The Satara Sahakari Bank Ltd

REVISED KYC & AML POLICY

2025-26

REVISED KYC & AML POLICY

INDEX

The Satara Sahakari Bank Ltd

KYC & AML Policy 2025-26

INTRODUCTION:

The Bank has its existing KYC and Anti Money Laundering (AML) Policy approved by the Board vide the Resolution No.28, of the Board Meeting dated 24/07/2024. This policy is formulated the rules and regulations for Governing the Norms of KYC and Anti Money Laundering (AML), in addition to the various regulatory guidelines and prudential norms applicable on the basis of guidelines issued by Reserve Bank of India from time to time.

Policies in respect of opening of an account, customer acceptance policy, customer identification policy, policy in respect of monitoring of transactions and Risk Categorization of accounts.

Opening of Account & Customer identification Policy.

The KYC norms as specified by the Reserve Bank of India stipulate four key elements such as:

a. Customer Acceptance Policy.

b. Customer Identification Procedure.

c. Monitoring of Transactions and

d. Risk Management.

This policy of the Bank deals with all the four aspects.

Customer Acceptance Policy

In the beginning we now deal with the policy as regards acceptance of prospective customers who wish to open an account with our Bank. The policy also deals with closure of an existing account of a customer who is unable to furnish documents relating to his identification, where applicable.

Objective of Policy:

Branches should be vigilant while opening new account for preventing misuse of banking system for perpetration of frauds, identifying money laundering and suspicious activities, monitoring of large value cash transactions, etc. Customer identification means identifying and verifying his or her identity through reliable and independent documents and data and information.

Opening of Account and Identification of Customer

As regards the former i.e. opening of an account of prospective customer, following norms has been stipulated for the Branch Managers and for all staff working at branches who should meticulously observe compliance of these norms. The norms are mandatory.

1. a) No account should be opened unless the requisite identification documents are produced to the Bank, except small accounts as defined by RBI where strict KYC norms are not applicable.

   b) The Permanent Account Number (PAN) of customers shall be obtained and verified while undertaking transactions as per the provisions of Income Tax (I.T.) rule 114B applicable to Banks, as amended from time to time. Form 60 shall be obtained from persons who do not have PAN.

   Note: I.T. Rule 114B – Every person shall quote his Permanent Account Number (PAN) at the time of Opening of account with Bank and provide the copy of PAN Card to the Bank.

   c) PROFIT EARNING INSTITUTIONS cannot open saving bank Account. If, in any exceptional case, said account is opened, the interest will not be paid to this account.

   d) Video based Customer Indentification process can be an alternate method of customer identification with facial recognition and

customer due diligence. The Bank should take due care at the time of Video based Customer Identification Process.

2. **Deposit account in single name:** The person opening the account should furnish two recent passport size photographs, any one of the identification documents such as Identity card issued by various corporations / firms / Mathadi Kamgar Sangh, which are Registered with State Government under various acts, Job Card or Identification Letter issued by Various Govt. Offices / Companies / Corporations / Firms / Mathadi Kamgar Sangh & duly signed by officer, **Aadhar Card, Letter issued by the Unique Identification Authority of India (UIDAI),** voter's card, PAN card, driving license (with photograph), passport, etc. The concerned prospective depositor should also produce address proof such as Letter issued by Govt. Offices signed by officer with detailed address, **Aadhar Card, Letter issued by the Unique Identification Authority of India (UIDAI),** voter's card, Driving license, passport, latest copy of electricity/telephone bill, Latest Property or Municipal tax Receipt, Latest statement of accounts of other bank with detailed address, Pension or Family Pension Payment orders, Letter issued by Close Relative with his address proof, Recommendation Letter issued by Local Corporater with detailed address.

   Bank can accept and carry out Aadhar authentication / Offline verification of an individual, who voluntarily uses his Aadhar Number for identification purpose. Customer should submit the copy of Aadhar Card in such form as are issued by the Unique Identification Authority of India (UIDAI), if he provide as a proof of Possession.

   In case the person who wishes to open an account does not have the "proof of Address", then he shall provide the Proof of Address" of the relative, subject to submission of a declaration containing the words as "the said person is a relative and is staying with him / her".

With a view to reduce hardships to new customers, if the identity proof submitted by him has the same address as mentioned in the account opening form, a single document of identity may be accepted by the branches as a valid proof for both, identity and address (such as passport, driving license, etc.) In case the address mentioned in the account opening form is different than the one mentioned in the identity document, a separate proof of address should be obtained by the branches.

A rent agreement indicating address shall be Unregistered (Notarized) / registered (with the Government Authorities) before it can be accepted as an address proof.

Aadhar letter can be accepted as identity proof and address proof provided the address mentioned in the account opening form matches with that mentioned in the Aadhar letter. In case the address mentioned in the account opening form is different from the one mentioned in the Aadhar letter, a separate proof of address should be obtained by the branches.

So far as salaried employees are concerned, branches can rely on certification of identity as well as address only from reputed corporate, Mathadi Kamgar Sangh Officials.

If a professional intermediary has opened an account on behalf of his client/s, such client/s must be identified. For pooled accounts, branches should identify beneficial owners. In case such identity cannot be established, such accounts should not be opened.

A literate Minor, who has completed the age of 10 years, can open an Individual Saving account or Fixed Deposit account and operate the same. In the said account only the cash transactions are allowed. Deposit limit up to Rs.1,00,000/- in the year is allowed but withdrawal limit at a time will be Rs.5000/- and 5 times in a month is allowed, Maximum balance limit up to Rs.50,000/- is allowed. Additional

banking facilities such as ATM/Debit Card as per product suitability and customer appropriateness will be offered to this account, subject to safeguard of "NO overdraft" is allowed in the account. This account will be opened in the single name.

In case of change in Name of account due to Marriage or Otherwise, a copy of Marriage certificate issued by the State Government or Gazette notification indicating change in name together with a certified copy of the "officially Valid Document" in the existing name of the person shall be obtained for proof of address and identity, while establishing an account based relationship or while undertaking periodic updation exercise.

3. **Deposit accounts in Joint Names:** All the above norms would also be equally applicable for all the depositors in a joint account. Each depositor in a joint account is required to produce to the bank all the aforesaid documents in support of his / her individual identity, residential address, etc.

   The number for Joint holders will be restricted to FOUR only. A joint account will NOT be opened for more than four joint holders / depositors, if any one requires to open the joint account for more than four joint holders, the data and reason to be informed to Head Office.

4. **Loan account in single or joint names:** All the above norms as stated in items 2 and 3 above would also be equally applicable for any borrowing account, whether in a single name or in joint names. Even the surety/ies shall have to comply with these norms.

5. **Account of a proprietor:** In addition to the documents already mentioned, the proprietor desirous of opening deposit or borrowing account should furnish any **Two valid document** as Shop Act License, UDYAM Certificate, GST Registration, Service Tax Registration, VAT Registration, Sale Tax /

Excise Registration, License / Certificate of practice issued in the name of the proprietary concern by any professional body incorporated under statue, Complete Income Tax Return / GST Return (not only the acknowledgement, the return in the name of sole proprietor, where the firms income is reflected, duly authenticated / acknowledged by the Income Tax authorities) with Telephone & Electricity Bill in the name of business. **If the business has a turnover of over Rs.40 Lakh, audited financial statements should be obtained and in other cases, unaudited financial statements would be sufficient. Even in cases where the turnover is less than Rs. 40 Lakh, the Bank may at its sole discretion insist upon audited financial statements depending upon the credit needs and other relevant aspects involved in the credit proposal.**

In case where the accepting authority is satisfied that, it is not possible to furnish two such documents, authority at their discretion, accept only ONE document as proof of business activity. Provided authority undertake contact point verification and collect such other information & clarification as would be required to establish the existence of such firm, and shall confirm & satisfy itself that the business activity has been verified from the address of the proprietary concern.

6. **Account of partnership firm**: In addition to the **documents already mentioned in 5 above**, the Branches should obtain Registration Certificate, Copy of partnership deed, PAN Card in the name of firm, identification documents of all the individual partners and an officially valid document in respect of the person holding an attorney to transact on its behalf.

7. **Accounts of Limited Companies:** The Branches should obtain Certificate of Incorporation, Memorandum of Association, Articles of Association, PAN Card in the name of Company, and Board Resolution for opening of the account, in addition to the documents already mentioned **in 5 above**. The

persons, who are authorized to operate the account in terms of the board resolution, should submit necessary identification documents as mentioned above in item 2.

8. **Accounts of Trusts:** Trust deed should invariably be obtained irrespective whether it is a private trust or public trust. Registration certificate with Trust Deed for public & private trust with Copy of PAN Card, Latest Electricity & Telephone Bill in the name of trust should be obtained. Copy of the resolution signed by all the trustees for opening & operating the account should also be furnished. Identification documents of all the individual trustees, authorised Signatories, Beneficiaries must be obtained as mentioned above in item 2. For Operating the account of Trust, the Power of Attorney, issued by any trustee for operation in account is not permitted

9. **Accounts of Societies:** Bye-Laws of the societies along with registration certificate and resolution for opening & operating account, Copy of PAN Card must be obtained. Identification documents as mentioned above in item 2 should be obtained from the persons who are authorized to operate the account.

10. **Deposit accounts of an unicorporated association or a body of Individuals:** Resolution of the managing body of such association or body of individuals with power of attorney granted to transact on behalf and OVD of the person holding an attorney should be obtained. Also any such information as required by Branch to establish the legal existence of such an association or body of individuals may be obtained.

11. **Deposit accounts of minors:** Minor above 10 years can open saving bank account individually. Birth certificate of the minor should be obtained and the date of attaining majority should be carefully noted and recorded in the Bank's books. NO overdraft is permitted in this type of individually operated Minor account. Minor Guardian can open any type of deposit account

EXCEPT CURRENT ACCOUNT. Birth certificate of the minor should be obtained and the date of attaining majority should be carefully noted and recorded in the Bank's books. Identification documents of the natural guardian or the guardian appointed by the Court as the case may be should also be obtained as mentioned above in item 2.

For customers who are legal entities, branches should verify the legal status through proper and relevant documents, verify identity and address of the person who would act on behalf of the legal entities. Branches should ascertain the ownership and control structure of such legal entity and determine as to who are natural persons who would ultimately control the legal entity. Branches should also identity the beneficial owner and verify his identity. The beneficial owner is a natural person who would ultimately own and control the customer on whose behalf the transactions are conducted in the account.

Branch should obtain the latest open face photograph of "padadanashin" lady at the time of opening of account.

Rubber seal or metal seal should be affixed, while opening of company accounts, trust accounts and society accounts.

Customer Acceptance:

Where the documents as specified above for different categories of depositors and borrowers are not produced, the Branches should refrain from opening of the account. Further, while opening current accounts of partnership firms and limited companies, it should be confirmed that these entities do not have borrowing facilities with any other bank / banks. In case borrowing from other bank is noticed, the branches should either refrain from opening the account or should obtain NOC from such other lending bank / banks. The declaration regarding the borrowing from other bank should be taken at the time of opening of current account.

In case of difficulties, the Branches may contact Head Office.

Branches should note the following important points before opening of an account:

a. No account should be opened in anonymous /fictitious/benami name/s.

b. Not to open an account or close an existing account where the bank is unable to apply appropriate customer due diligence measures.

c. Branches should make necessary enquiries and exercise appropriate caution where the prospective customer is acting on behalf of another person/entity. This should be permitted only when it is in conformity with the established law and practice of banking. Such caution is also warranted when the account is operated by a mandate holder or a power of attorney holder or where the account is opened by an intermediary in fiduciary capacity. The Official Valid Documents (OVD) will be certified by the authorised officer.

d. Branches should apply necessary checks to ensure that the identity of the prospective customer does not match with the banned entities.

e. If an account is transferred from one branch to another, the transferee branch may open an account without insisting upon KYC documents, provided full KYC exercise has been done by the transferor branch. A fresh address proof may be obtained within six months from transfer of the account.

f. It is necessary that the customer does not have multiple identities with the bank and for that purpose branches should allot Unique Customer Identification Code (UCIC) for all new accounts opened by them. Since the code number helps branches to identify the customer, track the facilities availed, monitoring of transactions and have a better approach to risk profiling of the customer, due importance should be given for allotment of Unique Customer Identification Code (UCIC).

g. Branches should not insist upon introduction of the prospective customer provided the account opening process is document based, verification of identity and address proof is compulsory.

h. In case the proof of address furnished by the customer is not the local address or the address where the customer is currently residing, branches may take a declaration of local address on which the correspondence could be made with the customer. No proof is required to be submitted for such address. The address can be verified through positive confirmation such as acknowledgement of receipt of letters/cheque books, ATM cards, etc. In the event of change in the address, the customer should intimate the new address at the earliest.

i. When the account is operated by a mandate holder on behalf of the account holder, KYC norms are required to be complied with not only for the account holder alone but also for the mandate holder.

j. Branches should obtain **latest photograph** of the minor upon his/her attaining majority.

k. In view of RBI findings that the customer/prospective customer desiring to open the account/walk in customers not having an account with the branches, furnish dummy/fake Permanent Account Numbers (PANs) which are quoted on vouchers for transactions of Rs. 50,000/- and above, branches should follow the following procedure meticulously:

a) Branches should obtain xerox copy of PAN card duly verified with the original and keep the same on records. **PAN should be mandatory in all accounts where Cash transactions are occurred.**

b) If the existing customer has already submitted xerox copy of PAN card with the branches duly verified with the original, branches should confirm and verify the PAN number quoted on the relative voucher.

c) The above procedure shall also apply mutatis mutandis for sale of third party products such as mutual fund products, life insurance products and asset insurance.

d) The above procedure shall also apply mutatis mutandis for sale of our bank's own products such as issue of demand drafts, issue of ATM cards and other ancillary business.

l. If Individual Customer desirous to receiving any benefit or subsidy under any scheme notified under Aadhar Act, 2016, the bank shall obtain the Aadhar and may carry out its e-KYC authentication based on his declaration that he is desirous of receiving benefit / subsidy under the act.

m. While submitting Aadhar for Customer Due Diligence, the bank will redact or blackout their Aadhar Number.

n. Bank will give timeline (As Notified by Government) for submission of PAN or Form No.60 for existing customers, failing to that Bank will temporarily cease the operations in the account by giving notice to customer.

o. Bank can make "Digital KYC" or Video based Customer Identification Process (V-CIP) of the Customer, by taking all necessary precaution regarding the verification of Aadhar, PAN, etc. Bank will also obtained the latest Photograph of the customer.

p. If an e-document is obtained from the customer (for KYC or otherwise), the officer will verify the digital signature as per the provisions of the Information Technology Act, 2000.

Branches should keep in mind that the information collected from the customer for the purpose of opening of the account be treated as confidential. Information sought from the customer is relevant for KYC purpose and not intrusive and not an encroachment to his privacy.

Special Categories of Customer Accounts

Before opening the following categories of accounts, the Branches should take prior permission of Head Office:

1. Politically Exposed Persons (PEPs)

Politically Exposed Person (PEP) is an individual who is entrusted with prominent public function in a foreign country such as Head of the State or Government, Senior Politician, Senior Government/Judicial/Military Officer, Senior Executive of the State Owned Corporations, important political party official, etc.

Person of foreign origin on diplomatic mission to India shall also qualify as PEP. Person holding prominent position in multi-lateral agency (such as United Nations, World Bank, etc.) shall also qualify as PEP.

All the accounts of persons named above shall be considered as 'High Risk' accounts. Additional Due Diligence (ADD) is required to be exercised.

2. Non face-to-face customers.

Prospective customers with whom the bank has not had direct interaction at the time of opening of the account are called non face to face customers. Such customers include foreign resident banks, correspondent banks, embassy officials, etc.

All the accounts of persons named above shall be considered as 'High Risk' accounts. Additional Due Diligence (ADD) is required to be exercised.

3. Persons of dubious reputation.

Such persons include persons with criminal background, persons convicted by the court of law for criminal offences, persons convicted for moral turpitude, persons involved in drug trafficking, etc. Dubious reputation of such persons can be determined on the basis of information available on public domain.

All the accounts of persons named above shall be considered as 'High Risk' accounts. Additional Due Diligence (ADD) is required to be exercised.

4. Impersonal accounts having legal entity

Where the account is opened in the name of a legal entity, persons controlling the interest and persons who are beneficial owners should be identified and identification documents should be obtained. Matter should be referred to Head Office in case of doubt.

5. Fiduciary Accounts:

An advocate or chartered accountant or share broker opening the account for their clients, the matter should be referred to Head Office. Title of the account would reflect the nature of the account held by a fiduciary.

Fiduciary accounts are also opened by intermediaries such as administrators, assignees, etc. While opening the account, letter of administration and other relative documents as applicable should be obtained.

6. Pooled Accounts:

These are also fiduciary accounts where investments of a number of persons are pooled together. Title of the account would reflect the nature of the account held by a fiduciary. Mutual funds, pension funds, etc. are regulated entities and opening of account of such funds may not pose much problems. Pooled accounts managed by other persons on behalf of wide range of clients should be exposed to enhance due diligence and identity of individual investors and beneficiaries should also be established at the time of opening of the account.

7. No account should be opened of an entity which is banned by Law.

While opening the accounts, Branches should refer to the list of banned entities and banned persons published by Reserve Bank of India in respect of terrorists and terrorist organizations. Head Office has already circulated

lists of such banned entities and banned persons from time to time. This list should be referred to by the Branches to confirm that the person/entity opening the account does not belong to the list circulated by Head Office.

There are three lists of terrorists and terrorist entities published by United Nations Organization (UNO). These are

a. Consolidated list of individuals and entities which can be accessed at the UNO's website at http://www.un.org/sc/committees/1267/aq sanctions list.shtml.

b. The updated A-Qaida Sanctions List is available at https://scsanctions.un.org/ohz5jen.al-quida.html

c. The updated 1988 Sanctions list (Individuals associated with Taliban and entities and groups associated with Taliban) is available at https://scsanctions.un.org/3ppp1en-taliban.htm

Branches should visit the above websites before opening of an account and ensure that the name of the proposed customer does not appear in the list. Further, branches should scan all existing accounts to ensure that no account is held by or linked to any of these individuals or entities included in the list.

In case the particulars of the customer match with the individuals/entities, branches should report the matter to Head Office.

Branches should ensure that the identity of the customer does not match with any person with known criminal background.

8. **The following type of accounts should NOT be opened**.

a. Liquidator's account.

b. Executor's account.

c. Account opened under Married women property act / Guardians of Estate.

d. Mad person Insane.

e. Foreign Origin Person.

Closure of Account.

1. For an existing account where the account holder does not furnish the requisite documents of identity and other relative documents as mentioned above for any reason, Branches can consider closing the account after giving due notice to such account holder and giving a period of one month for submission of the documents. During the intervening period, debits should not be allowed in such accounts. In case no positive response is received from the customer within the stipulated period of one month from the date of notice, the account can be closed by issuing pay order by post on the last known address of the customer by Registered Acknowledgement Due.

2. As regards closure of account in the name of deceased depositor, the nominee or the holder of succession certificate or legal heirs as the case may be should be properly identified before making payment.

3. As regards closure of account for the reasons such as transfer of the account holder to another city or town or change in location in the same city, the reasons should independently be confirmed/ ascertained.

Transactions in the account, Risk classification and Monitoring of account.

At the time of opening of any customer, the risk category will be “Low Risk”, but it may be changed to High risk on the basis of customer’s background, nature and location of activity, country of origin and his client profile, etc. Branches are required to classify all accounts according to risk perception. The accounts should be classified as accounts having low risk, accounts having moderate risk and accounts having high risk. Customers that are likely to pose a higher risk than the normal risk to the bank should be categorized as high risk depending

upon the customer's background, nature and location of activity, country of origin, sources of funds and his client profile, etc. Branches should apply enhanced due diligence measures based upon the risk assessment, thereby requiring intensive due diligence for higher risk customers, particularly those for whom the sources of funds are not clear. The following are some of the examples of customers having "High Risk" category.

1) Politically Exposed Persons (`s)
2) Person having nationality of High Risk Countries.
3) Trust Accounts.
4) Jewellers Accounts.
5) Accounts having the business of Expolsives.
6) Non Resident Indians (NRIs) / Foreign Nationals.
7) Non face-to-face customers.
8) Fiduciary ccounts.
9) Pooled Accounts.
10) Accounts having the high amount of Transactions.
11) Heavy Transactions Accounts.
12) Fraudster's Account.
13) Persons of Dubious reputation, etc.

The transactions includes deposit, withdrawal, exchange or transfer of funds in whatever currency, whether in cash or by cheque, payment order or other instruments or by electronic or other non physical means.

Branches should pay special attention to any money laundering threats that may arise from new or developing technologies including internet banking that might favour anonymity, and take measures, if needed, to prevent the same being used for money laundering purposes. At the time of issuance of variety of Electronic Cards that are used by customers for buying goods and services, drawing cash from ATMs, and can be used for electronic transfer of funds, Branches should ensure that appropriate KYC procedures are duly applied

before issuing the cards to the customers. Branches are required to ensure full compliance with all KYC/AML/CFT guidelines issued from time to time, in respect of add-on/ supplementary cardholders also.

The definition of transactions has now been modified by RBI and the ambit has been enlarged to additionally include the following:

a. Any transaction of purchase, sale, loan, pledge, gift, transfer, delivery or any arrangement therefore.

b. Opening of an account.

c. Safe deposit vault transactions.

d. Any transaction involving fiduciary relations.

e. Any payment made or received in whole or in part of any contractual or legal obligation.

f. Any transaction establishing or creating a legal person or legal arrangement.

Branches should note the revised definition of transactions for the purpose of monitoring.

1. Branches should closely monitor cash withdrawals of large amounts. Where third party cheques/drafts/instruments are deposited in the existing and newly opened accounts followed by cash withdrawals for large amount, branches should keep a proper vigil over such transactions and file STR if need be.

2. For cash credit and overdraft accounts, cash deposits and cash withdrawals of Rs. 5 Lakh and above should be closely monitored. The purpose of withdrawal of cash of such high magnitude should be inquired into. If suspicious/dubious nature is observed and ascertained, STR should be filed with cogent and justifiable rationale.

3. If any savings/current account shall be treated as inoperative, if there are no **customer induced transactions** in the account for a period of over two years. Customer induced transactions are of following types.

Financial Transactions:

a. ATM/Cash withdrawals / deposit
b. RTGS/NEFT/IMPS/UPI/AePS/ABPS transactions
c. Internet Banking Transactions.
d. Debit Crd Trnsactions.
e. Transafer of funds from /to the linked CBDC (e-Rupee) account.
f. Cheque Clearing.
g. Remittance of funds by way of demand drafts.
h. Cash withdrawals by third party through cheque.
i. Standing instructions issued by the customer.
j NACH Debit / Credits.
k.Term deposit interst proceeds.
l. Dividend on shares / Interest on Denebturesor any other investment proceeds.
m. Direct Benefit Transfer (DBT) credits.
n. Refunds like refunds related to e-commerce payment. Income Tax Returns, etc.
o. National Elecronic Toll Collection (NETC) debits **OR**

Non Financial Transactions **OR**

KYC Updation through Digital channel i.e Internet banking or Mobile Banking.

Branches should take on going review of all accounts with a view to identify inoperative / dormant accounts and ensure that these accounts are locked in the system. These accounts should be made operative at the request of the customer only upon proper identification. Since dormant accounts are deemed as fraud prone area, branches should exercise strict vigil over these accounts. Fresh due diligence, genuineness of transaction, verification of signature and establishing due identity of the customer should be carried out before activating the dormant account.

4. Branches should ensure that any remittance of funds by way of demand draft, mail transfer or telegraphic transfer or any other mode such as

RTGS/NEFT for Rs. 50,000/- and above is effected only by way of debit to the customer's account and not against cash payment.

5. Large value cash transactions inconsistent with the normal activity of the customer as also very high turnover inconsistent with the size of the balance maintained in the account should be strictly monitored. Such accounts be classified as high risk accounts requiring enhanced due diligence.

6. **It is necessary for the branches to verify all high value transactions and find out whether they involve any element of suspicious nature. In case branches are satisfied that these transactions do not involve any suspicious nature by ascertaining the reasons and due verification, the transactions could be white listed. Otherwise, they may be reported in STR with rational and cogent reasons. Branches should verify all alert generated transactions regularly on daily basis. These transactions should be scrutinized thoroughly and their genuineness should be verified. Source of fund should be ascertained and documentary evidence should be kept on record. Branches should strictly note that such alert generated high value cash transactions are white listed at the branch by an official not below the rank of Branch Manager / Officer.**

7. All cash transactions where forged or counterfeit currency notes are used as genuine should be reported in STR.

8. Where forged/fake documents have been submitted to the bank, such transactions should be reported in STR.

Monitoring of transactions

Receipt of Foreign Contribution Policy.

Any Indian Association receiving foreign contribution is required to get itself registered with Ministry of Home Affairs (MHA), Government of India. If the

association is not registered with Ministry of Home Affairs (MHA), the bank cannot accept the foreign contribution for the customer unless prior permission is obtained from Ministry of Home Affairs (MHA) by the concerned association.

In view of the above, branches should take following precautions:

a. To give credit of the foreign contribution only if the association is registered with Ministry of Home Affairs (MHA). Branches should note registration number and keep the same on record.

b. In case the association is not registered with Ministry of Home Affairs (MHA), branches should insist on production of written permission of Ministry of Home Affairs (MHA) for acceptance of specific amount of contribution.

In addition, branches are also required to submit a return, to Head Office, furnishing the details of foreign contributions credited to the accounts of the associations on half yearly basis on 30th September and 31st March every year in the specified format.

Monitoring of transactions

Wire transfers and cross border wire transfers

Foreign Inward Remittance

Where the branches receive remittance of fund from foreign banks by way of wire transfers or cross border wire transfers, it would be necessary to confirm and ascertain that the remitter has submitted requisite Know Your Customer (KYC) documents to the remitter bank. The inquiry should be made with the remitter bank and in case of doubt, xerox copies of Know Your Customer (KYC) documents may be called for. Branches should note this aspect meticulously for implementation. In so far as remittance coming from foreign countries which are declared by United Nations Organisation (UNO) as deficient countries in

respect of compliance of Know Your Customer (KYC) norms, combating financing of terrorism and anti money laundering, enhanced due diligence should be exercised by the branches before effecting credit to the account.

Legal Entity Identifier (LEI):

The Legal Entity Identifier (LEI) is a 20 digits number used to uniquely identify parties to financial transactions worldwide to improve the quality and accuracy of financial data system.

Reserve Bank of India vide their notification No. A. P. (DIR Series) Circular No.20 dated 10/12/2021, has instructed the banks to obtain the LEI number from resident entities (Non-Individuals) undertaking capital or current account transactions of Rs.50.00 Crores and above (Per Transaction) Under FEMA Act, with effect from 01/10/2022.

The banks are also instructed to develop the required systems in place to capture the LEI information and ensure that any LEI captured is validated against the global LEI database available on the website of the Global Legal Entiry Identifier Foundation (GLEIF).

The general guidelines in respect of classification are given below:

1. The customers who have not furnished requisite documents such as photograph, PAN card, address proof and photo identity documents despite reminders should be classified as high risk accounts.
2. The transactions in the customer's account are very high in value and in number not commensurating with his known income should be classified as high risk account.
3. Where the customer is a salary earner, there are several credit transactions other than monthly salary; the Branches should obtain satisfactory explanation for such transactions. If the explanation is not furnished or the

explanation furnished is not satisfactory, the account should be construed as high risk account.

4. Where there are several cash transactions each below Rs. 1 Lakh in a single month in a personal account, such account should be treated as high risk account if no satisfactory explanation there for is furnished by the customer concerned.

5. In case of small accounts where average balance in the account does not exceed say Rs. 1,000/- and that high value cheques (say above Rs. 5 Lakh) are deposited, such accounts should be classified as high risk accounts where there is no satisfactory explanation as regards source of funds.

6. Where the transactions are far in excess of the known income of the customer, such accounts should be classified as high risk accounts.

7. Where the turnover in the account is not commensurating with the known means or with the nature of business of the customer, such accounts should be classified as high risk accounts.

8. In a newly opened account where high value cheques are deposited and the amount is immediately siphoned out upon realization of the cheques, the account should be classified as high risk account.

9. Accounts of Politically Exposed Persons (PEPs) should be classified as high risk accounts.

10. Customers having business where value of goods is not easily assessable should be classified as high risk accounts (e.g. trader dealing in sale/export of antique articles)

11. Any business which deals in money as commodity like money exchange bureaus should be classified as high risk accounts.

12. Trust accounts are considered as popular vehicles which avoid the identification and mask the origin of money and as such should be classified as high risk accounts.

13. Indians resident overseas (NRI) and foreign nationals based in India should be classified as high risk accounts.

14. Accounts of non face to face customers should also be classified as high risk accounts. The First payment of Non-face-to-face customer will be effected

through the customers Know Your Customer (KYC) complied account with another Regulated Entity (RE).

15. For transactions conducted through correspondent banking, it should be ascertained whether the correspondent bank is regulated under Financial Action Task Force (FATF) guidelines and has adopted the said guidelines. Where the correspondent bank does not follow Financial Action Task Force (FATF) guidelines, such transactions should be classified as high risk transactions and the account in which such transactions take place should also be classified as high risk account.

16. Pooled accounts where identity of individual investors and that of the beneficiaries is obscure, such accounts should be classified as high risk accounts.

17. Accounts of bullion dealers should be classified as High Risk accounts requiring enhanced due diligence on the part of branches. Monitoring should be intensive in such high risk accounts for the purpose of identifying suspicious transactions.

Note: High risk accounts and transactions therein should be carefully monitored by the branches. All documentary evidence in respect of identity and other relevant documents depending upon the category of the account should be obtained. In addition, information on net worth, business activity of Non Resident Indian (NRI) customers, verification of customer information from independent sources etc. should also be obtained. High risk categories also include Non Government Organizations (NGOs), companies having close share holding structure, partnership firms having sleeping partners, etc.

Parameters for risk categorization

Some indicative parameters which can be used to determine risk category of the customers are given below:

1. **Customer constitution:** Individual, proprietorship, partner-ship, private limited, etc.
2. **Business segment:** Retail, Corporate, etc.
3. **Country of residence/ Nationality:** Whether India or any overseas location/ Indian or foreign national.
4. **Product subscription:** Salary account, Non Resident Indian (NRI) products, etc.
5. **Economic profile:** High Net worth Individuals (HNIs), public limited company, etc.
6. **Account status**: Active, inoperative, dormant.
7. **Account vintage:** less than six months old, etc.
8. **Presence in regulatory negative:** Politically Exposed Persons (PEP)/ defaulter/fraudster lists.
9. **Filing of STR:** Suspicious Transaction Report (STR) already filed for the customer.
10. **Alerts generated from system:** AML Alerts
11. **Source of funds:** Indigenous or Foreign, obscure or clear, verifiable or non verifiable.
12. **Occupation**: Salary earner or businessman, exporter or otherwise, etc.
13. **Purpose of opening the account:** For personal reasons or for business.
14. **Nature of business**: Trader or manufacturer, importer or exporter, retailer or whole Seller.
15. **Mode of operation**: Single or joint, by self or power of attorney, etc.
16. **Credit rating:** Rating based upon past experience on utilization of limits and operations in the account.

Each customer would be classified based upon the risk parameters and assigned risk on case to case basis. Loan accounts which are of non operative nature (e.g. term loans) having a pre determined cash flow can be regarded as low risk accounts.

A high risk account requires a more enhanced monitoring by way of periodical reviews as compared to low risk accounts.

When should a Branch apply Customer Due Diligence (CDD)?

Customer Due Diligence (CDD) should be conducted as a part of the Customer Identification Procedure. The Branch should apply Customer Due Diligence measures when it:

i. establishes a business relationship;

ii. Carries out an occasional transaction;

iii. Suspects money laundering or terrorist financing, or

iv. Doubts the veracity of documents, data or information previously obtained for the purpose of identification or verification

v. On going basis i.e. after completion of period of two years or before, after the date of submission of KYC documents.

When the Branch is unable to apply Customer Due Diligence measures, it:

i. must not establish a business relationship or should not carry out an occasional transaction with the customer;

ii. Should not carry out a transaction with or for the customer through a bank account;

iii. Should terminate all existing business relationship with the customer;

iv. Should consider whether it ought to report to Financial Intelligence Unit of India (FIU-IND)/ Regulators, in accordance with extant guidelines.

Types of Customer Due Diligence (CDD)

There are three types of Customer Due Diligence (CDD) that can be used by a bank in accordance with the risk category of the customer. These are listed as follows:

1. **Basic Due Diligence:** This implies collection and verification of identity proof, address proof and photograph to establish the identity of the customer. This is based on documents required. Different sets of documents have been listed for different types of customers. The Branch can draw reference from the list of indicative documents prescribed in this policy. The Branch should not restrict itself solely to that list. Documents other than the indicative list such as a property tax bill, registration certificate, license issued by the local authorities, shop act license, sales tax returns, income tax returns, GST Reurn, GST certificate, VAT certificate, certificate of practice issued by institute of Chartered Accountants of India, certificate issued by Companies Secretaries of India, Indian Medical Council, Food & Drug Control Authorities, registration certificate issued by Sales Tax, Service Tax, Professional Tax authorities, etc. as acceptable.

2. **Simplified Due Diligence:** Any due diligence applied to establish the identity of customer, which involves measures less stringent than basic due diligence can be termed as 'Simplified Due Diligence'. Simplified due diligence can be applied to accounts of people belonging to low income group, both in urban as well as rural areas, to enable 'Financial Inclusion' of this segment. It can also be applied to accounts which have a financial cap, like the "Small Deposit Accounts" where the balances of the account and total credits of the account at any point of time in a year should not exceed Rs. 50,000/- and Rs. 1,00,000/- respectively as also the aggregate of all withdrawls and transfers in a month should not exceed Rs.10000/-.

3. **Enhanced Due Diligence (EDD):** Any additional due diligence measures undertaken over and above the basic due diligence can be termed as 'Enhanced Due Diligence'. Enhanced Due Diligence (EDD) needs to be undertaken for all the high-risk customers of a branch. Other Enhanced Due Diligence (EDD) measures like enhanced level of transaction monitoring for high-risk customers should be undertaken by the branches for customers

who fall in the high-risk category. Enhanced Due Diligence (EDD) on existing accounts may also be conducted if required when Anti Money Laundering (AML) alerts are generated as a part of the transaction monitoring process.

Specific types of relationships where Enhance Due Diligence (EDD) measures could be applied are:

i. **Politically Exposed Persons (PEPs):** Politically exposed persons are individuals who are or have been entrusted with prominent public functions in a foreign country, e.g., Heads of States or of Governments, senior politicians, senior government/judicial/military officers, senior executives of state-owned corporations, important political party officials, etc. Persons of foreign origin/ diplomatic missions, such as the ones listed above, located in India, also qualify as Politically Exposed Persons (PEPs). Persons holding prominent positions in multilateral agencies such as the United Nations, World Bank, etc, can also be construed as Politically Exposed Persons (PEPs). Politically Exposed Persons (PEPs) of foreign origin and their associates and relatives form group of customers, which should be considered as 'High Risk' by the Bank. Bank should obtained additional information/carry out additional due diligence depending on the risk perception in respect of transactions handled on their behalf. Banks should however, take care not to deny service to Politically Exposed Persons (PEPs) on account of their higher risk perception.

ii. **High Risk Countries:** Customers who live in countries that are considered High Risk or deficient in respect of implementation of Know Your Customer (KYC) and Anti Money Laundering measures should be classified by the branches as high risk. The list of such countries based on parameters such as **F**inancial **A**ction **T**ask **F**orce (FATF) membership, advisories issued by Financial Action Task Force (FATF)/United Nations (UN) on certain countries, etc. A country risk rating can be further integrated into the customer risk emanating from the country of their residence.

iii. **Specific types of business:** Customers having business where value of the goods is not easily assessable like antique dealers and businesses dealing in money as a commodity like money exchange bureaus need to classify as high risk.

iv. **Trust accounts:** Trust accounts require strict documentation and due diligence to be exercised. Trusts are popular vehicles for criminals wishing to avoid the identification procedures and mask the origin of the criminal money they wish to launder. The principal objective for money laundering prevention via trusts is to verify the identity of the provider of trust funds/ those who have control over the trust funds, i.e. the grantors, settlers & trustees.

v. **Non resident Indians (NRIs)/Foreign Nationals:** Indian customers resident overseas and foreign nationals based in India pose a bigger risk from money laundering perspective than ones placed domestically.

vi. **Non face-to-face customers:** Customers with whom the bank has not had direct interaction at the time of opening the account would require stricter documentation e.g. Certification by independent authority such as notary, foreign resident banks, correspondent banking partners, embassy officials; insisting on additional documentation to establish identity and address etc.

vii. **Correspondent Banking:** Transactions conducted through correspondent relationships need to be managed taking a risk-based approach. "Know Your Correspondent" procedures should be followed to ascertain whether the correspondent bank or counterparty is itself regulated for money laundering prevention and, if so, whether the correspondent is required to verify the identity of their customers to **F**inancial **A**ction **T**ask **F**orce (FATF) standards. Where the correspondent bank are not following **F**inancial **A**ction **T**ask **F**orce (FATF) guidelines, additional due diligence should be exercised by the branches. Additional due diligence would be required to ascertain and assess

the correspondent's internal policy on money laundering prevention and its Know Your Customer (KYC) procedures. Transactions conducted through correspondent relationships need to be monitored by the branches taking a risk-based approach. Particular attention should be paid by the branches to the type of business that the correspondent engages in, the market place in which it operates, etc. A country risk rating model can also be used to evaluate money laundering risk emanating from the country of location & operations.

viii. **Fiduciary Accounts:** Bank may exercise enhanced due diligence at the time of opening fiduciary accounts by intermediaries such as guardians of estates, executors, administrators, assignees, receivers etc. For example while opening of the account of an administrator of the estate, it may be necessary to examine the Letter of Administration (Authority) as it would give a picture of the assets of the estate.

ix. **Pooled Accounts -** Pooled Accounts are essentially fiduciary accounts where investments of a number of persons are pooled together. Normally, such accounts are titled to reflect that the account is being held by a fiduciary. The fiduciary or financial intermediary operating the pool is expected to maintain records that contain statements of all accounts giving investments and disbursements. Pooled accounts managed by professional intermediaries on behalf of entities like mutual funds, pension funds, etc. may not pose much difficulties as these are generally regulated entities. Branches may also come across pooled accounts managed by lawyers, chartered accountants or stockbrokers on behalf of a range of clients. Branches should endeavour to satisfy about the identity of individual investors/beneficiaries of the pool at the time of opening such account. Branches should also satisfy that the intermediary managing the pool in a fiduciary capacity maintain proper accounts of individual investors.

Customer Due Diligence (CDD) of all the members of Self Help Group (SHG) may be undertaken at the time of credit linking of Self Help Group (SHG)

In case of high risk customers, branches may obtain additional information on the customer beyond documentary evidence. An indicative list is as under:

• Information on net worth

• Intended business activity in case of Non Resident Indians (NRI) customers

• Report by relationship manager/ branch manager

• Higher level of approvals

• Verification of customer information with independent data sources

Review of Risk Categorization:

Risk Categorization of an account is neither once for all nor permanent in nature.

Branches should note that classification of the customer's account as high risk, moderate risk or low risk is neither once for all nor permanent in nature. For example, where the customer's account is classified as high risk on account of non submission of documents as mentioned above, the classification could be lowered if the requisite documents are subsequently furnished to the satisfaction of branches.

It should be noted that the accounts should be classified by the Branches depending upon nature of operations in the account. Further, the nature of transactions such as deposit/withdrawal of high amount and that too in cash not commensurating with the known means or nature of business, etc. should be the deciding criteria for classification of accounts.

Frequency of review of risk categorization:

Branches should review risk classification of all accounts at a half yearly frequency in the normal course of business. Where suspicious transactions are noticed, the Branches should **immediately** change the status. Further, when any of the circumstances as mentioned elsewhere in this policy are observed, the risk categorization of the account should immediately be changed.

Customer profile should be updated at a frequency as under:

a. Once in 10 years for Low Risk category

b. Once in 8 years for Medium / Moderate Risk Category and

c. Once in every two years in High Risk accounts.

Customer profile should be updated by obtaining all Know Your Customer (KYC) documents required as per the constitution of the customer (such as natural person and legal person).

Branches should note further that all the accounts where the fraud has been committed by the account holder (with or without connivance with outsiders or staff), such accounts should be classified as high risk accounts and that all the transactions in the account should be reported as Suspicious Transactions in Suspicious Transactions Report (STR).

'Tipping off'

All Branch Managers and all staff members working in branches should carefully ensure that the customers are not informed (i.e. tipped off) that his account is under monitoring for suspicious activities and that a disclosure has been made to Financial Intelligence Unit - India (FIU-IND).

Where the Branches make enquiries to learn more about the transactions in an account for determining whether the transactions are of suspicious nature, in such circumstances care must be taken to ensure that the suspicion is not disclosed to anybody.

Other guidelines for branches

1. Branches should not open any account, unless full scale Customer Due Diligence (CDD) is carried out, where there is a suspicion of money laundering, terrorist element and other elements giving rise to high or moderate risk.

2. Branches should consider to close the existing accounts by following due procedure where they are unable to apply customer due diligence (CDD) measures. Before closure of such accounts, the branches should file **S**uspicious **T**ransaction **R**eport (STR) with Financial Intelligence Unit, India (FIU-IND) through Head Office in respect of the transactions taking place in the mean time.

3. Branches should strictly monitor and report all transactions and suspicious transactions falling in Know Your Customer (KYC), Anti Money Laundering (AML) and combating the Financing of Terrorism (CFT) violations to Head Office from time to time. Non-reporting of transactions eligible for reporting shall be viewed seriously.

4. All the accounts of political parties, political persons and their relatives should also be applied full scale enhanced customer due diligence.

5. Sometimes bank accounts are also opened by professionals (such as Lawyers, Chartered Accountants, Stock Brokers, etc) for and on behalf of their clients (ultimate beneficiaries). Here also full scale enhanced customer due diligence be applied not only for the professionals alone but also for ultimate beneficiaries, even though the professionals may have been bound by client confidentiality.

6. Certain countries (as mentioned in the notification published by United Nations on its web site **http://www.un.org**) have not adopted or insufficiently adopted Know Your Customer (KYC) procedures or

recommendations of **F**inancial **A**ction **T**ask **F**orce (FATF). Any transactions relating to such countries or persons from such countries are required to be examined thoroughly. The lawful purpose and background of such transactions should not only be examined but also the documents relating to such transactions should be preserved for Reserve Bank of India (RBI) inspection or any other inspection.

7. There are certain financial institutions in foreign countries (as mentioned in the notification published by United Nations on its web site (**http://www.un.org**) which allows their accounts to be used by other banks. Any transactions with such banks should also be thoroughly examined by applying strict enhanced Customer Due Diligence (EDD).

8. The Regulatory Entity (RE) will carry out "Money Laundering (ML) and Terrorist Financing (TF) Risk Management" exercise periodically to identify, assess and take effective measures to mitigate its money laundering and terrorist financing risk for clients, countries or geographical areas, products, services, transaction or delivery channels, etc. While assessing the Money Laundering (ML) or Terrorist Financing (TF) risk, the Regulatory Entity (RE) will take cognizance of the overall sector- specific vulnerabilities, if any, that the regulator / supervisor may share with Regulatory Entity (RE) from time to time. The internal Risk assessment carried out by the Regulatory Entity (RE) will be commensurate to its size, geographical presence, complexity of activities / structure, etc. Also Regulatory Entity (RE) shall apply a Risk Based Approach (RBA) for mitigation and management of the identified risk.

CENTRAL KYC RECORDS REGISTRY:

Government of India established the Central KYC Records Registry for recording of Know Your Customer (KYC) documents of each and every accountholders with the Banks. It is mandatory to Primary Co-operative Banks to upload the Know Your Customer (KYC) data pertaining to all new

Individual accounts opened on or after 01st April 2017 with CERSAI in terms of the provisions of the Prevention of Money Laundering Rules, 2005. The said information is to be uploaded to KYC registry in ONLINE Mode and every bank should register their entity with them. It is now necessary to all Co-operative Banks to upload the Know Your Customer (KYC) data pertaining to all new Legal Entities (LE) from 01st April 2021.

Reports to be furnished to FIU-IND:

a) Cash Transaction Report (CTR):

(i) The Cash Transaction Report (CTR) for each month should be submitted by Branch to Head Office by 10th of the succeeding month. Cash transaction reporting by branches should invariably be submitted on monthly basis for ensuring to submit Cash Transaction Report (CTR) for every month to Financial Intelligence Unit - India (FIU-IND) within the prescribed time schedule.

(ii) All cash transactions, where forged or counterfeit Indian currency notes have been used as genuine should be reported to the Principal Officer of the bank in the specified format (Counterfeit Currency Report – CCR), by 5th day of the next month. These cash transactions should also include transactions where forgery of valuable security or documents has taken place and may be reported to Principal Officer at Head Officer in plain text form.

(iii) While filing Cash Transaction Report (CTR), details of individual transactions below Rupees Fifty thousand need not be furnished.

(iv) Cash Transaction Report (CTR) should contain only the transactions carried out by the branch on behalf of their clients/customers excluding transactions between the internal accounts of the bank.

(v) A summary of cash transaction reports for the bank as a whole should be compiled by the Principal Officer of the bank every month in physical

form as per the format specified. The summary should be signed by the Principal Officer and submitted to Financial Intelligence Unit - India (FIU-IND). If the Cash Transaction Report (CTR) compiled centrally by bank for the branches having Core Banking Solution (CBS) at their central data centre, bank may generate centralised Cash Transaction Report (CTR) in respect of the branches under core banking solution at one point for onward transmission to Financial Intelligence Unit - India (FIU-IND), provided the Cash Transaction Report (CTR) is to be generated in the format prescribed by Financial Intelligence Unit - India (FIU-IND);

(vi) A copy of the monthly Cash Transaction Report (CTR) submitted to Principal Officer at Head Office in respect of the branch should be available at the branch for production to auditors/inspectors, when asked for.

b) Suspicious Transaction Report (STR):

The STR should be furnished within seven days of arriving at a conclusion that any transaction, whether cash or non-cash, or a series of transactions integrally connected are of suspicious nature. The Principal Officer should record his reasons for treating any transaction or a series of transactions as suspicious. It should be ensured that there is no undue delay in arriving at such a conclusion once a suspicious transaction report is received from a branch. Such report should be made available to the competent authorities on request.

The reporting of suspicious transactions by the employees of the bank does not constitute a breach of bank's duty of confidentiality owed to the customers. In terms of provisions under Prevention of Money Laundering Act (PMLA) Act, 2002, the bank and its employees are not liable to any civil proceedings against them for furnishing the information on any suspicious transaction.

As far as our bank is concerned, the transactions of the nature mentioned in items 4, 5, 6 & 7 above would be rare or mostly absent. However, instructions are reproduced to take care of any future eventuality as and when such transaction may take place.

Having regard to the fact that Government of India, FIU-IND and RBI attaches great importance to the above subject; branches are harped upon to take utmost care. Branches should also go through the list of terrorist and terrorist organizations published and updated from time to time by United Nations on its web site http://www.un.org.

In order to detect the nature of suspicious activities of the customer, following details would be useful for the branches:

a. Customer behaviour indicators

b. An indicative list of suspicious activities such as

i. Transactions involving large amounts of cash

ii. Transactions that do not make economic sense

iii. Activities not consistent with the customer's business

iv. Customers attempting to avoid reporting/record keeping requirements

v. Unusual activities

vi. Customers who provide insufficient or suspicious information

vii. Customers making suspicious transfer of funds

viii. Certain employees of the bank arousing suspicion

ix. Certain suspicious activities/transactions to be monitored by the branch staff

c. checklist for preventing money laundering activities.

Customer Behaviour Indicators

1. Customers who are reluctant in providing normal information while opening an account, providing minimal or fictitious information or when applying to open an account, providing information that is difficult or expensive for the institution to verify.

2. Customer expressing unusual curiosity about secrecy of information involved in the transaction.

3. Customers who decline to provide information that in normal circumstances would make the customer eligible for banking services.

4. Customer giving confusing details about a transaction.

5. Customer reluctant or refuses to state a purpose of a particular large / complex transaction/ source of funds involved or provides a questionable purpose and / or source.

6. Customers who use separate tellers to conduct cash transaction or foreign exchange transactions.

7. Customers who deposit cash / withdrawals by means of numerous deposit slips / cheques leaves so that the total of each deposits is unremarkable, but the total of all credits / debits is significant.

8. Customer's representatives avoiding contact with the branch.

9. Customers who repay the problem loans unexpectedly.

10. Customers who appear to have accounts with several institutions within the same locality without any apparent logical reason.

11. Customers seeks to change or cancel a transaction after the customer is informed of currency transaction reporting/ information verification or record keeping requirements relevant to the transaction.

12. Customer regularly issues large value cheques without balance and then deposits cash.

An Indicative List of Suspicious Activities

Transactions Involving Large Amounts of Cash

1. Exchanging an unusually large amount of small denomination notes for those of higher denomination;
2. Purchasing or selling of foreign currencies in substantial amounts by cash settlement despite the customer having an account with the bank;
3. Frequent withdrawal of large amounts by means of cheques, including traveller's cheques;
4. Frequent withdrawal of large cash amounts that do not appear to be justified by the customer's business activity;
5. Large cash withdrawals from a previously dormant/inactive account, or from an account which has just received an unexpected large credit from abroad;
6. Company transactions, both deposits and withdrawals, that are denominated by unusually large amounts of cash, rather than by way of debits and credits normally associated with the normal commercial operations of the company, e.g. cheques, letters of credit, bills of exchange etc.
7. Depositing cash by means of numerous credit slips by a customer such that the amount of each deposit is not substantial, but the total of which is substantial.

Transactions that do not make Economic Sense

1. A customer having a large number of accounts with the same bank, with frequent transfers between different accounts;
2. Transactions in which assets are withdrawn immediately after being deposited, unless the customer's business activities furnish a plausible reason for immediate withdrawal.

Activities not consistent with the Customer's Business

1. Corporate accounts where deposits or withdrawals are primarily in cash rather than cheques.

2. Corporate accounts where deposits & withdrawals by cheque/telegraphic transfers/foreign inward remittances/any other means are received from/ made to sources apparently unconnected with the corporate business activity/dealings.

3. Unusual applications for Demand Draft (DD)/ Telegraphic Transfer (TT)/ Pay Order (PO) against cash.

4. Accounts with large volume of credits through Demand Draft (DD)/ Telegraphic Transfer (TT)/ Pay Order (PO) whereas the nature of business does not justify such credits.

5. Retail deposit of many cheques but rare withdrawals for daily operations.

Attempts to avoid Reporting/Record-keeping Requirements

1. A customer who is reluctant to provide information needed for a mandatory report, to have the report filed or to proceed with a transaction after being informed that the report must be filed.

2. Any individual or group that coerces/induces or attempts to coerce/induce a bank employee not to file any reports or any other forms.

3. An account where there are several cash deposits/withdrawals below a specified threshold level to avoid filing of reports that may be necessary in case of transactions above the threshold level, as the customer intentionally splits the transaction into smaller amounts for the purpose of avoiding the threshold limit.

Unusual Activities

1. An account of a customer who does not reside/have office near the branch even though there are bank branches near his residence/office.

2. A customer who often visits the safe deposit area immediately before making cash deposits, especially deposits just under the threshold level.

3. Funds coming from the list of countries/centres, which are known for money laundering.

Customer who provides Insufficient or Suspicious Information

1. A customer/company who is reluctant to provide complete information regarding the purpose of the business, prior banking relationships, officers or directors, or its locations.

2. A customer/company who is reluctant to reveal details about its activities or to provide financial statements.

3. A customer who has no record of past or present employment but makes frequent large transactions.

Certain Suspicious Funds Transfer Activities

1. Sending or receiving frequent or large volumes of remittances to/from countries outside India.

2. Receiving large TT/DD remittances from various centers and remitting the consolidated amount to a different account/center on the same day leaving minimum balance in the account.

3. Maintaining multiple accounts, transferring money among the accounts and using one account as a master account for wire/funds transfer.

Certain Bank Employees arousing Suspicion

1. An employee whose lavish lifestyle cannot be supported by his or her salary.

2. Negligence of employees/willful blindness is reported repeatedly.

Some examples of suspicious activities/transactions to be monitored by the operating staff

1. Large Cash Transactions

2. Multiple accounts under the same name

3. Frequently converting large amounts of currency from small to large denomination notes

4. Placing funds in term Deposits and using them as security for more loans
5. Large deposits immediately followed by wire transfers
6. Sudden surge in activity level
7. Same funds being moved repeatedly among several accounts
8. Multiple deposits of money orders, Banker's cheques, drafts of third parties
9. Multiple deposits of Banker's cheques, demand drafts, cross/ bearer cheques of third parties into the account followed by immediate cash withdrawals
10. Transactions inconsistent with the purpose of the account
11. Maintaining a low or overdrawn balance with high activity

Check list for preventing money-laundering activities:

1. A customer maintains multiple accounts, transfer money among the accounts and uses one account as a master account from which wire/ funds transfer originates or into which wire/funds transfer are received (a customer deposits funds in several accounts, usually in amounts below a specified threshold and the funds are then consolidated into one master account and wired outside the country).

2. A customer regularly depositing or withdrawing large amounts by a wire transfer to, from, or through countries that are known sources of narcotics or where Bank secrecy laws facilitate laundering money.

3. A customer sends and receives wire transfers (from financial haven countries) particularly if there is no apparent business reason for such transfers and is not consistent with the customer's business or history.

4. A customer receiving many small incoming wire transfer of funds or deposits of cheques and money orders, then orders large outgoing wire transfers to another city or country.

5. A customer experiences increased wire activity when previously there has been no regular wire activity.

6. Loan proceeds unexpectedly are wired or mailed to an offshore Bank or third party.

7. A business customer uses or evidences or sudden increase in wire transfer to send and receive large amounts of money, internationally and/or domestically and such transfers are not consistent with the customer's history.

8. Deposits of currency or monetary instruments into the account of a domestic trade or business, which in turn are quickly wire transferred abroad or moved among other accounts for no particular business purpose.

9. Sending or receiving frequent or large volumes of wire transfers to and from offshore institutions.

10. Instructing the Bank to transfer funds abroad and to expect an equal incoming wire transfer from other sources.

11. Wiring cash or proceeds of a cash deposit to another country without changing the form of the currency.

12. Receiving wire transfers and immediately purchasing monetary instruments prepared for payment to a third party.

13. Periodic wire transfers from a person's account/s to Bank haven countries.

14. A customer pays for a large (international or domestic) wire transfers using multiple monetary instruments drawn on several financial institutions.

15. A customer or a non-customer receives incoming or makes outgoing wire transfers involving currency amounts just below a specified threshold, or that involve numerous Bank or travelers cheques

16. A customer or a non customer receives incoming wire transfers from the Bank to 'Pay upon proper identification' or to convert the funds to bankers' cheques and mail them to the customer or non-customer, when

    a. The amount is very large (say over Rs.10 lakhs)

    b. The amount is just under a specified threshold (say just below Rs. 10 Lakh)

    c. The funds come from a foreign country or

    d. Such transactions occur repeatedly.

17. A customer or a non-customer arranges large wire transfers out of the country which are paid for by multiple Bankers' cheques (just under a specified threshold)

18. A Non-customer sends numerous wire transfers using currency amounts just below a specified threshold limit.

Grounds of suspicion reported in STRs(Extracted from the Annual Report of Financial Intelligence Unit -India (FIU-IND))

No.	Suspicion	Summary of detection and review
1	False Identity	Identification documents were found to be forged during customer verification process. The account holder was not traceable
2	Wrong Address	Welcome pack was received back as the person was not staying at the given address or address details given by the account holder were found to be false. The account holder was not traceable
3	Doubt over the real beneficiary account.	The customer not aware of transactions in the account. Transactions were inconsistent with of the account customer's profile.
4	Account of persons under investigation	The customer was reported in media for being under investigation.
5	Account of wanted criminal	Name of the account holder and additional criteria (Date of birth / Father's name / Nationality) were same as a person on the watch list of UN, Interpol etc.

6	Account used for cyber crime	Complaints of cyber crime were received against a customer. No valid explanation for the transactions by account holder.
7	Account used for lottery fraud	Complaints were received against a bank account used for receiving money from the victims. Deposits at multiple locations followed by immediate cash withdrawals using ATMs. No valid explanation provided by the account holder.
8	Doubtful activity of a customer from high risk country	Cash deposited in a bank account at different cities on the same day. The account holder a citizen of a high risk country with known cases of drug trafficking.
9	Doubtful investment in IPO	Large number of accounts involving common introducer or authorized signatory. Accounts used for multiple investments in IPOs of various companies.
10	Unexplained transfers between multiple accounts	Large number of related accounts with substantial inter-account transactions without any economic rationale.
11	Unexplained activity in dormant accounts	Sudden spurt in activity of dormant account. The customer could not provide satisfactory explanation for the transactions.
12	Unexplained activity in account inconsistent with the declared business	Transactions in account inconsistent with what would be expected from declared business. The customer could not provide satisfactory explanation.
13	Unexplained large value transactions inconsistent with client's apparent financial standing	Large value transactions in an account which usually has small value transactions. No valid explanation provided by the account holder.
14	Doubtful source of payment for credit card purchases	Credit card topped up by substantial cash first and then used for incurring expenses. Cumulative payment during the year was beyond known sources of income.
15	Suspicious use of ATM card	Frequent cash deposits in the account followed by ATM withdrawals at different locations. No valid explanation.
16	Doubtful use of safe	Safe deposit locker operated frequently though

	deposit locker	the financial status of client
17	Doubtful source of cash deposited in bank account	Frequent cash transactions of value just under the reporting threshold. Cash transactions split across accounts to avoid reporting. No valid explanation provided.
18	Suspicious cash withdrawals from bank account	Large value cheques deposited followed by immediate cash withdrawals.
19	Doubtful source of foreign inward transfers in bank account	Deposit of series of demand drafts purchased from Exchange House abroad. Sudden deposits in dormant account immediately followed by withdrawals.
20	Doubtful remitter of foreign remittances	Name and other details of the remitter matches with a person on watch list.
21	Doubtful beneficiary of foreign remittances	Name and other details of the beneficiary matches with a person on watch list.
22	Doubtful utilizations of foreign remittances	Foreign remittance being withdrawn in cash immediately. No valid explanation.
23	Misappropriation of funds	Reports of misappropriation of funds. Substantial cash withdrawals in account of a charitable organization.
24	Doubtful source of insurance	Substantial premium paid by cash/demand draft in premium multiple insurance policies without valid explanation. Substantial premium paid by multiple demand drafts of amounts below Rs.50,000/-. Insurance premium much beyond declared sources of income.
25	Doubtful source of loan foreclosure	Substantial amount paid in cash / demand draft for foreclosure of loan account. No valid explanation provided.
26	Doubtful source of the inward foreign	Inward foreign remittance received from a non relative. No valid explanation provided

	remittances	by the beneficiary.
27	Suspicious inward foreign remittances	Splitting of inward foreign remittances to collect funds in cash in an apparent attempt to avoid fund trail
28	Doubtful beneficiary of foreign remittances	Doubtful credentials of the beneficiary. No valid explanation for the remittance provided.
29	Doubtful purchase of foreign exchange by a customer	Substantial foreign exchange purchased in cash or demand draft. No valid explanation provided.
30	Doubtful sale of foreign exchange	Substantial foreign exchange sold without any valid explanation.

FOREIGN ACCOUNT TAX COMPLIANCE ACT (FATCA) AND COMMON REPORTING STANDARDS (CRS)

As per the inter-Government agreement with USA for improving the International Tax Compliance and implementing the Foreign Account Tax Compliance Act (FATCA), every eligible Bank has to report the transactions of applicable accounts to Income Tax Department through e-filing portal. Our Bank is defined under "a financial Institution with a Local Client base", so we are exempted from the maintenance and reporting of the information under the said agreement.

Staff Awareness and Training to Staff

With a view to equip staff members with an intention to have the system of prevention and detection of money laundering in place as also to make them alert to the risks of money laundering and terrorist financing, training is considered utmost essential. The training shall also be imparted as to how to

recognize risks associated with remittances for facilitating money laundering and terrorist financing.

Induction training on the subjects of prevention of money laundering, recognizing suspicious transactions, Know Your Customer (KYC) requirements, etc. shall be imparted.

Ongoing training shall be ensured at appropriate intervals to keep the staff members abreast of latest developments on the subject. The Bank's policy on the subject shall also be explained. Further, the staff members shall be made aware of the requirements contained in Prevention of Money Laundering (PML) Act and Rules and Regulations framed there under, besides Reserve Bank of India guidelines on the subject. The responsibilities and accountability shall also be the part of the syllabus for the training. Similarly, preservation of record and all other relevant aspects shall be explained during such training programmes.

Customer Awareness

The Branches should explain to the customers to see Know Your Customer (KYC) checks as a sensible contribution to the fight against crime and terrorism. The customer awareness can be created by following measures:

a. incorporating the requirements in the account opening forms,

b. Branch staff should address to customer queries,

c. requirements under Know Your Customer (KYC) shall be displayed on the notice boards of the branches,

d. bank's web site should also furnish the details about Anti Money Laundering (AML), Know Your Customer (KYC), Prevention of Money Laundering Act (PMLA), etc.

Maintenance of records of transactions

Branches should maintained proper record of transactions, as mentioned below:

(i) All cash transactions of the value of more than Rupees Ten Lakh or its equivalent in foreign currency;

(ii) Series of all cash transactions individually valued below Rupees Ten Lakh, or its equivalent in foreign currency which are that have taken place within a month and the monthly aggregate which exceeds rupees ten lakhs or its equivalent in foreign currency. It is clarified that for determining 'integrally connected transactions' 'all accounts of the same customer' should be taken into account.

(iii) All transactions involving receipts by non-profit organisations of value more than rupees ten lakh or its equivalent in foreign currency.

(iv) All cash transactions where forged or counterfeit currency notes or bank notes have been used as genuine and where any forgery of a valuable security or a document has taken place facilitating the transaction and

(v) All suspicious transactions, whether or not in cash, made as mentioned in the Rules.

Branches should maintain all necessary information in respect of transactions, including the following information:

(i) the nature of the transactions;

(ii) the amount of the transaction and the currency in which it was denominated;

(iii) the date on which the transaction was conducted; and

(iv) the parties to the transaction.

Preservation of Records

Record keeping enables the bank to demonstrate that it has operated in conformity with the rules and regulations. This would also facilitate the bank and the individual staff members to defend themselves against any allegations. The records also enable the bank to have the complete picture of the financial profile of the suspect account.

The records also facilitate in identifying the beneficial owner of the account, volume of funds transacted in the account, origin of funds, nature of transactions, currency in which the transaction has taken place, whether funds were withdrawn in cash, the destination of funds, etc.

Branches should note the period of preservation of records as under:

a. All the identification documents are required to be preserved for a period of 10 years from the date of closure of the account.

b. All the vouchers are required to be preserved for a period of 10 years from the date of transaction.

c. Any report (CCR, STR, CTR, etc.) made to FIU-IND should be preserved for a period of 10 years.

d. In case the matter of suspicious transaction is pending in the Court of Law, records should be preserved for a period of 10 years from the date of final verdict of the Court.

Designated Director*:*

Bank will nominate a Director on their Board as "designated Director", as required under provisions of the Prevention of Money Laundering (Maintenance of Records) Rules, 2005 (Rules), to ensure compliance with the obligations under the Act and Rules. The name, designation and address of the Designated Director will be communicated to the FIU-IND. Bank will designate a person who holds the position of senior management or equivalent as a 'Designated Director'. However, in no case, the Principal Officer should be nominated as the 'Designated Director'.

Principal Officer:

Bank will appoint a senior officer as Principal Officer (PO). The Principal Officer (PO) will be independent and report directly to the senior management or to the Board of Directors. The Principal Officer (PO) will be responsible for ensuring compliance, monitoring transactions, and sharing

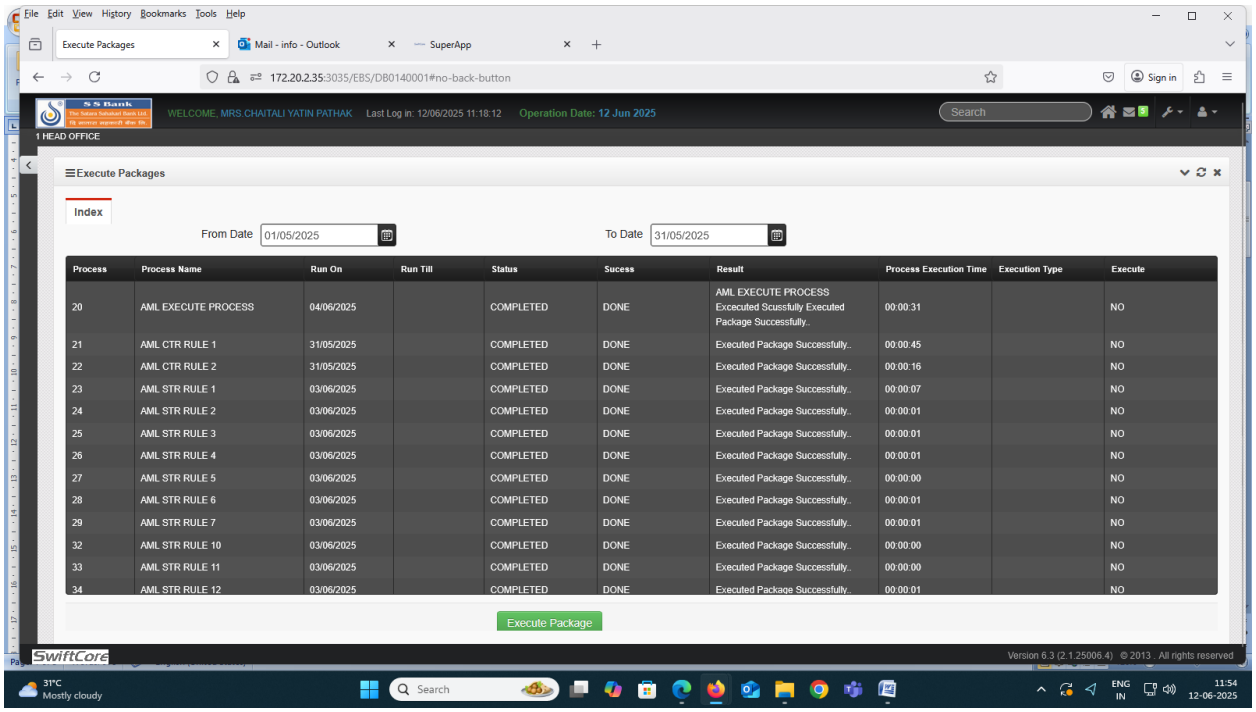
and reporting information as required under the law/regulations. The name, designation and address of the Principal Officer will be communicated to the Financial Intelligence Unit - India (FIU-IND).

Procedure for AML REPORT FILE GENERATION (CTR / NTR/ STR/CCR)

DATA EXTRACTION AND CASE GENERATION

Execute package :

Use AML Execute package with search option (screen attached) and Run below processes one by one (use reporting month's 1 st date as "From date" and last date as "To date")



Process 1 – AML LIVE TO LANDING

Process 2 – AML LANDING TO MART

Process 3 – AML CUMMULATIVE TURNOVER

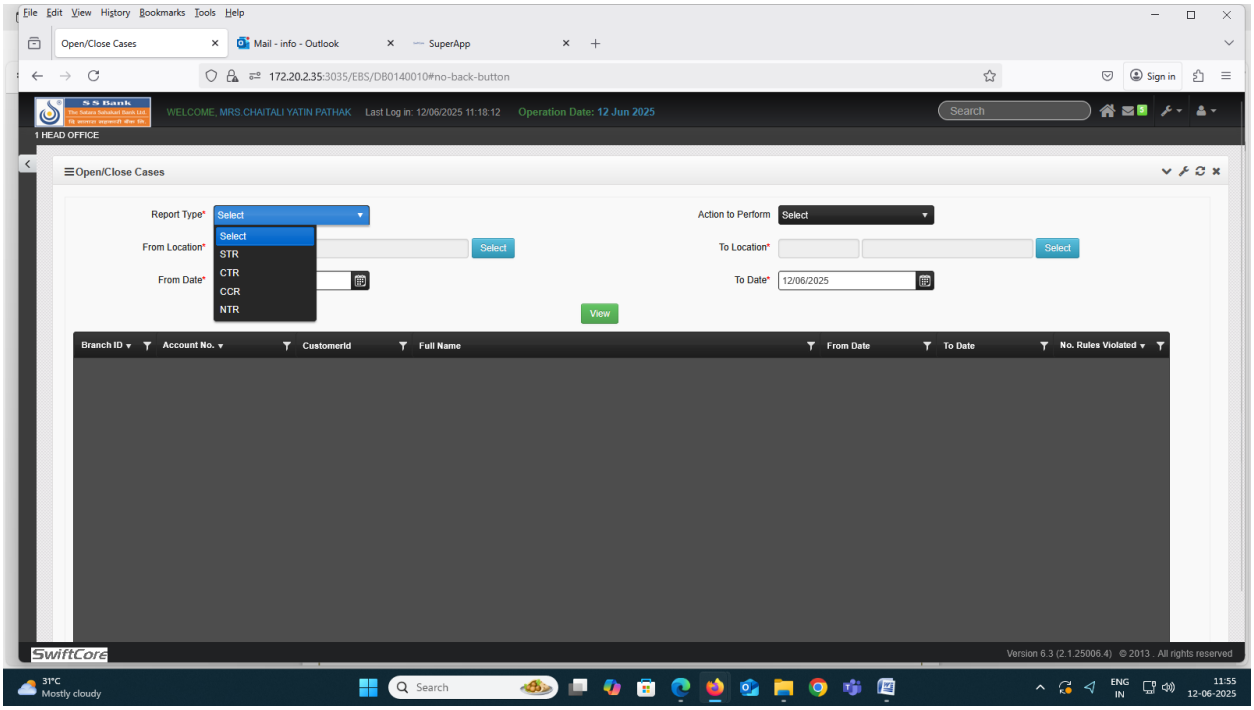
Process 4 – AML CUBE PROCESS

After completion of above processes you will start rule execution for CTR , NTR and STR, before rule execution please check and Close all pending cases if any with "AML

OPEN/CLOSE CASES" or "CLOSE/OPEN CASES" option in search menu (screen attached below) for each report.

Close Cases:-

- Select report type
- Action to perform – closed
- From Location as –select 1 st branch
- To location – select last branch
- From date and to date – last reported month dates



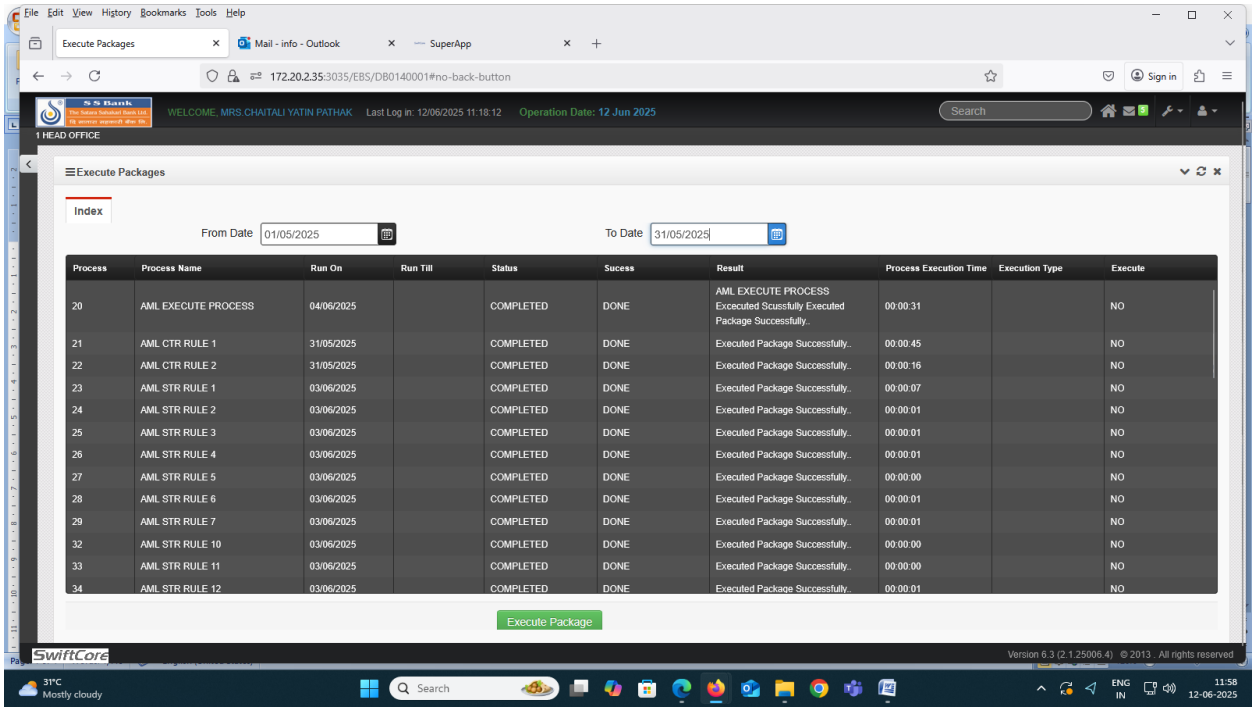
Click on "View" button which showing previous cases, after that click on "Process" button to close all cases which available on bottom of the page.

Rule Execution :

RULE Execution FOR CTR / STR / NTR –

AML Rules are listed under AML Execute package search menu option for each AML report type i.e. CTR /STR/NTR which are easily recognizable with Process Name. For

execution of rule set “From Date” and “To Date” as per rule’s frequency (i.e. Daily or Monthly) and select “YES” in EXECUTE column for that rule and click on “Execute package” button available in the bottom of screen. Execute each AML rule one by one and wait till completion, Result Column available in screen which shows that the Rule successfully processed or not. In case of any error in Result column, execute failed rule again with date set.

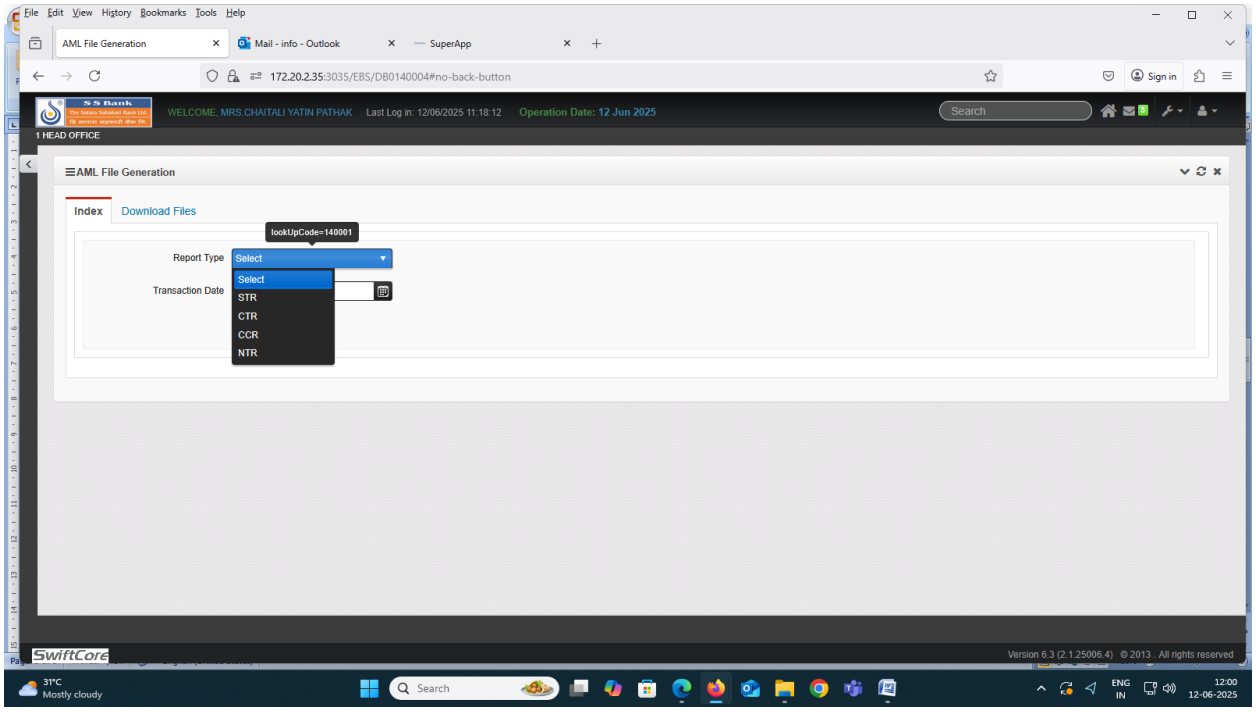


Process	Process Name	Run On	Run Till	Status	Sucess	Result	Process Execution Time	Execution Type	Execute
20	AML EXECUTE PROCESS	04/06/2025		COMPLETED	DONE	AML EXECUTE PROCESS Excecuted Scussfully Executed Package Successfully..	00:00:31		NO
21	AML CTR RULE 1	31/05/2025		COMPLETED	DONE	Executed Package Successfully..	00:00:45		NO
22	AML CTR RULE 2	31/05/2025		COMPLETED	DONE	Executed Package Successfully..	00:00:16		NO
23	AML STR RULE 1	03/06/2025		COMPLETED	DONE	Executed Package Successfully..	00:00:07		NO
24	AML STR RULE 2	03/06/2025		COMPLETED	DONE	Executed Package Successfully..	00:00:01		NO
25	AML STR RULE 3	03/06/2025		COMPLETED	DONE	Executed Package Successfully..	00:00:01		NO
26	AML STR RULE 4	03/06/2025		COMPLETED	DONE	Executed Package Successfully..	00:00:01		NO
27	AML STR RULE 5	03/06/2025		COMPLETED	DONE	Executed Package Successfully..	00:00:00		NO
28	AML STR RULE 6	03/06/2025		COMPLETED	DONE	Executed Package Successfully..	00:00:01		NO
29	AML STR RULE 7	03/06/2025		COMPLETED	DONE	Executed Package Successfully..	00:00:01		NO
32	AML STR RULE 10	03/06/2025		COMPLETED	DONE	Executed Package Successfully..	00:00:00		NO
33	AML STR RULE 11	03/06/2025		COMPLETED	DONE	Executed Package Successfully..	00:00:00		NO
34	AML STR RULE 12	03/06/2025		COMPLETED	DONE	Executed Package Successfully..	00:00:01		NO

AML REPORT FILE GENERATION (CTR / NTR/ STR/CCR) File Generation

Method of the file generation is same for each AML report, which steps given below.

Type “AML File Generation” in search option



Select AML Report type and month end date of reporting month and click on Submit button. Now system will check if all previous processes i.e. Data Extraction and Related Rules Execution have been executed successfully for the given month. If not then a message “DATA is not available for report” will pop-up and system will not allow any further processing. (Sample message screen given below)

The “Submit” button will be replaced by “Generate File” button (screens attached below)

After Click on “Generate File” system will check whether ARF Invalid Data process has finished. No further processing will be allowed until the process has finished and system will show warning message till then.

Once ARF Invalid Data process has finished, again click on “Generate File” system will check for any invalid data in violated records and will show below messages. Invalid Data found: If system found any invalid data in violated records, will show below message.

User should clear all invalid data from respective customers / accounts which showing in ARF Invalid

Data report under AML reports of ANY DAY REPORTS search menu option.

No Invalid Data: In case there is no invalid data, confirmation box will showing to generate Report files.

After clicking "YES" button system enquired the ARF File Generation process.

Once the ARF File Generation process is finished, the files will be available for download in the Download Files tab.

SUSPECIOUS TRANSACTION WORKFLOW (STR)

AML STR Work-flow

STR or Suspicious Transaction Report can be generated only if the violated accounts are manually escalated and approved. AML STR work-flow defines the various actors and their roles. Work flow Stages: Defines the various stages an account has to pass through before being approved. Current default in AML is 3 stages which can be changed at the time of implementation as per Bank's requirements.

A. Stage 1: Branch Officer (BO)

B. Stage 2: Branch Manager (BM)

C. Stage 3: Senior Manager (SM)

STR Account Life-cycle: An account can be in any one of the following status during its life-cycle

A. Pending: Account which is awaiting action by either one of BO,BM or SM.

B. Action Taken: Account which has been processed by the Stage actor.

C. Approved: Account which has been approved by MLRO and will be included in STR file.

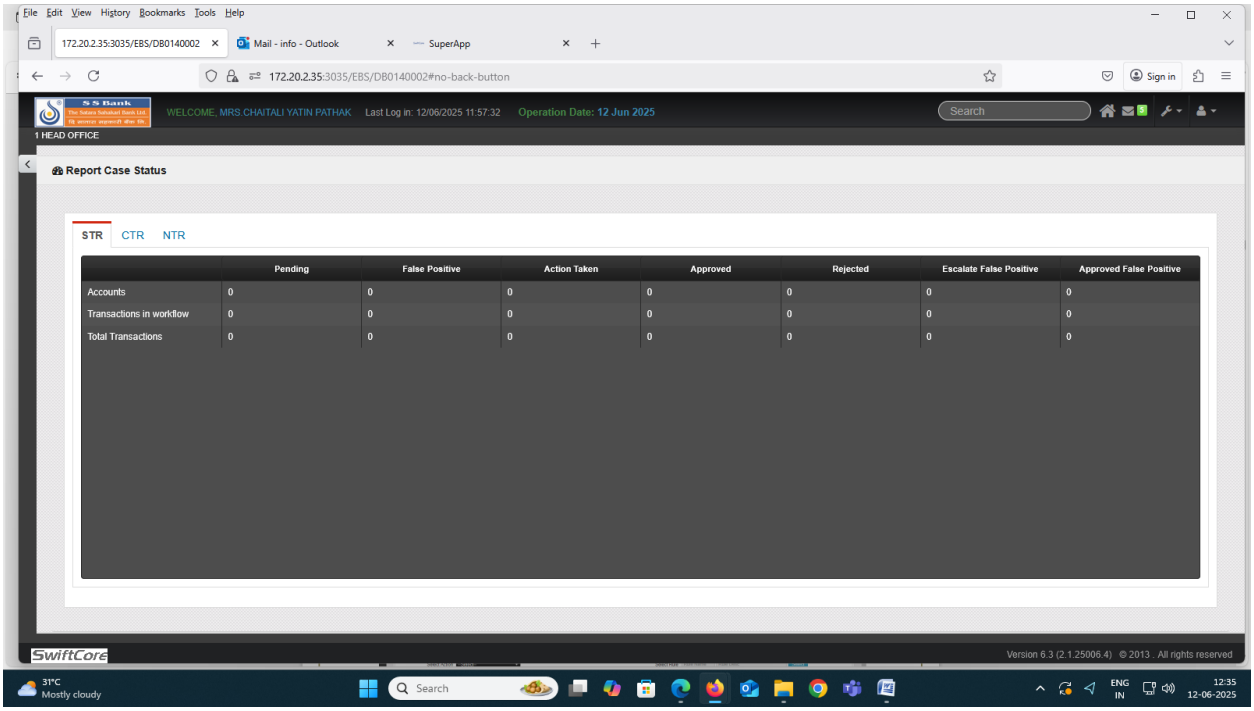
D. Rejected: Account whose escalation/false positive was rejected by higher stage actor e.g. BM escalated an account but it was rejected by SM.

E. False Positive: Account which has been marked False Positive and will not be reported

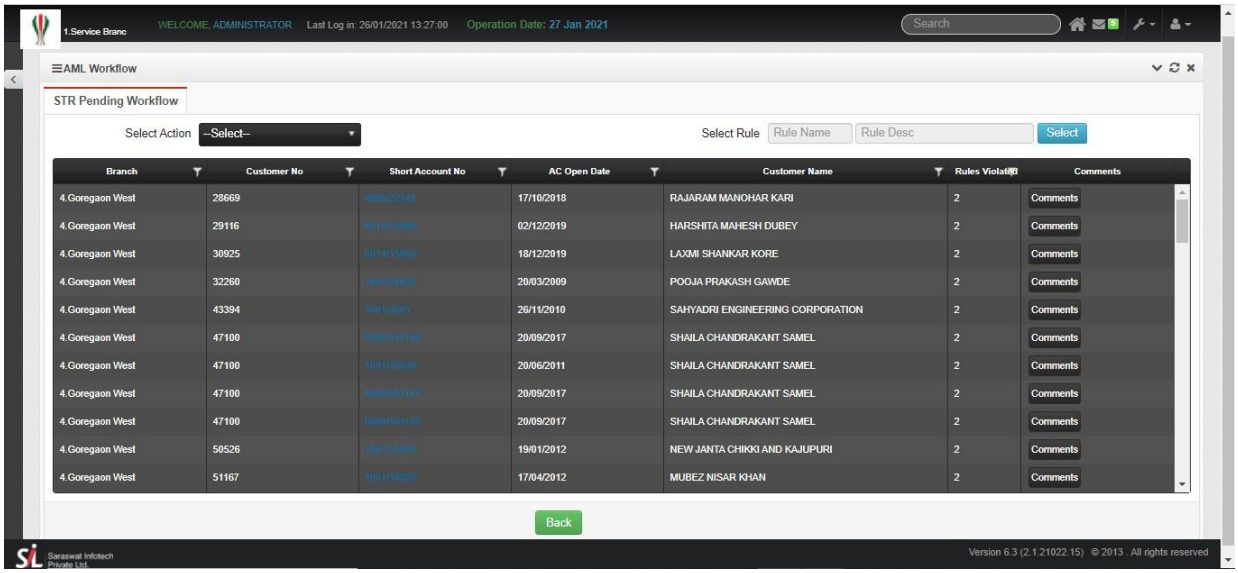
Stage 1:Branch Officer

1. An STR Account starts at first stage with Branch Manager. If all respective STR Rules has executed successfully through Rule execution AML Execute Package

screen the a Branch Manager can view all the STR accounts that belong to his/her branch through Menu ->AML- >Report Case Status



2. All newly generated account cases have Pending status. The cell values are links which, on clicking, take the user to relevant screen. On clicking the given cell value of Pending Accounts user is taken to the AML Workflow screen.



3. AML Workflow screen displays all the accounts for which STR have been generated along with the no. of STR rules violated. The Select Action dropdown lists all the valid actions that can be performed on the pending accounts by branch manager which are Escalate and False Positive.

4. False Positive flow: BO can mark all those accounts which he deems to be not suspicious as False Positive. These accounts will then not be included in file generation. The process to mark accounts as False Positive is as follows: a. Select False Positive in Select Action dropdown. New columns Reason, Reason Desc and Set False Positive will be displayed in the grid. b. Select the reason for which BM is marking the account as False Positive in the Reason dropdown. Next mark Set False Positive as YES. Do this activity for all eligible accounts in the grid and click Submit. All accounts will be moved to False Positive status

Escalate flow: All accounts which are acknowledged as suspicious by BM have to be escalated to next stage. The process for escalating is as follows:

a. Select Escalate in the Select Action dropdown.
b. Click on Comments button of the account which is to be escalated. This will open a popup screen Comment Details which has two tabs: Comment Details and Existing Comments. c. The grid in Comment Details tab shows all the violated cases and their status. BM can decide which cases are to be included in the file and mark those as YES in “Send To FIU” dropdown. The transactions of selected cases will be included in STR files and those of rejected cases will be excluded. BM also has to provide details regarding the nature of escalation. These details are in the Other Details section and will be included in the STR file
c. Once all details have been filled, BM navigates to Existing comment tab and clicks Submit button. This escalates the selected account to next stage where it can be viewed by MLO.
d. Going back to the Menu ◊ AML ◊ Report Cases screen, we have 4 more statuses viz. Action Taken, Approved, Rejected and False Positive. BM does not have rights to take any action on these accounts. He can only view the accounts and their details.

Stage 2 :Money laundering Branch Manager Stage

1. MLBM can view all STR accounts for which action has been taken by the BOs. The screen is same as that of BO and can be accessed through Menu ◊ AML ◊ Report Cases.

2. All accounts that have been escalated by respective BOs are aggregated in the Pending column. The cell values are links which, on clicking, take the user to relevant screen. On clicking the cell value '5' of Pending Accounts user is taken to the AML Workflow screen. An MLBM has access to accounts of BOs that belong to same Branches.
3. AML Workflow screen displays all the accounts that have been escalated by the BMs. The Select Action dropdown lists all the valid actions that can be performed on the pending accounts by MLO which are Escalate and Reject.
4. Reject flow: MLBM can send escalated accounts back to BO for reconsideration. The process to mark accounts as Rejected is as follows:
   a. Select Rejected in Select Action dropdown. Two new columns Reason and Set Reject will be displayed in the grid.
   b. b. Select the reason for which MLO is marking the account as Rejected in the Reason dropdown. Next mark Reject as YES. Do this activity for all eligible accounts in the grid and click Submit. All accounts will be moved to Rejected status.
5. Escalate flow: All accounts which are acknowledged as suspicious by MLBM have to be

   Escalated to next stage. The process for escalating is as follows:
   a. Select Escalate in the Select Action dropdown.
   b. Click on Comments button of the account which is to be escalated. This will open a pop-up screen Comment Details which has two tabs: Comment Details and Existing Comments.
   c. The grid in Comment Details tab shows all the violated cases and their status as marked by BM. MLO can either go with the BM's selection or he/she can make changes to the selected cases. The screen-shot below shows that all cases were marked to be sent to FIU by BM. MLO can exclude any cases from it or send all cases as is to MLBM.
   d. The Other Details section has escalation details required for file generation. These details have already been filled by BM. However MLO can modify any of these fields as he/she sees fit. The only field unique to MLO is Select Comment in the Additional Comments (Only for bank reference) section.
   e. Once all details have been filled, MLBO navigates to Existing Comment tab and clicks Submit button. This escalates the selected account to next stage where it can be viewed by MLBM. The Existing Comment grid shows all the comments tagged to the account along with User and comment date. In the screen shot below BM user had marked the account as suspicious on date.
6. Going back to the Menu ◊ AML ◊ Report Cases screen, we have 4 more statuses viz. Action taken, Approved, Rejected and False Positive. MLO does not have

rights to take any action on the Action Taken and Approved accounts. He can only view these accounts and their details. However for Rejected and False Positive accounts he is allowed to revert them. The flow for each is in the following steps.

7. Revert Back Rejected Account flow:
   a. MLBM clicks on the cell value of Rejected Account column. He/she is taken to the AML Workflow screen for STR Rejected.
   b. Select Revert Back in Select Action dropdown. Two new columns Reason and Revert will be displayed in the grid.
   c. Select the reason for which MLO is reverting back the account in the Reason dropdown. Next mark Revert as YES. Do this activity for all eligible accounts in the grid and click Submit. All accounts will be reverted to their previous status.
8. Revert False Positive Account flow:
   a. MLBO clicks on the cell value of False Positive Account column. He/she is taken to the AML Workflow screen for STR False Positive.
   b. Select Revert False Positive in Select Action dropdown. Two new columns Reason and Revert FP will be displayed in the grid.
   c. Select the reason for which MLO is reverting back the account in the Reason dropdown. Next mark Revert FP as YES. Do this activity for all eligible accounts in the grid and click Submit. All accounts will be reverted to their previous status.

Stage 3: Money Laundering Reporting Officer

1. MLRO can view all STR accounts for which action has been taken by the MLOs. The screen is same as that of MLO and can be accessed through Menu ◊ AML ◊ Report Cases.
2. All accounts that have been escalated by respective MLOs are aggregated in the Pending column. The cell values are links which, on clicking, take the user to relevant screen. On clicking the cell value '1' of Pending Accounts user is taken to the AM Workflow screen. MLRO has bank-level access and can view accounts of all MLOs irrespective of branch or zone.
3. AML Workflow screen displays all the accounts that have been escalated by the MLOs. The Select Action dropdown lists all the valid actions that can be performed on the pending accounts by MLRO which are Approve and Rejected.

4. Reject flow: MLRO can send escalated accounts back to MLO for reconsideration. The process to mark accounts as Rejected is as follows:

a. Select Rejected in Select Action dropdown. Two new columns Reason and Set Reject will be displayed in the grid.

b. Select the reason for which MLRO is marking the account as Rejected in the Reason dropdown. Next mark Reject as YES. Do this activity for all eligible accounts in the grid and click Submit. All accounts will be moved to Rejected status.

5. Approve flow: All accounts which are acknowledged as suspicious by MLRO and adjudged to be included in STR file have to be approved. The process for approving is as follows:

a. Select Approve in the Select Action dropdown. Two new columns Reason and Set Reject will be displayed in the grid.

b. Select the reason for which MLRO is marking the account as approved in the Reason dropdown. Next mark Approve as YES. Do this activity for all eligible accounts in the grid and click Submit. All accounts will be approved and included in the STR file when it is generated.

6. Going back to the Menu ◊ AML ◊ Report Cases screen, we have 4 more statuses viz. Action Taken, Approved, Rejected and False Positive. MLRO cannot take any action on the Action Taken accounts. He can only view these accounts and their details. However for Approved, Rejected and False Positive accounts he is allowed to revert them. The flow for each is in the following steps.

7. Revert Back Approved Account Flow:

a. MLRO clicks on the cell value of Approved Account column. He/she is taken to the AML

Work flow screen for STR Approved.

b. Select Reject Approved in Select Action dropdown. Two new columns Reason and Reject Approved will be displayed in the grid.

c. Select the reason for which MLRO is reverting back the approved account in the Reason dropdown. Next mark Reject Approved as YES. Do this activity for all eligible accounts in the grid and click Submit. All accounts will be reverted to their previous status

8. Revert Back Rejected Account flow:

a. MLRO clicks on the cell value of Rejected Account column. He/she is taken to the AML Workflow screen for STR Rejected.

b. Select Revert Back in Select Action dropdown. Two new columns Reason and Revert will be displayed in the grid.

c. Select the reason for which MLRO is reverting back the account in the Reason dropdown. Next mark Revert as YES. Do this activity for all eligible accounts in the grid and click Submit. All accounts will be reverted to their previous status.

9. Revert False Positive Account flow:

a. MLO clicks on the cell value of False Positive Account column. He/she is taken to the AML Workflow screen for STR False Positive.

b. Select Revert False Positive in Select Action dropdown. Two new columns Reason and Revert FP will be displayed in the grid.

c. Select the reason for which MLRO is reverting back the account in the Reason dropdown. Next mark Revert FP as YES. Do this activity for all eligible accounts in the grid and click Submit. All accounts will be reverted to their previous status

LIST OF STR/CTR/NTR RULES

STR Rule1	Corporate customer's turnover>Rs500000.00 and quarterly credit flows in the account is > 50% of the turnover.
STR Rule2	Cash deposits>=Rs500000.00 in a month.
STR Rule3	Total cash deposits during the month is > = Rs500000.00 and > = 50% of the average cash deposits for the last 3 months.
STR Rule4	Transactions of a customer for which total monthly debit is >Rs500000.00 and cash debitis >=50% of total monthly debit
STR Rule5	Transactions of a customer for which total monthly credit>Rs500000.00 and cash creditis >=50% of total monthly credit
STR Rule6	Credit transactions of a customer for which total number of credit transactions >25 credit transactions per day
STR Rule7	Large Transaction Exceeding Rs2000000.00

STR Rule8	Transactions in inoperative or dormant accounts
STR Rule9	High cash transactions in new accounts (2Lac&above) in last six months
STR Rule9.1	High cash transactions in new accounts (2Lac&above) in last six months for SB having limit >=200000
STR Rule9.2	High cash transactions in new accounts(2Lac&above) in last six months for CD having limit >=500000
STR Rule10	Rapid movement of funds
STR Rule11	Debit transactions just under there porting threshold amount(Rs1000000.00) to avoid reporting
STR Rule12	Credit transactions just under there porting threshold amount(Rs1000000.00) to avoid reporting
STR Rule14	Turn over in month>last quarter average balance
STR Rule15	Credits>500000 in month
STR Rule16	Top 10 Cash Transactions>=Rs.500000
STR Rule17	Top 10 Credit Transaction>= 500000
STR Rule18	All transactions of OF AC list customers
STR Rule19	Single Credit Transaction exceeding Rs25Lac in Current Account
STR Rule20	Total Deposit in Current Account>=Rs 1Cr during the month
STR Rule21	Total Cash Depositor Withdrawal in Current Account>=Rs25 Lac during the month
STR Rule22	Single Cash Debitor Credit Transaction exceeding Rs5 Lac in Current Account
STR Rule23	No.of Cash Transactions > 20 during the month for Current account
STR Rule24	Dishonor of deposited cheques in CA exceeding 10 times during the month
STR Rule25	Dishonor of issued cheques for CA exceeding 2 times during the

	month
STR Rule27	No.ofTransactions>50duringthemonthforSavingaccount
STR Rule28	Total Deposit in Saving Account >Rs 25Lac during the month
STR Rule29	Total Cash Depositor Withdrawal in Saving Account>=Rs10 Lac during the month
STR Rule30	Single Debitor Credit Transaction exceeding Rs5Lac in SavingAccount
STR Rule31	Dishonor of deposited cheques in Saving account exceeding 5 times during the month
Manual STR	Manually Escalation of Transaction
Daily STR 1	JEWELLER ACCOUNT
Daily STR 2	STAFF ACCOUNT
Daily STR 3	CASH DEPOSIT BY MULTIPLE SLIPS
Daily STR 4	PEP CUSTOMER
Daily STR 5	HIGH KYC RATING CUSTOMER
Daily STR 6	CASH TRANSACTION OVER 2 LAC IN NPO
CTR Rule1	Total Debit Cash Transactions >Rs.10,00,000/-during the month.
CTR Rule2	Total Credit Cash Transactions>Rs.10,00,000/-during the month.
NPO Rule1	For non-profit organizations, Society & Trust (Omni Acct Types:5&13)single txn>= 10,00,000 during the reporting month to be identified.

*Note: 1) Branch Officer is Maker who creates or submits a record or transaction.
2) Branch Manager reviews and approves or rejects the records.
3) After completion process of Branch Level, in HO Level IT Manager Approve or rejects the records.
4) Cash Transaction Report (CTR) should be uploaded to the FINGate portal by the 15th of the following month.: Principal Officer and Alternate

Principal Officer upload the data in Fin gate 2.0.

Conclusion:

The policy of the Bank as given above is quite exhaustive and all the staff members are required to follow these guidelines meticulously while functioning at the Branch level. It is in the national interest to prevent such money laundering transactions. It is also national duty to report to Financial Intelligence Unit - India (FIU-IND) such transactions when they come across any.

Review of the Policy:

Yhe policy will be effective from the date of approval and it will continue to be in force till it is amended / midified.

Asst.General Manager **Chief Executive Officer**

Approved:
Board Resolution No.- 23
B.O.D. Meeting dated.- 30.06.2025