

**TO BE PUBLISHED IN GAZZETTE OF PAKISTAN EXTRA-ORDINARY**

Government of Pakistan  
Finance Division  
Budget Wing  
\*\*\*

Islamabad, the 23<sup>rd</sup> January, 2020.

**NOTIFICATION**

S.R.O. (I)/2020.- In exercise of the powers conferred by section 28 of the Public Debt Act, 1944 (XVIII of 1944), the Federal Government is pleased to make the following National Savings Schemes (AML and CFT) Rules, 2019, the same having been previously published *vide* Finance Division's Notification No.F.16(1)GS-I/2019, dated the 19<sup>th</sup> December, 2019, as required under sub-section (1) of the said section 28, namely:-

**NATIONAL SAVINGS SCHEMES (AML AND CFT) RULES, 2019**

**CHAPTER – I**

1. **Short title, extent and commencement.**- (1) These rules shall be called the National Savings Schemes (AML and CFT) Rules, 2019.
  - (2) These rules shall come into force at once.
  - (3) These rules shall apply to all offices and persons responsible for the issuance, management, marketing, registration, replacement, sale and discharge of the instruments issued by and the accounts opened at and maintained with the National Savings Centers, Pakistan Post and any other office designated as offices of issue.
2. **Definitions.** - (1) in these rules, unless there is anything repugnant in the subject or context,-

- (a) “**account**” means any type of account of the depositor, opened and maintained with any office of issue;
- (b) “**AML Act**” means the Anti-money Laundering Act, 2010 (VII of 2010);
- (c) “**beneficial owner**” means the natural person who ultimately owns or controls a customer or the person on whose behalf a transaction is being conducted and includes legal heirs and the person who exercises ultimate effective control over a person;
- (d) “**Board**” means the National Savings AML/CFT Supervisory Board to oversee implementation of these rules;
- (e) “**controlling office**” means head office of the National Savings, State Bank of Pakistan Banking Services Corporation (SBP(BSC), Pakistan Post Office Department (PPOD) or head office of any office of issue ;
- (f) “**CTR**” shall have the same meaning as assigned thereto in the AML Act;
- (g) “**customer**” means a person having business relationship with the office of issue by holding an account or instrument;
- (h) “**customer due diligence**” or “**CDD**” means.-
- (i) identifying the customer and verifying the customer’s identity on the basis of documents, data or information obtained from customer or from reliable and independent sources;
- (ii) identifying, where there is a beneficial owner who is not the customer, the beneficial owner and taking adequate measures, to verify his identity so that the office of issue is satisfied that it knows who the beneficial owner is, including, in the case of a legal person, trust or similar legal arrangement, measures to understand the ownership and control structure of the person, trust or arrangement;
- (iii) understanding and, as appropriate, obtaining information on the purpose and intended nature of the business relationship; and

(iv) monitoring of accounts and transactions on ongoing basis to ensure that the transactions being conducted are consistent with the office of issue's knowledge of the customer, their business and risk profile, including, where necessary, the source of funds and, updating records and data and information to take prompt action when there is material departure from usual and expected activity through regular matching with information already available with the office of issue.

(i) **“enhanced due diligence” or “EDD”** means diligence in addition to CDD and may be carried out in case of existing customers or intending customers generating suspicion for the office of issue;

(j) **“FATF recommendations”** means the applicable recommendations of Financial Action Task Force for combating money laundering and terror financing ;

(k) **“FMU”** shall have the same meaning as assigned thereto in the AML Act;

(l) **“Government institutions”** means institutions of Federal and provincial governments and include a ministry within such a government, a local government or an agency specially established by any such government or a department, organization or corporation owned or controlled by such government under a Federal, provincial or local law;

(m) **“instruments”** means the National Savings Schemes and financial instruments of various kinds that includes savings certificates and bonds issued, accounts opened and any other instruments of investment issued under the Public Debt Act, 1944 (XVIII of 1944) and rules thereunder;

(n) **“legal person”** means body of persons or an entity as a corporation, non-profit organization (NPO), non-governmental organization (NGO), trust, charity, society, association, club, etc., established under any law and considered as having many of the rights and responsibilities of a natural person and especially the capacity to sue and be sued;

- (o) "**National Savings**" or "**CDNS**" means the Central Directorate of National Savings, being an attached department of the Ministry of Finance, Government of Pakistan;
- (p) "**National Savings Centre**" means a branch, outlet or office of the CDNS;
- (q) "**office of issue**" means National Savings Centers or any other office associated with issuance, management, marketing, registration, replacement, sale and discharge of the instruments;
- (r) "**person**" includes an individual, association, authority, company, firm, institutions, partnership, society, trust or other entities;
- (s) "**politically exposed person**" or "**PEP**" means any person entrusted with a prominent public function by the state of Pakistan, a foreign country or an international organization and includes heads of state or government and members and senior officials of legislature, judiciary, executive, military and regulatory authorities and senior executives of corporations, departments or bodies that are owned or controlled by the state;
- (t) "**risk**" refers to risk associated with money laundering and financing of terrorism;
- (u) "**senior management**" means the officers of the controlling office as designated by the Board for the purpose of these rules;
- (v) "**suspicious transaction report**" shall have the same meaning as assigned thereto in the AML Act;
- (w) "**third party**" means a commercial bank regulated by the State Bank of Pakistan and engaged by CDNS under a third party arrangement to perform Know Your Client (KYC) or CDD or EDD on behalf of the office of issue; and
- (x) "**UNSCR**" means the United Nations Security Council Resolution.

(2) The words and expressions used but not defined herein shall have the meanings as assigned thereto in the Public Debt Act, 1944 (XVIII of 1944) and the AML Act, 2010 (VII of 2010).

## **CHAPTER – II**

### **AML/CFT Measures**

3. **Responsibilities of the office of issue and controlling office.**- (1)The office of issue, including all its officers and employees, shall-

(a) comply with the provisions of the AML Act and the rules and regulations issued there under for reporting of STRs and CTRs in the context of money laundering and financing of terrorism; and

(b) implement appropriate internal policies, procedures and controls for meeting the obligations specified by the AML Act and the rules and regulations issued there under.

(2) The controlling office in their respective jurisdiction in respect of the matters covered under these rules shall:

(a) make use of technology and upgrade their systems and procedures in accordance with the nature of risks of money laundering and financing of terrorism and shall for prevention of such activities and offences establish criteria for management of alerts for such risks; and

(b) maintain human resource for ensuring compliance with provisions of AML Act.

(3) The office of issue shall report all suspicious transactions, including attempted transactions, to FMU, regardless of the amount of the transaction.

(4) A CTR shall be generated by the concerned office of issue for every cash transaction of the threshold notified pursuant to the AML Act.

(5) The basis of decision to file an STR with FMU shall be documented and kept on record together with all internal findings in relation to the suspicion.

(6) The office of issue shall:-

(a) Pay special attention to the patterns of transaction, history and profile of the customers and upon finding any transaction contrary to these aspects shall examine the background of these transactions, as far as possible, and after its satisfaction that grounds warrant for reporting of such transaction, shall generate the STR to the concerned authorities; and

(b) not disclose to any person the fact of filing of an STR or CTR with FMU, except where so required by law.

(7) CDNS shall undertake measures to identify and assess the money laundering / terrorist financing (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.

(8) CDNS shall undertake risk assessments prior to the launch or use of such products, practices and technologies and take appropriate measures to manage and mitigate these risks.

### **CHAPTER – III**

#### **ASSESSING RISKS AND APPLYING A RISK-BASED APPROACH**

**4. Risk assessment and precautions.-** (1) The controlling office shall take appropriate steps to identify, assess and understand their ML/TF risks for customers, countries or geographic areas and products, services, transactions or delivery channels which include to-

(a) document their risk assessments;

- (b) consider all the relevant risk factors before determining what is the level of overall risk and the appropriate level and type of mitigation to be applied;
  - (c) keep these assessments up to date; and
  - (d) have appropriate mechanisms to provide risk assessment information to relevant authorities.
- (2) The controlling office shall-
- (a) have policies, controls and procedures, which are approved by senior management, to enable them to manage and mitigate the risks that have been identified, either by the country or office of issue or controlling office;
  - (b) monitor the implementation of those controls and to enhance them if necessary; and
  - (c) take enhanced measures to manage and mitigate the risks where higher risks are identified.
- (3) The office of issue and controlling office shall ensure that Pakistan's national ML/TF risk assessment and other risk assessments prepared by FMU or any other government stakeholder, as updated from time to time, is incorporated into their internal risk assessments and the office of issue and controlling office shall take enhanced measures to manage and mitigate the risks identified therein.

## **CHAPTER –IV**

### **Customer Due Diligence (CDD) and Know Your Client (KYC)**

5. **Application of CDD measures.**- (1) The office of issue or the third party shall apply CDD measures-
- (a) when establishing business relationship;
  - (b) while dealing with occasional customers and walk-in customers in line with sub-rule (i) of rule 4.

- (c) in other situations and scenarios when there is suspicion of money laundering or financing of terrorism, regardless of threshold; and
  - (d) when there are doubts about the veracity or adequacy of previously obtained customer identification data.
- (2) The office of issue or third party shall identify the occasional customers and walk-in-customers and verify their identity using reliable, independent source of information, i.e. NADRA verification system (Verisys) or biometric identification system (Biosys).
- (3) Every customer, whether permanent or occasional and whether natural or legal person or legal arrangement, shall be identified for establishing business relationship and for the purpose following information shall be obtained, verified using reliable, independent source documents, data or information and recorded namely: -
- (a) full name as per identity or registration documents;
  - (b) national identity card, passport, national identity card for overseas pakistanis, Pakistan origin card or alien registration card number, etc.
  - (c) registration or incorporation number of business, if applicable;
  - (d) residential address, telephone numbers and e-mail, if available;
  - (e) business address, telephone numbers and e-mail, if available;
  - (f) date of birth;
  - (g) date and place of registration or incorporation of business, if applicable;
  - (h) nationality
  - (i) place of birth;
  - (j) national tax number (NTN), if applicable;
  - (k) nature of business and location, if applicable;
  - (l) sources of earnings;



(m) customer's net worth in respect of legal persons, legal arrangements and high risk customers; and

(n) annual income

(4) The minimum set of documents to be obtained by the office of issue or third party in case of each category of customers shall be as follows:-

(a) In respect of individuals, a photocopy of any one of the following valid identity documents namely:-

(i) computerized national identity card (CNIC) issued by NADRA;

or

(ii) national identity card for overseas Pakistani (NICOP) issued by NADRA; or

(iii) Pakistan origin card (POC) issued by NADRA; or

(iv) alien registration card (ARC) issued by NADRA; or

(v) passport having valid visa on it or any other proof of legal stay along with passport in respect of foreign national individuals only.

(b) In respect of limited corporations and companies.-

(i) certified copies of-

(A) resolution of board of directors for opening of account specifying the persons authorized to open and operate the account (not applicable for single member company);

(B) memorandum of association;

(C) articles of association, wherever applicable;

(D) certificate of incorporation;

(E) Securities and Exchange Commission of Pakistan (SECP) registered declaration for commencement of business as required under the Companies Act, 2017 (XIX of 2017); and

- (F) list of directors required to be filed under the Companies Act, 2017 (XIX of 2017), as applicable;
- (ii). photocopies of identity documents as per sub-clause (b) of all the directors and persons authorized to open and operate the account;
- (c) In respect of trust clubs, societies and associations, etc.-
  - (i) Certified copies of-
    - (A) certificate of registration or instrument of trust; and
    - (B) by-laws, rules and regulations;
  - (ii) resolution of the governing body, board of trustees or executive committee, if it is ultimate governing body, for opening of account authorizing the person to operate the account;
  - (iii). photocopy of identity document as per sub-clause (i) of clause (c) of the following:
    - (A) authorized persons;
    - (B) members of governing body, board of trustees or executive committee, if it is ultimate governing body; and
    - (C) settlor, the trustees, the protector if any, the beneficiaries or class of beneficiaries
- (d) In respect of NGOs, NPOs and charities,-
  - (i) certified copies of -
    - (A) registration documents and certificates; and
    - (B) by-laws, rules and regulations;
  - (ii) resolution of the governing body, board of trustees or executive committee, if it is ultimate governing body, for opening of account authorizing the persons to operate the account;

(iii) photocopy of identity document as per sub clause (i) of clause (d) above of the authorized persons and of the members of governing body, board of trustees or executive committee, if it is ultimate governing body; and

(iv) any other documents as deemed necessary including its annual accounts and financial statements or disclosures in any form which may help to ascertain the detail of its activities, sources and usage of funds in order to assess the risk profile of the prospective customer;

(e) In respect of minor accounts,-

(i) photocopy of Form-B or birth certificate of the minor; and

(ii) photocopy of identity document as per sub-clause (i) above of the guardian of the minor;

(f) In respect of government institutions and entities not covered herein above.-

(i) CNICs of the authorized persons; and

(ii) letter of authorization from the concerned authority.

(5). the office of issue or third party shall verify identity documents of the customers from relevant authorities and bodies, including through NADRA's verification system or biometric identification system and, where necessary, use other reliable, independent sources and retain copies of all reference documents used for identification and verification.

(6). the office of issue or third party shall be responsible for verification of the identity documents and the customer shall neither be obligated nor the cost of verification be charged to the customer.

(7). where the customer is represented by an authorized agent or representative, or where customer is a legal person, the Office of issue or third party shall identify the

natural persons who act on behalf of the customer and verify the identity of such persons and the authority of such natural persons shall be verified through documentary evidence, including specimen signature of the persons so authorized.

(8). where beneficial owner is different from the customer, the office of issue or third party shall identify and take reasonable measures to verify identity of the beneficial owners using relevant information or data obtained from a reliable source, to the satisfaction of the office of issue.

(9). the verification of the identity of customers and beneficial owners, if any, shall be completed before business relations are established.

(10). the office of issue shall conduct ongoing due diligence on the business relationship, including;-

(a) scrutinizing transactions undertaken throughout the course of that relationship to ensure that the transactions being conducted are consistent with the office of issue's knowledge of the customer, their business and risk profile, including where necessary, the source of funds; and

(b) ensuring that documents, data or information collected under the CDD process is kept up-to-date and relevant, by undertaking reviews of existing records, particularly for higher risk categories of customers.

(11). the office of issue or third party shall maintain a list of all such customers and accounts where the business relationship needed to be closed on account of negative verification that includes all type of customer identity verification such as NADRA, UNSCR or any other document or information etc.

(12). The office of issue or third party shall adopt counter measures including, but not limited to, enhance due diligence proportionate to the risks to the business relationship and transactions with natural and legal persons, belonging to such countries for which

this is called upon to do so by FATF and independently of any call by the FATF to do so.

(13). in relation to legal persons and legal arrangements, the office of issue or third party shall,-

- (a) identify and verify-
  - (i) the ownership and control structure of the customer; and
  - (ii) the natural persons who ultimately own or control the customer;
- (b) obtain information about the purpose and intended nature of their business relationship;
- (c) identify the customer and verify its identity through the following information, namely:-
  - (i). name, legal status and proof of existence;
  - (ii). the powers that regulate and bind the legal person or arrangement, as well as the names of the relevant persons having a senior management position in the legal person or arrangement;
- (d) identify and take reasonable measures to verify the identity of the natural persons who ultimately has a controlling ownership interest in a legal person;
- (e) to the extent that there is doubt under clause(d) as to whether the person with the controlling ownership interest is the beneficial owner or where no natural person exerts control through ownership interests, the identity of the natural person if any, exercising control of the legal person or arrangement through other means;
- (f) where no natural person is identified under (d) or (e), the identity of the relevant natural person who holds the position of senior managing official;

(g) identify and take reasonable measures to verify the identity of beneficial owners through the following information, namely:-

(i) for trusts, the identity of the settlor, the trustee, the protector, if any, the beneficiaries or class of beneficiaries and any other natural person exercising ultimate effective control over the trust, including through a chain of control or ownership;

(ii) for other types of legal arrangements, the identity of persons in equivalent or similar positions.

(14). The controlling office shall annually review the adequacy of information obtained in respect of customers and any beneficial owners and ensure that the information is kept up to date, particularly, for high-risk categories of customers. In this respect, SOPs shall also be developed accordingly for its effective implementation.

(15). The controlling office shall establish criteria for identifying and assessing risks that may arise in relation to new products, services, business practices and delivery mechanisms, including the review of existing products and services on an on-going basis.

(16). In case of joint holders of accounts or instruments, the CDD and KYC measures specified in this chapter shall be performed on all the joint holders as if each of them was an individual customer.

(17). The office of Issue or third party shall perform the CDD measures in relation to its 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.

(18). The office of issue shall not provide any services to the individuals and entities and to those persons who are associated with such individuals and entities, whether under the proscribed or designated name or with a different name proscribed under the

Anti-terrorism Act, 1997 (XXVII of 1997), or designated under the United Nations Security Council's Resolutions Nos. 1267, 1373 and 1718 and successor resolutions, related to combating terrorism financing and proliferation financing.

(19). The office of issue shall monitor its relationships on a continuous basis and ensure that no relationship with the proscribed or designated, individuals and entities exists and where, any such relationship is found, the same should be immediately reported to FMU and other actions shall be taken as per the applicable law.

(20). The office of issue shall ensure implementation of targeted financial sanctions to comply with United Nations Security Council resolutions relating to the prevention, suppression and disruption of proliferation of weapons of mass destruction and its financing.

(21). The Office of issue shall ensure compliance with the Guidelines for Implementation of UNSC Sanctions issued by the Ministry of Foreign Affairs under the UNSC (Freezing and Seizure) Order, 2019 and the Guidelines on Actions to be taken by Competent Authorities for Implementation of United Nations Security Council Resolution No. 1373 issued by the National Counter Terrorism Authority (NACTA).

(22). The office of issue or third party shall ensure that EDD is performed in case of customers with FATF high risk jurisdictions or countries that are susceptible to proliferation financing.

(23). The CDNS may rely on a third party to conduct CDD on its behalf provided that CDNS shall-

- (a) immediately obtain necessary information relating to identification of the customer, identification of the beneficial owner and the nature of business of the customer;

(b) 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;

(c) satisfy itself that the third party is regulated and supervised or monitored for and has measures in place for compliance with CDD and record-keeping requirements in line with these rules; and

(d) maintain data or information confidentiality and in accord with non-disclosure agreement with the third party.

(e) when determining in which countries the third party that meets the conditions can be based, CDNS should have regard to information available on the level of country risk.

(24) In relation to politically exposed persons (PEPs) and their close associates or family members, the Office of issue or third party shall-

(a) implement appropriate internal policies, procedures and controls to determine if a customer or beneficial owner is a PEP;

(b) obtain approval from the senior management to establish or continue business relations where the customer or a beneficial owner is a PEP or subsequently becomes a PEP;

(c) take reasonable measures to establish the source of wealth and the source of funds of customers and beneficial owners identified as PEPs; and

(d) conduct enhanced monitoring of business relations with the customer.

(25) In relation to domestic PEPs or persons who have been entrusted with a prominent function by an international organization, in addition to performing the CDD measures, the office of issue or third party shall-

(a) take reasonable measures to determine whether a customer or the beneficial owner is such a person; and



(b) in cases when there is higher risk business relationship with such a person, adopt the measures contained in clauses (b) to (d) of sub-rule (24).

(26) In relation to non-governmental organizations (NGOs), non-profit organizations (NPOs) and charities, the office of issue or third party shall-

(a) conduct enhanced due diligence of the customer;

(b) ensure that the business relationship may not be used for unlawful objects;

(c) issue the instruments in the name of the relevant NGO, NPO or charity, as given in its constituent documents;

(d) conduct comprehensive CDD and KYC of the authorized agents or representatives as well as members of the governing body of the trust, NGO, NPO or charity; and

(e) ensure that the authorized agents or representatives as well as members of the governing body of any trust, NGO, NPO or charity having existing relationship are not affiliated with any proscribed or designated individual or entity, whether under the same name or a different name and in case of any positive match, the office of issue shall consider filing STR and take other actions as per law.

(27) The office of issue or third party shall perform enhanced due diligence where the ML and TF risks are higher.

(28) The office of issue shall not open or maintain anonymous or numbered accounts or accounts in the name of obviously fictitious names.

(29) In case the office of issue or third party is not able to satisfactorily complete required CDD measures, account shall not be opened or any service provided and consideration shall be given if the circumstances are suspicious so as to warrant the filing of an STR. If CDD of an existing customer is found unsatisfactory, the

relationship should be terminated and reporting of suspicious transaction be considered as per law and circumstances of the case.

(30) In cases where the office of issue or third party form suspicion of money laundering, terrorist financing or other criminal activity and they reasonably believe that performing the CDD process will tip-off the customer, they may not pursue the CDD process and instead file an STR with FMU.

## **CHAPTER – V**

### **Record Keeping**

6. **Record Keeping.-** (1)The office of issue or third party shall maintain all necessary records on transactions, both domestic and international, including the results of any scrutiny or analysis for a minimum period as specified but not less than ten years from completion of the transaction.

(2) The records shall be maintained showing reconstruction of individual transactions including the nature and date of the transaction, the type and amount of currency involved and the type and identifying number of any account involved in the transactions so as to provide, when necessary, evidence for prosecution of criminal activity.

(3) The records may be maintained in paper or electronic form or on microfilm, provided it is admissible as evidence in a court of law.

(4) The records of identification data obtained through CDD and KYC process, including copies of identification documents, application forms, KYC forms, verification documents and other documents along with business correspondence and results of any analysis undertaken shall be maintained for a minimum period of ten years upon termination of the business relationship.

(5) The office of issue or third party shall retain such records for longer periods of time where transactions, customers or instruments are involved in litigation or the same are required by a court of law or other competent authority.

(6) The controlling office shall satisfy, on timely basis, any enquiry or order from the relevant authorities, including law enforcement agencies and FMU, for supply of CDD information and transaction records as per law.

## CHAPTER – VI

### Internal Controls, Compliance and Audit

**7. International controls, Compliance and Audit.-** (1) CDNS shall have in place detailed policies, procedures and controls, including CDD and KYC measures, record retention, detection of suspicious transactions and obligation to file STRs and CTRs with FMU.

(2) In formulating policies, procedures and controls, CDNS shall consider the threats of money laundering and financing of terrorism that may arise from the use of new or developing technologies including transaction monitoring system, especially those having features of anonymity or inconsistency with the spirit of CDD and KYC measures.

(3) The AML and CFT measures provided in these rules shall be applicable to the office of issue outside Pakistan to the extent that laws and regulations of the host country permit and, where the AML and CFT requirements in the host country differ from those in Pakistan, the office of issue shall apply the higher of the two standards to the extent that the law of the host country so permits.

(4) The controlling office shall develop appropriate AML and CFT compliance program including through the following, namely:-

(a) appointment of a senior management level officer as compliance officer;

- (b) ensuring that the compliance officer, as well as any other persons appointed to assist him, has timely access to all customer records and other relevant information required to discharge their functions;
  - (c) ensuring establishment of high standard screening process for hiring employees;
  - (d) including compliance and AML and CFT related responsibilities in performance indicators of responsible staff down the line, in order to strengthen the compliance AML and CFT function;
  - (e) regularly assessing working strength of the compliance function and deficiency, if any, observed should be addressed on priority basis;
  - (f) devising appropriate internal mechanism for taking action against delinquent employees in case of their non-compliance with the requirements of AML and CFT; and.
  - (g) taking appropriate measures as per rules and regulations against employees found involved in money laundering (ML) and terrorist financing (TF), including referring the case to concerned law enforcement agencies for taking action under applicable laws.
- (5) The controlling office shall maintain an independent audit function reporting directly to the supervisory board that is adequately resourced and able to regularly assess the effectiveness of internal policies, procedures and controls and its compliance with regulatory requirements.

## **CHAPTER – VII**

### **Training**

8. **Capacity Building.-** (1) The National Savings shall develop and implement training programs for officers and employees concerned with AML and CFT measures, on annual basis, in order to effectively implement such measures.

(2) The training of officers and employees shall be so devised so as to enable them to understand new developments, techniques methods and trends concerning prevention of money laundering and financing of terrorism.

(3) The training shall include the responsibilities relating to AML and CFT measures, especially requirements relating to CDD and KYC and analysis of unusual transactions and alerts generated therein for possible reporting of STRs and CTRs.

(4) National Savings may acquire or develop comprehensive AML and CFT training programs, including online training programs and tests, under a comprehensive plan with clear timelines for its implementation.

## **CHAPTER – VIII**

### **National Savings AML and CFT Supervisory Board**

9. **Supervisory Board.-** (1) The Finance Division shall, constitute National Savings AML and CFT Supervisory Board to provide independent oversight of implementation of these rules and take necessary enforcement actions against violations thereof. The composition of the Board shall be as follows, namely:-

- |    |   |                             |
|----|---|-----------------------------|
| a) | Additional Secretary, Finance Division                          | <i>Chairman</i>             |
| b) | Representative of SBP not below a BPS-20 or equivalent officer  | <i>Member</i>               |
| c) | Representative of SECP not below a BPS-20 or equivalent officer | <i>Member</i>               |
| d) | Representative of FMU not below a BPS-20 or equivalent officer  | <i>Member</i>               |
| e) | Joint Secretary, Finance Division                               | <i>Member-cum-Secretary</i> |

(2) The Finance Division shall provide all secretarial and administrative support to the Board for effective discharge of its responsibilities.

(3) The Board shall, within two months of the commencement of these rules, devise its SOPs for supervision of CDNS to ensure compliance with AML and CFT requirements.

(4) The Board shall have powers to issue appropriate standard operating procedures (SOPs), demand receipt of appropriate management information system on periodical basis, direct CDNS to take such actions as may be required to address deficiencies pointed out during such assessments and advise such enforcement actions as it may deem necessary.

(5) The Board shall have powers to direct CDNS to take all reasonable measures to ensure compliance with provisions of the AML Act, 2010 and these rules.

(6) The Board shall have powers to compel production of any information or record it may require for the discharge of its responsibilities and CDNS shall provide the information and record in such format and within such timelines as may be specified by the Board.

(7) The Board shall have powers to engage chartered accountant firms from SBP's approved panel of auditors to conduct onsite examinations, assess ML and TF risks posed, assess corresponding controls and determine compliance with the AML Act, 2010 and these rules and regulations issued from time to time.

(8) If any provision of these rules, is contravened, or if any default is made in complying with any requirement of these rules or orders or SOPs issued thereunder, by any officer or official of CDNS, the person who contravened shall be punishable in accordance with the law for the time being in force.

---

[F.No.16(1)GS-I/2019-98]

-sd-  
**(Fahad Ahmed)**  
Section Officer (CDNS)

The Manager,  
Printing Corporation of Pakistan Press,  
Islamabad.

**Copy to:**

- 1) The Governor, State Bank of Pakistan, Karachi.
- 2) The Director General, Financial Monitoring Unit, SBP Building, Karachi.
- 3) The Director General, Central Directorate of National Savings, Islamabad.
- 4) The Director General, Pakistan Post Office Department, Islamabad.
- 5) The Chairman, Securities and Exchange Commission of Pakistan, Islamabad
- 6) The Managing Director, Banking Services Corporation (BSC), SBP, Karachi.
- 7) Additional Finance Secretary (Internal Finance), Finance Division, Islamabad.

-sd-  
**(Fahad Ahmed)**  
Section Officer (CDNS)