org/sc/suborg/en/sanctions/1718/materials
http://www.un.org/en/sc/2231/list.shtml

https://www.un.org/sc/suborg/en/sanctions/1718/prohibited-items

v. The Ministry of Interior issues Notifications of proscribed individuals/entities pursuant to the Anti-Terrorism Act, 1997, to implement sanction measures under UNSCR 1373(2001), and the regularly updated consolidated list is available at the National Counter Terrorism Authority's website, at following link;

http://nacta.gov.pk/proscribed-organizations/

The Company shall maintain the database of all its customers, their beneficial owners/associates, board of directors, trustees, and office bearers of its customers, for the required matching, screening, etc.

Following the above, required actions will be taken immediately on the receipt of notifications issued by the Ministry of Foreign Affairs on United Nations Security Council Resolutions, intimation from the National Counter Terrorism Authority or Securities and Exchange Commission of Pakistan regarding updates in the list of proscribed persons

vi. PCS make its sanctions compliance program an integral part of its overall AML/CFT compliance program and accordingly should have policies, procedures, systems and controls in relation to sanctions compliance. PCS provides adequate sanctions related training to its staff.

vii. When conducting risk assessments, the Compliance Officer has to take into account any sanctions that may apply (to customers or countries).

viii. The Compliance Officer has to screen customers, beneficial owners, transactions, and other relevant parties to determine whether they are conducting or may conduct business involving any sanctioned person or person associated with a sanctioned person/country. In the event of updates to the relevant sanctions lists, The Compliance Officer has to may

discover that certain sanctions are applicable to one or more of their customers, existing or new.

ix. Where there is a true match or suspicion, The Compliance Officer takes steps that are required to comply with the sanctions obligations including freeze without delay and without prior notice, the funds or other assets of designated persons and entities and reporting to the Commission, if they discover a relationship that contravenes the UNSCR sanction or a proscription.

x. The obligations/ prohibitions regarding proscribed entities and persons mentioned in the above lists are applicable, on an ongoing basis, to proscribed/ designated entities and persons or to those who are known for their association with such entities and persons, whether under the proscribed/ designated name or with a different name. The Compliance Officer has to document and record all the actions that have been taken to comply with the sanctions regime, and the rationale for each such action.

xi. PCS is expected to keep track of all the applicable sanctions, and where the sanction lists are updated, shall ensure that existing customers, suppliers, vendors, advisor and retainer ship are not listed in 4th schedule and UNSC data base.

xii. In case there is not 100% match but sufficient grounds of suspicion that customer/funds belong to sanctioned entity/ individual, the Compliance Officer may consider raising an STR to FMU.

18. AML/CFT PROGRAM IN A GROUP-WIDE AND CROSS-BORDER CONTEXT

i. The Regulations require a financial group to have group-wide AML/CFT policies and

procedures that are consistently applied and supervised across the group.
The group-wide policies should be appropriate to all branches and majority owned subsidiaries of the RP, even though reflecting host jurisdiction. PCS have no such operations and business activities.

ii. Where the minimum regulatory or legal requirements of the home and host countries differ, offices in host jurisdictions should apply the higher standard of the two. In cases where the host jurisdiction requirements are stricter than the group's, it allows the relevant branch or subsidiary to adopt and implement the host jurisdiction local requirements. PCS have no such operations and business activities.

iv. Where the AML/CFT requirements of host jurisdiction are less strict than those of Pakistan, it shall ensure to have AML/CFT measures consistent with the requirements of Pakistan. Where the host jurisdiction does not permit the proper implementation of AML/CFT measures consistent with those of Pakistan, it shall inform the same to the Commission along with the appropriate additional measures that they wish to apply to manage ML/TF risks. Where the proposed additional measures are not sufficient to mitigate the risks, the Commission may make recommendations to the it on further action. PCS have no such operations and business activities.

v. Policies and procedures should be designed not merely to comply strictly with all relevant laws and regulations, but more broadly to identify, monitor and mitigate group-wide risks. Every effort should be made to ensure that the group's ability to obtain and review information in accordance with its global AML/CFT policies and procedures is not impaired as a result of modifications to local policies or procedures necessitated by local legal requirements. In this regard, it should have robust information-sharing among the head office and all of its branches and subsidiaries. It's compliance and internal audit staff, in particular the compliance officer should evaluate compliance with all aspects of their group's policies and procedures, including the effectiveness of centralized CDD policies and the requirements for sharing information and responding to queries from head office. PCS have no such operations and business activities.

19. FOREIGN BRANCHES AND SUBSIDIARIES

The regulated person shall ensure that their foreign branches and majority-owned subsidiaries in countries which do not sufficiently apply the FATF Recommendations, apply AML & CFT measures consistent with Pakistan's AML/CFT requirements, to the extent that host country laws and regulations permit. If the foreign country does not permit the proper implementation of AML/CFT measures consistent with that of Pakistan requirements, financial groups should apply appropriate additional measures to manage the risks, and inform the Commission when a foreign branch or subsidiary is unable to observe appropriate AML/CFT measures.";

20. INTERNAL CONTROLS (AUDIT FUNCTION, OUTSOURCING, EMPLOYEE SCREENING AND TRAINING)

i. PCS are expected to have systems and controls that are comprehensive and proportionate to the nature, scale and complexity of its activities and the ML/TF risks they identified. PCS is established and maintain internal controls in relation to:

- an audit function to test the AML/CFT systems, policies and procedures;
- outsourcing arrangements;
- employee screening procedures to ensure high standards when hiring employees; and
- an appropriate employee training program.

The type and extent of measures to be taken should be appropriate to the ML/TF risks, and to the size of PCS.

a) Audit Function

i. PCS will, 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 market behavior, size of transaction, complexity, and risks identified during the risk assessments. The AML/CFT audits should be conducted to assess the AML/CFT systems which include:

Test the overall integrity and effectiveness of the AML/CFT systems and controls;
Assess the adequacy of internal policies and procedures in addressing identified risks, including;

(a) overall governance structure of the RP for AML/CFT, including the role, duties and responsibilities of the Compliance Officer/function;
(b) 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;
(c) integrity and effectiveness of the AML/CFT systems and controls and the adequacy of internal policies and procedures in addressing identified risks, including:
(d) CDD measures, monitoring and updating of customer data;
(e) Screening process for Terror Financing Sanction (TFS), and test its functionality;
(f) testing transactions with emphasis on high–risk customers, geographies, products and services;
(g) Record keeping and documentation.
(h) the effectiveness of parameters for automatic alerts and the adequacy of RP's process of identifying suspicious activity, internal investigations and reporting;
(i) the adequacy and effectiveness of training programs and employees' knowledge of the laws, regulations, and policies & procedures.
(j) Implemented on recommendation in relation to VAs/ VCs and VASPs.

- Assess compliance with the relevant laws and regulations;

- Test transactions in all areas with emphasis on high-risk areas;
- Assess employees' knowledge of the laws, regulations, guidance, and policies &procedures and their effectiveness in implementing policies and procedures;
- Assess the adequacy, accuracy and completeness of training programs;
- Assess the effectiveness of compliance quality control; and
- Assess the adequacy controls process of identifying suspicious activity including screening sanctions lists.

b) Outsourcing

i. PCS maintains policies and procedures in relation to outsourcing where they intend to outsource some of their functions. The Compliance Officer will conduct the due diligence on the proposed service provider to whom it intends to outsource as appropriate and also ensure that the service provider ("OSP") is fit and proper to perform the activity that is being outsourced.

ii. PCS decides to enter into an outsourcing arrangement(s), the Compliance Officer will ensure that the outsourcing agreement clearly sets out the obligations of both parties. PCS entering into an outsourcing arrangement will develop a contingency plan and a strategy to exit the arrangement in the event that the OSP fails to perform the outsourced activity as agreed.

iii. The OSP should report regularly to PCS within the timeframes as agreed upon with PCS. The Compliance Officer has access to all the information or documents relevant to the outsourced activity maintained by the OSP. PCS must not enter into outsourcing arrangements where access to data without delay is likely to be impeded by confidentiality, secrecy, privacy, or data protection restrictions.

iv. PCS ensure that the outsourcing agreement requires OSPs to file a STR with the FMU in case of suspicions arising in the course of performing the outsourced activity.

d) Employee Screening and Due Diligence

i. PCS maintains adequate policies and procedures to screen prospective and existing employees to ensure high ethical and professional standards when hiring. 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.

ii. Employee screening should be conducted at the time of recruitment, periodically thereafter, i.e., at least annually and where a suspicion has arisen as to the conduct of the employee.

iii. PCS ensures that their employees are competent and proper for the discharge of the responsibilities allocated to them. While determining whether an employee is fit and proper, PCS may:

- Verify the references provided by the prospective employee at the time of recruitment
- Verify the employee's employment history, professional membership and qualifications
- Verify details of any regulatory actions or actions taken by a professional body
- Verify details of any criminal convictions; and
- Verify whether the employee has any connections with the sanctioned countries or parties.

d) Employee Training

i. PCS ensure that all appropriate staff, receive training on ML/TF prevention on a regular basis, ensure all staff fully understand the procedures and their importance, and ensure that they fully understand that they will be committing criminal offences if they contravene the provisions of the legislation.

ii. Training to staff should be provided at least annually, or more frequently where there are changes to the applicable legal or regulatory requirements or where there are significant changes to PCS business operations or customer base.

iii. PCS provides its staff training in the recognition and treatment of suspicious activities. Training should also be provided on the results of risk assessments. Training should be structured to ensure compliance with all of the requirements of the applicable legislation.

iv. PCS staff has awareness on the AML/CFT legislation and regulatory requirements, systems and policies. They should know their obligations and liability under the legislation should they fail to report information in accordance with internal procedures and legislation. PCS will be encouraged its staff to provide a prompt and adequate report of any suspicious activities.

v. All new employees should be trained on ML/TF know the legal requirement to report, and of their legal obligations in this regard.

vi. PCS will consider obtaining an undertaking from their staff members (both new and existing) confirming that they have attended the training on AML/CFT matters, read

the RP's AML/CFT manuals, policies and procedures, and understand the AML/CFT obligations under the relevant legislation.

vii. Staff members who deal with the public such as trading and settlement staff are the first point of contact with potential money launderers, and their efforts are vital to PCS's effectiveness in combating ML/TF. Staff responsible for opening new accounts or dealing with new customers should be aware of the need to verify the customer's identity, for new and existing customers. Training should be given on the factors which may give rise to suspicions about a customer's activities, and actions to be taken when a transaction is considered to be suspicious.

viii. Trading and settlement staff are involved in the processing of transactions have to receive relevant training in the verification procedures, and in the recognition of abnormal settlement, payment or delivery instructions. Staff should be aware of the types of suspicious activities which may need reporting to the relevant authorities regardless of whether the transaction was completed. Staff should also be aware of the correct procedure(s) to follow in such circumstances.

ix. Trading and settlement staff are vigilant in circumstances where a known, existing customer opens a new and different type of account, or makes a new investment e.g. a customer with a personal account opening a business account. Whilst PCS may have previously obtained satisfactory identification evidence for the customer, the Compliance Officer will take steps to learn as much as possible about the customer's new activities.

x. PCS Directors and CEO may not be involved in the handling ML/TF transactions, it is important that they understand the statutory duties placed upon them, their staff and the firm itself given that these individuals are involved in approving AML/CFT policies and procedures. Supervisors, managers and senior management (including Board of Directors) should receive a higher level of training covering all aspects of AML/CFT procedures, including the offences and penalties arising from the relevant primary legislation for non-reporting or for assisting money launderers, and the requirements for verification of identity and retention of records.

xi. The Compliance Officer will receive in-depth training on all aspects of the primary legislation, the Regulations, regulatory guidance and relevant internal policies. He will also receive appropriate initial and ongoing training on the investigation, determination and reporting of suspicious activities, on the feedback arrangements and on new trends of criminal activity.

Level of Understanding of front/operational level staff on Virtual Assets and Virtual Currency and Virtual Asset Service Providers.

Trainings arranged by FI in high risk areas identified by PCS in internal risk rating in relation to VAs/ VCs and VASPs.