COMMERCIALCREDITAND

FINANCEPLC

PROCEDURE ON ANTI MONEY LAUNDERING, TERRORIST FINANCING AND FINANCING OF WEAPONS OF MASS DESTRUCTION

(This replaces all previous documents covering the operating metrics of the procedure on Anti-Money Laundering and Countering the Financing of Terrorism)

TABLE OF CONTENT

1. INTRODUCTION

1.1. The Financial Intelligence Unit of Sri Lanka (FIU) is vested with powers to combat Money Laundering (ML), Terrorist Financing (TF) , Proliferation Financing (PF) and related crimes in Sri Lanka in line with international standards and best practices in the industry. The FIU has issued Customer Due Diligence Rules applicable to institutions engaged in the "Finance Business" which include Non-Bank Financial Institutions such as Commercial Credit and Finance PLC.

1.2. The Rules require that every Financial Institution should identify and analyse and design effective implementation of policies and procedures to mitigate identified risks related to ML/TF/PF. This procedure has been prepared to guide operational staff in key procedures enacted in the Company's overall approach towards complying with AML & CFT rules and regulations in Sri Lanka.

2. VERSION CONTROL

This procedure will be reviewed once every Three (3) financial years or in the event of any changes in the regulatory or environmental requirements. The updates will be recorded in the "Version Control" with details of revisions and effective dates.

Version Code	Release Date	Prepared by
1.0	October 2018	Compliance Officer
2.0	December 2021	Compliance Officer
3.0	September 2024	Compliance Officer

3. OBJECTIVES

3.1 To ensure that the customers are adequately evaluated to identify risk of ML ,TF and PF, and, in addition, identification of PEPs, with the overall aim of mitigating identified ML & TF risks based on policies and procedures developed by the Company that are in line with FIU requirements and regulations.

3.2 To provide guidelines in carrying out AML/CFT/PF procedures to comply with FIU regulations and guidelines.

4. RESPONSIBILITY

4.1 All staff are responsible for the combating of ML,TF and PF activities in the institution.

4.2 The Executive Management , Location Heads, Product Head and Operation Heads, Customer Relationship Officers and Marketing Officers (Operational Staff) are particularly responsible for effective operation of this procedure.

4.3 AML Compliance officer is responsible to ensure the overall functioning of these procedures.

5. DEFINITIONS

5.1 AML Coordinator

The designated officer in the Branch who is mainly responsible for ensuring the compliance with AML / CTF/PF requirements. Presently all Location Head / Location in Charge are designated as the AML coordinator. This is included in the Location head Job Description

5.2 Customer

A customer for the purpose of these guidelines is defined as any of the following persons who enter into a business relationship with the Company:

i. A person or an entity, maintaining an account with the company and/or partakes in business relationships with the company.

ii. Person on whose behalf the account is maintained [i.e. the beneficial owner]

iii. Signatory and Beneficiaries of transactions conducted by professional intermediaries, (e.g. stock brokers, chartered accountants, solicitors etc. as permitted under the law.)

iv. Any person or entity connected with a financial transaction of the company

6. AML/CFT/PF PROCESS

6.1 On boarding

a) CCFP should obtain the customer information and evaluate the customer risk at the time of on boarding a customer as required by the regulator. This includes,

I. Completion of product application forms, KYC forms

II. Carrying out initial Due Diligence on customers,

1. Verification of documents provided by the customer
2. Verification of information provided by the customer
3. Identify the nature and the purpose of the transactions
4. Verification of sources of funds

III. Assessing of Customer AML risk based on the information provided by the customer

b) CCFP should Identify each customer , and verify identification as is reasonably capable of identifying a customer on the basis of any official document or other reliable and independent source documents.

c) If evaluating officer believes that conducting the process of CDD measures would “tip-off” the customer , the officer shall terminate conducting the CDD measures and report a Suspicious Transaction Reporting (STR) to the compliance officer through AML compliance coordinator.

6.2 Information collection and KYC

a) The CRO, Marketing Officer and Location Head should ensure that necessary forms are completed and ERP system is updated on timely manner and all the fields are filled up accurately.

b) The application forms and other collected documents should be scanned and updated to the system

c) CCFP should obtain following information from all the customers using the Product application forms/KYC forms designed for each product.

6.2.1 Required Information

CCFP should obtain following information from all the customers using the Product application forms/KYC forms designed for each product.

1) Individual Customers

a) In the case of all individual customers following information should be obtained (Resident)

i. Full name as appearing in the identification document;

ii. Official personal identification national identity card, valid passport, or valid driving license.

iii. Permanent address as appearing on the identification document. If residential address differs from the permanent address residential address shall be supported by a utility bill not over three months old or any other reliable proof of residence approved by the CCFP.

Utility bills are to be specified as **Electricity bill**, **Water bill** and **fixed line telephone bill**. No post-box number shall be accepted except for State owned enterprises. In the case of 'C/o', property owner's consent or other relevant address verification documents such as a valid lease agreement are required to be obtained.

iv. Telephone number, facsimile number, and e-mail address (if available)

v. Date of Birth

vi. Nationality

vii. Occupation, business, public position held and the name of the employer and geographical areas involved (if available)

viii. Purpose for which the account is opened

ix. Expected turnover / volume of business

x. Expected mode of transactions

xi. Satisfactory reference, as applicable

b) In the case of non-resident individual customers

I. The reason for opening the account in Sri Lanka

II. Name, address and the copy of passport of the person or persons authorized to give instructions

c) Both Residential and Non-resident individuals, following documents shall be obtained and should be verified against the original)

(i) Copy of identification document (NIC/Passport/Valid Driving License)

(ii) Copy of address verification document (Electricity bill, water bill, Fixed telephone bill, Lease agreement etc)

(iii) Copy of the valid visa/permit in the case of accounts for non-national customers.

d) For each type of product, relevant Application form/ KYC form should be completed as applicable.

I. Term Deposit - Term deposit Application form

II. Savings deposit – Savings deposit Application form

III. Loan Facilities – Applicable Credit Application form

IV. For joint holder/borrower - Individual KYC form

Refer Annexure 1 for the specimen forms

2) Proprietorship/Partnership Accounts

a) The following information should be obtained from Proprietorship/Partnership Accounts

(i) Full names of the partners or proprietors as appearing in the business registration document

(ii) Nature of the business

(iii) Registered address or the principal place of business

(iv) Identification details of the proprietor/partners as in the case of individual accounts

(v) Contact telephone, fax numbers

(vi) Income Tax file number

(vii) The extent of the ownership controls

(viii) Other connected business interests

b) The following documents shall be obtained and should be verified against the original,

(i) Copy of the business registration documents

(ii) Proprietors' information / Partnership agreement/ Deed

(iii) Copy of identification and address verification documents (of each proprietor/partner)

c) For each type of product, relevant Application form/ KYC form should be completed as applicable.

I. Term Deposit - Term deposit Application form

II. Savings deposit – Savings deposit Application form

III. Loan Facility – Applicable Credit Application form

IV. Pawning Facility – Applicable Pawning KYC form

V. For joint partner - Individual KYC

form Refer Annexure 1 for the specimen forms

3) Corporations/Limited Liability Company

a) The following information shall be obtained from Corporations/Limited Liability Company

(i) Registered name and the Business Registration Number of the institution

(ii) Nature and purpose of business

(iii) Registered address of the principal place of business

(iv) Mailing address, if any

(v) Telephone/Fax/E-mail

(vi) Income Tax file number

(vii) Bank references (if applicable)

(viii) Identification of all Directors as in the case of individual customers

(ix) List of major shareholders with equity interest of more than ten percent

(x) Lists of subsidiaries and affiliates

(xi) Details of names of the signatorie

b) The copies of the following documents shall be obtained and should be verified against the original

(i) Copy of the Certificate of Incorporation (BR)

(ii) Certified Copy of Form 40 (Registration of an existing company) or certified copy of Form l (Registration of a company) under the Companies Act No. 7 of 2007

(iii) Certified Articles of Association

(iv) Certified Board Resolution authorizing the opening of the deposit and Loan facility

(v) Certified Copy of Form 20 (Change of Directors/Secretary and Particulars of Directors/Secretary) under the Companies Act

(vi) Certified Copy of Form 44 (Full address of the registered or principal office of a company incorporated outside Sri Lanka and its principal place of business established in Sri Lanka) under the Companies Act

(vii) Certified Copy of Form 45(List and particulars of the Directors of a company incorporated outside Sri Lanka with a place of business established in Sri Lanka) under the Companies Act

(viii) Copy of the Board of Investment Agreement if a Board of Investment approved company

(ix) Copy of the Export Development Board (EDB) approved letter if EDB approved company

(x) Copy of the certificate to commence business if a public quoted company

(xi) Name of the person or persons authorized to give instructions for transactions with a copy of the Power of Attorney or Board Resolution, as the case may be

(xii) Latest audited accounts if available

c) For each type of product, relevant Application form/ KYC form should be completed as applicable.

I. Term Deposit (Fixed Deposit) - Term (Fixed) deposit Application form

II. Savings deposit – Savings deposit Application form

III. Loan Facilities – Applicable Credit Application form

IV. For each director - Individual KYC form

V. For the Institution – Corporate

KYC Refer Annexure 1 for the specimen forms

4) Clubs, Societies, Charities, Associations and Non-Governmental Organizations (NGO) / Not-for-Profit Organization (NPO)

- The Company shall conduct enhanced CDD measures when entering into a relationship with a NGO or a NPO ,Charities, Clubs , Societies to ensure that their accounts are used for legitimate purposes and the transactions are commensurate with the declared objectives and purposes.
- The individuals who are authorized to operate the accounts and members of their governing bodies shall also be subject to enhanced CDD measures.
- CCFP shall not allow personal accounts of the members of the governing bodies of a NGO, NPO or Charity to be used for charity purposes or collection of donations.
- CCFP should consider Charities, NGO or NPO as High AML-CFT risk clients

a) The following information shall be obtained,

(i) Registered Name and the Registration Number of the institution

(ii) Registered address as appearing in the Charter, Constitution etc

(iii) Identification of at least two office bearers, signatories, administrators, members of the governing body or committee or any other person who has control and influence over the operations of the entity as in the case of individual accounts

(iv) Committee or Board Resolution authorizing the account opening

(v) The source and level of income/funding

(vi) Other connected institutions/associates/organizations

(vii) Telephone/Facsimile numbers/E-mail address

b) The following documents should be obtained and verified against the original

(i) Copy of the registration document/constitution charter etc

(ii) Board Resolution authorizing the account opening

(iii) Name of the persons authorized to give instructions for transactions with a copy of the Power of Attorney or Board/Committee Resolution

c) For each type of product, relevant Application form/ KYC form should be completed as applicable.

I. Term Deposit - Term deposit Application form

II. Savings deposit – Savings deposit Application form

III. Loan Facilities – Applicable Credit Application form

IV. For each office bearer - Individual KYC form

V. For the Institution – Corporate

KYC Refer Annexure 1 for the specimen forms

5) Trust nominees and Fiduciary accounts

a) The following information shall be obtained,

1. Identification of all trustees, settlers/grantors and beneficiaries in case of trusts as in the case of individual accounts;
2. Whether the customer is acting as a 'front' or acting as a trustee, nominee, or other intermediary;

b) The following documents should be obtained and verified against the original

(i) Copy of Trust deed, as applicable

(ii) Particulars of all individuals

c) For each type of product, relevant Application form/ KYC form should be completed as applicable.

I. Term Deposit - Term deposit Application form

II. Savings deposit – Savings deposit Application form

III. Loan Facilities – Applicable Credit Application form

IV. For each trustee - Individual KYC form

V. For the trust – Corporate KYC

Refer Annexure 1 for the specimen forms

d) Stocks and Securities Sector specific requirements

The following information should be obtained from the Funds approved by the "Securities and Exchange Commission" of Sri Lanka (sec),

(i) Name of the Fund

(ii) Purpose of the Fund

6) Occasional Customers, One-off Customers, Walk-in Customers and Third Party Customers

With regard to all cash deposit exceeding rupees **two hundred thousand** or its equivalent in any foreign currency made into an account separately or in aggregate by a third party /one – off customer, CCFP shall conduct CDD and have on record

(i) Name

(ii) Address

(iii) Identification number of valid identity document

(iv) Signature of third party customer

Exception - clerks, accountants, employees, agents, or authorized persons of business places who are authorized to deal with the accounts shall not be considered as a third party.

If CCFP has reasonable grounds to suspect that the transaction or series of linked transactions are suspicious or unusual, CRO/Marketing officer/Location Head shall, obtain such information irrespective of the amount specified above.

6.3 Initial Due Diligence

CCFP should perform due diligence using the information obtained through KYC.

- Verification of copies of documents provided against the original documents
- Verification of sources of funds
- Identification of Ultimate beneficiaries (Refer 5.8 for more guidelines)
- Identification of Politically Exposed Persons (PEP) (Refer 5.9)

6.4 Customer Risk Rating

a) CCFP should assess the ML/TF risk of all of its customers on an ongoing basis using the information collected through KYC process and continuous CDD process.

b) Accordingly, the customers should be classified in to following risk levels based on the evaluation performed using the "Risk Categorisation of Accounts" form (refer Annexure 2).

c) Company adopts an exceptional risk-based approach to evaluate ML-TF risk of credit facilities which is primarily based on the value of the facility. For the credit facilities of the customer below Rs. 750,000 will be treated as low risk products considering the nature, size and complexity of the business.

d) The risk grid is developed based on the general factors that drives the ML/TF risk of customers. Based on the score of the grid, the customer is rated in to "High", "Medium" or "Low" categories.

Risk Category	**Risk Mark**
High	14 and above
Medium	8 to 13
Low	7 or below

e) The form should be duly completed and signed off by CRO or marketing officer accurately based on the information provided by the customer both manually and in the ERP system.

f) The Location head/ Head of the department should verify and approve the completed document.

g) Duly completed document should be filed along with the product application for

6.4.1 Special considerations

a) Irrespective of other factors, of the individual customer is a Politically Exposed Person (PEP), such customer should be rated as high risk customer.

b) If the Ultimate beneficiary of the Customer is difficult to identify, the **risk score of 10** should assign to the customer.

c) For any following Unacceptable businesses, the relevant officers should consult the location head and take necessary steps to reject on-boarding.

    I. Customer screening - with sanction lists such as UN regulations (Specially designated Nationals and blocked persons list - SDN) and others
    II. Customer/Beneficial owner name appears in the list of specially designated nationals SDNs of OFAC
    III. Unable/Doubtful as to the identity of the UBO/s
    IV. Engage in narcotics & dealing in arms and ammunition
    V. Unregistered financial institutions

d) If CCFP identified any sanctioned party during this process, such information should be reported to FIU immediately. (refer section 6 of this procedure manual for more details)

e) Geographical locations listed under section 5.5 should be considered as high risk jurisdictions.

f) If the customer's residential address is more than 50 Km radius and whereas customer is unable to provide address proof, geographical risk should be rated as "Medium"

g) If the customer is an off shore customer(other than sanctioned/high risk geographical areas), the geographical risk should be rated as "Medium"

6.5 Geographical Risk assessment

a) CCFP shall not conduct any transaction with customers from black listed countries by the Financial Action Task Force and updated list can be found in the link provided (https://www.fatf-gafi.org/en/countries/black-and-grey-lists.html)

b) CCFP should extremely be vigilant if the transaction is with the high risk / Grey listed countries as highlighted by the Financial Action Task Force and updated list can be found in the link provided (https://www.fatf-gafi.org/en/countries/black-and-grey-lists.html) .

c) In the case of a prospective customer whose permanent address given in the application is at a location far away from that of the branch which receives the account opening request, CRO/Marketing officer shall discourage or turn down the request to open the account and shall request the prospective customer to open the account at the closest branch to the customer's residence or business, unless an acceptable and a valid reason is given to keep in record.

6.6 Product Service Risk assessment

a) CCFP should carry out a Product/ Service Risk assessment prior to launching a new product or service.

b) Chief Risk Officer and Compliance Officer should conduct a risk assessment for existing product/services on an annual basis and results should be reported to the BIRMC and to the Board of Directors.

c) Following factors should considered when assessing the product risk

I. Nature of the product

II. Expected market segment/ target customer base

III. Average size of the facility/deposit/transaction

IV. Delivery channels to be used

6.7 Enhanced Due Diligence (EDD)

a) Based on the risk of the Customer, the Company should perform EDD regularly to monitor transactions in accounts in order to ensure that they are consistent with the customers profile and source of funds. The supervising officials are required to verify the reports of accounts opened and/or amendments made to customer profile.

b) Where the risks of ML/TF are higher, financial institutions should be required to conduct enhanced due diligence (EDD) measures for higher-risk business relationships which may include:

- Obtaining and verifying additional information on the customer (e.g. occupation, volume of assets, information available through public databases, internet search, etc.)
- Updating more regularly the identification data of customer and beneficial owner
- Obtaining and verifying additional information on the intended nature of the business relationship
- Obtaining and verifying information on the source of funds or source of wealth of the customer
- Obtaining and verifying information on the reasons for intended or performed transactions
- Obtaining and verifying the approval of senior management to commence or continue the business relationship
- Conducting enhanced monitoring of the business relationship, by increasing the number and timing of controls applied, and selecting patterns of transactions that need further examination
- Requiring the first payment to be carried out through an account in the customer's name with a bank subject to similar CDD standards.

6.8 Ongoing Customer Due Diligence

a) CCFP should carry out Customer Due Diligence on its existing customers to identify the purpose, nature of the transactions and the sources of funds of the customers on an ongoing basis.

b) The Customer Relationship Officer/ Marketing Officer / Location Head must ensure that adequate information are obtained and verified prior to the transaction is processed.

c) If it is unable to obtain such information CCFP shall,

   I. In relation to a new customer, not to enter into a business relationship or perform the transaction

   II. In relation to an existing customer, terminate the business relationship, with such customer and consider making a Suspicious Transaction Report (STR) in relation to the customer

d) The CCFP should carry out Customer Due Diligence on an ongoing basis based on the initial risk assessment of the customer as follows,

Risk Category	**Frequency of Testing**
High	Annually
Medium	Once in three years
Low	Once in 5 years

e) Based on the risk rating, Customer due diligence should be carried out and customer information provided at the time of accepting the customer should be verified and updated. Details of such verification should be updated in the Interact history of the ERP.

f) Marketing officer/Customer Relationship officer/Location head should ensure that customer due diligence is carried out on timely manner

6.9 Delayed verification for low risk customers

a) Delayed verification can be carried out by the CCFP for specified products if the customer risk is rated as low and delay shall be essential so as not to interrupt the CCFP's normal conduct of business.

b) For each case where delayed verification is allowed, Location Head shall ensure that no suspicion of money laundering or terrorist financing risk is involved and prior approval shall be obtained from the Product Head for delayed verification.

c) List of customers who are allowed for delayed verification shall be forwarded to the Compliance team within 3 days of such transactions.

d) If the Delayed verification process is applied to a customer, the documents should be completed within 14 days of accepting the customer.

e) However, the withdrawal of such account is not permitted until the full CDD is completed. The Location Head will be responsible to follow-up with the customer until the full CDD is completed.

6.10 Identification of a Beneficial Ownership

a) CCFP should identify the beneficial owner of a Legal person.

b) Legal person means “any entity other than a natural person that is able to establish a permanent customer relationship with a financial institution or otherwise owns a property and includes a company, a body corporate, a foundation, a partnership or an associate.

c) CCFP should identify the ultimate beneficiary in one of the following methods,

   I. Which natural person owns or controls more than 10% of the customer’s equity?

   II. Which natural person has “effective control” of the legal person?

   III. On behalf of which natural person the transactions being conducted?

d) CCFP should obtain adequate information to identify and verify the identity of the beneficial owners of the customer using relevant information or data.

e) For this purpose “Ultimate beneficiary form” should be filled by an Authorized officer of the customer and CRO/Marketing officer should verify and sign off the information provided. (Refer Appendix 3)

f) The Authorized officer of the customer should declare that he/she is the authorized officer and should certify the information provided as accurate with official stamp.

g) Once the beneficial owner of the customer is identified, following information of each beneficial owner should be obtained,

   I. Full Name

   II. Official personnel identification or any other identification number (NIC/Passport etc.)

   III. Permanent/Residential address

h) CCFP is required to verify the identity of the beneficial owner using reasonable measures depending on the risk and complexities of the ownership and control structure of the legal person or management.

i) For the verification purpose, CCFP can rely on following documents,

   I. Share register
   II. Annual returns
   III. Trust deed
   IV. Partnership agreement
   V. The constitution or certificate of incorporation for an incorporated association
   VI. The constitution of a registered cooperative society
   VII. Minutes of the meetings of Board of Directors
   VIII. Information available through open source search or commercially available database.

j) CCFP should review the beneficial ownership of the customer periodically based on the AML risk assessment of the customer using the "Risk categorization of Customer" form,

   I. High risk Customers – Annually
   II. Medium risk Customers – Every 3 years' time
   III. Low risk customers – Every 5 years' time

k) If it is unable to identify and verify the beneficial ownership of any customer, the company should not enter into the business relationship or perform the transactions with new customers and terminate the business relationship with existing customers and consider making a Suspicious Transaction Report (STR).

l) The verification of beneficial ownership should be completed prior to establishing financial transaction with the customers and delayed verification of beneficial ownership is only allowed for low risk customers subject to procedures mentioned in this document.

6.10.1 Effective control of a legal person

a) Effective control of a legal person can be direct or indirect, formal or informal.

b) At a direct and formal level, it is essential to understand a legal person's governance structure to identify the natural persons that exercise effective control over the legal person.

c) In deciding the effective controller(s) in relation to a customer that is a legal person, CCFP should consider,

I. A natural person who can hire or terminate a member of senior level management;

II. A natural person who can appoint or dismiss Directors;

III. Senior managers who have control over daily/regular operations of the legal person/arrangement (e.g. a CEO, CFO or a Managing Director).

6.10.2 Beneficial owner of a legal arrangement (Trust/Fiduciary account or a nominee)

a) Company should take reasonable measures to obtain and verify the information about the beneficial ownership of a legal arrangements. A Legal arrangement includes trust, Fiduciary account or a nominee. In order to identify the beneficial ownership of a trust, the company should identify the,

I. The Identities of the Author /Settler of the trust
II. The Trustees
III. The beneficiary or class of beneficiaries
IV. Other natural persons exercising ultimate effective control over the trust

b) The company shall take reasonable measures to verify trust documents through Legal department

6.11 Politically Exposed Person (PEP)

a) “Politically Exposed Person" means an individual who is entrusted with prominent public functions either domestically or by a foreign country, or in an international organization and includes a, (refer **Appendix 4** for a list of PEPs identified by CCFP):

I. Head of a State or a Government
II. A Politician
III. A senior government officer
IV. A judicial officer
V. A Military officer
VI. A senior executive of a State owned Corporation ,Government or autonomous body but does not include middle rank or junior rank individuals
VII. Family members and close associates of any of above

b) Further, CCFP shall also check for and monitor customers that have relationships with PEPs as a business relationship with those parties involve reputational risks similar to those of the PEP; relationships include family members or close associates.

c) Immediate family members include,

I. Spouse (Current or past)
II. Siblings (including half siblings) and their spouses
III. children (including step-children and adopted children) and their spouses
IV. parents (including step-parents)
V. grand children and their spouses

d) A close associate include,

I. A natural person having joint beneficial ownership of legal entities and legal arrangements, or any other close business relationship with any person identified in guidelines

II. A legal person or legal arrangement whose beneficial owner is a natural person and is known to have been set up for the benefit of such person or his immediate family members identified

III. A PEP's widely- and publicly-known close business colleagues or personal advisors, in particular, persons acting in a financial fiduciary capacity

e) PEP is identified in following ways,

I. Declaration by the customer

II. Through the customer screening

III. Identification by the CCFP employees

f) Identified PEPs should be flagged as PEP in the ERP system

g) Approval from Genius Operation Level -5 and above should be obtained when a customer has been identified as a PEP. Genius Operation Level -5 and above shall evaluate the PEP customer carefully before granting the approval

h) Customer Risk rating of a PEP should designate as high irrespective off the other factors. The source of funds, source of wealth, and/or the beneficial owner should be verified distinctly with documentary evidence

i) It is required to conduct EDD of the business relationships of any customer identified as a PEP

j) List of PEPs identified shall be available in the ERP system

6.12 Sanctions Screening

a) CCFP has acquired a screening solution from KPMG Technologies named “KTMS” and currently subscribed to “worldcheck” data base.

b) Customers should be screened against “worldcheck” data base using the KTMS and should identify any sanctioned names.

c) The KTMS / “worldcheck” is configured to identify any matches which are having the match percentage decided by the company.

d) This should be carried out at the time of onboarding the customer.

e) Compliance team is alerted on identified match by KTMS

f) Compliance team should verify and clear the matches

g) Further information should be obtained by the compliance officer from the branch if required to satisfy himself.

h) Ongoing screening is enabled for existing customers where an existing customer become a sanctioned party.

i) Any matches identified should be cleared by the Compliance officer or authorized officer

j) CCFP should not onboard any party who is identified as a sanctioned party and periodic reviews should be conduced.

k) Steps should be taken to inform FIU immediately on any identified sanctioned party.

l) Updated Sanction lists need to be uploaded to the system and Identify the matches and any positive matches need to be immediately raised the STR and informed the FIU and Competent authority regarding the same.

m) Latest United Nations Security Council Resolutions can be downloaded using following link (https://competentauthority.gov.lk/)

6.13 Transactions Monitoring

a) Based on the risk sensitivity of the account, transactions should be monitored regularly. High risk customers must be monitored intensively. Branches must pay special attention to all complex, unusually large transactions and all unusual patterns, which have no apparent economic or visible lawful purpose.

b) Transaction of deposits/withdrawal/remittances of unusual, large amounts must be examined for detecting money laundering.

c) A sample list of suspicious indicators were listed in **Annexure 5** of this procedure Manual.

6.13.2 Systems Based Monitoring

a) KTMS system is used to monitor suspicious transactions based on the parameters established for each product type.

b) A list of parameters established are listed in Annexure 6 of this procedure manual.

c) Established parameters should be reviewed on periodic basis at least on an annual basis by the CRO and CO. Such reviewed parameters should be tabled at BIRMC for approval.

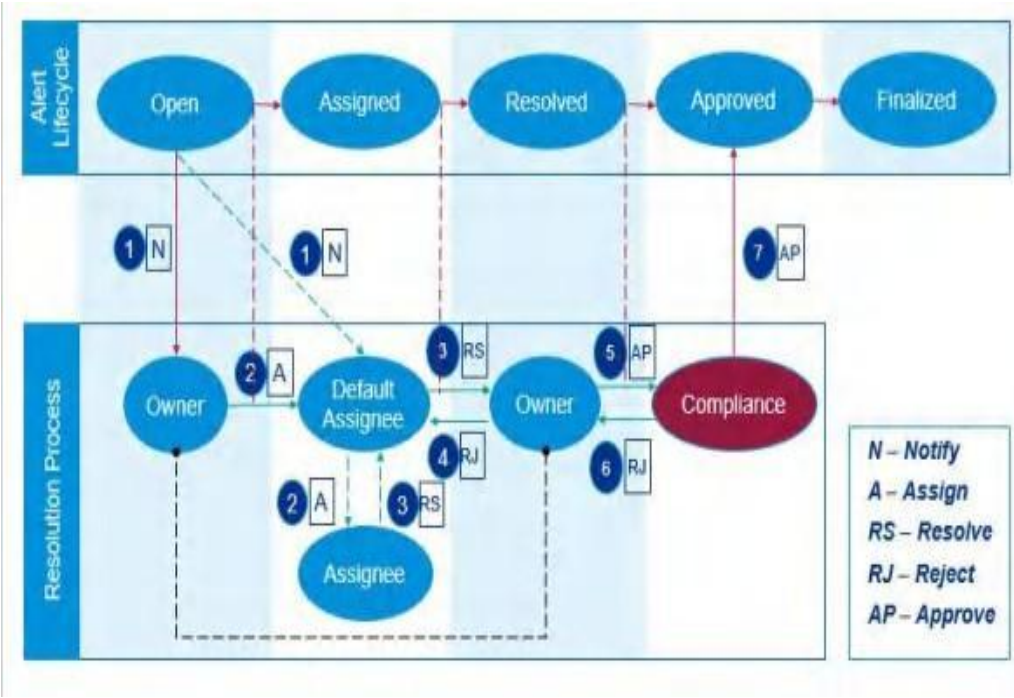
d) Any suspicious transaction highlighted by the KTMS is cleared by the product owner, Product head and Compliance officer.

e) Any suspicious transaction decided to report should be reported as per the guidelines set out in “Reporting unusual/suspicious transactions”

f) Alert Life cycle included the following steps

   a. Open - Based on the parameters
   b. Assigned- Representative from relevant product/service
   c. Resolved - Representative from relevant product/service
   d. Approved - Respective Product wise senior Administration team
   e. Finalized - Compliance Team

Detailed workflow of the process is show below,



6.13.3 Reporting unusual/ suspicious transactions

a) All branches are required report any suspicious transactions to the AML coordinating officer within 24 hours of such transaction including following information
    I. Name of the party
    II. Identification number
    III. Address
    IV. Amount of transaction
    V. Any other details required by the compliance officer
b) AML Compliance officer, after evaluation may decide to report such transaction to FIU and in such situation such reporting should be done within 48 hours of confirmation of the suspicious nature
c) For any unreported transactions compliance officer should document the reasons for such decision.

d) Suspicious transaction reporting should be kept confidential and branches are cautioned against "tipping-off' the customers whose suspicious transactions are being reported.

e) Any staff member of CCFP should not divulge/ disclose information to any other person that the suspicion has been formed or an STR has been filed with FIU that could affect the investigation or pervert the course of justice by alerting individuals to an investigation being, or about to be undertaken OR by destroying, concealing or falsifying relevant documents.

f) The Compliance Officer should maintain a STR Register with following minimum information,
    I. Customer Name
    II. NIC/PP
    III. Address
    IV. Contract number
    V. Transaction details

7. REPORTING

7.1 FIU Reporting

Compliance Officer should ensure that following reporting are made to FIU on timely manner.

a) Cash Transactions Reports (CTR)/ Electronic Fund Transfers (EFT)

I. Cash transactions/ Electronic Fund Transfers above Rs. 1 Mn. or its equivalent or any such threshold set by the FIU every 30 days or the deadline specified by the regulator

II. Such report is generated through the ERP system and is converted using the application provided by the FIU and IT team should ensure all the transactions are included as instructed by the compliance officer

III. Such converted report is uploaded to the web based system facilitated by FIU.

b) Suspicious Transactions Reports (STR)

I. Suspicious Transactions should be reported soon as practicable, after forming that suspicious or receiving the information, but not later than two working days therefrom.

II. Compliance officer should report STRs using the web based system provided by the FIU.

c) Apart from above, CCFP may provide any other ad-hoc reports requested by FIU or any other regulator on time to time.

6.2 Internal Reporting

The Following reporting should be made to the Board of Directors through BIRMC on a periodic basis,

1. Institutional risk assessment
2. Product risk assessment
3. Geographical risk assessment
4. Statistical details of followings,
    a. STRs raised
    b. FIU inquiries

c. No. of high risk customers identified

d. No. of PEPs identified

5. Compliance status of AML/CFT
6. Review and changes in transaction monitoring parameters

8. RECORD KEEPING

a) CCFP shall maintain the following information for a minimum period of six years from completion of such transactions in electronic form in the company's file systems.

I. All records of transactions and of correspondence relating to transactions and records of all reports furnished to the Financial Intelligence Unit should be maintained by the compliance department

II. All details in relation to incoming and outgoing transactions

III. Instructions received from customers

IV. CTR/EFT original data files

V. CTR/EFT encrypted data files

VI. Loan Agreements

VII. Suspicious Transaction Reports and analysis made in order to report the suspicious transaction

VIII. The records of identification data obtained through CDD process such as copies of identification documents account opening forms, know your customer related documents, verification documents and other documents along with records of account files and business correspondence,

b) Customer transaction records should be maintain in the ERP system

c) The records of identification data obtained through CDD process such as copies of identification documents account opening forms, know your customer related documents, verification documents and other documents along with records of account files and business correspondence either in physical form or electronic.

d) The Company must records of transactions, both domestic and international, including the results of any analysis undertaken such as inquiries to establish background and purpose of

complex, unusually, large transactions (above Rs. 100 Mn transactions or exposures).

I. Risk Assessment Reports

II. Review against sanction list, etc.

e) Training records in relation to training of employees and directors on AML/CFT

f) The Company Secretary shall retain the Board /BIRMC /BAC minutes regarding AML/CFT/PF issues and provide them to any investigation or regulators when requested

g) In the event where the transactions, customers or accounts are involved in litigation or required to be produced in a court of law or before any other appropriate authority, the company should maintain such records for longer periods than six years as stipulated above.

9. RECRUITING EMPLOYEES / DIRECTORS

a) The CCFP shall perform an employee due diligence and screening at the time of appointing or hiring of employees whether permanent, contractual or outsourced.

b) CCFP should collect following documents / information from the employees where applicable

I. National Identity Card

II. Grama sevaka certificate

III. Police clearance report

c) New recruits should be screened against the sanctions list before onboarding using the automated system function in the company system.

d) When appointing a Director to the Board of Directors of the Company, The Compliance team should screen such Director against the sanctions lists and results of the same may be reported to Nomination Committee on request by the committee.

10. TRAINING ON AML/CFT

a) The Compliance Department, in collaboration with Learning and Development Department, shall provide training on the AML/CFT to board of directors and all staff of the Company on timely basis

b) Such training program should include,

✔ Regulatory requirements relating to AML/CFT

✔ Internal policies and procedures, Risk Management relating to AML/CFT

✔ New developments of ML/TF techniques, methods and trends

✔ Roles and responsibilities of the Board of Directors and Staff Members

c) The Training programs should be carried out on following basis with the support of Learning and Development

I. Board of Directors – Annually
II. Senior Management – Annually
III. Locations Heads – Annually
IV. Marketing Staff/Customer Relationship Officers – Annually
V. Finance, Risk, Internal Audit – Annually
VI. Other support services – once in every two years
VII. New Recruitments – At the induction program

d) Apart from the regular training programs, the Compliance Department should ensure that the new Acts/Regulations/Rules/Circulars/ guidelines etc. were timely communicated to the staff members via training programs or any other means such as emails or memos.

11. NEW PRODUCTS AND TECHNOLOGIES

a) CCFP should carry out AML risk assessment prior to launching a new product

b) Compliance Officer should assess the AML risk of the product taking in to account following factors,

I. Nature of the product

II. Targeted customer segment

III. Delivery channels

IV. Expected average value of the transactions

V. Geographical factors

c) The results of such assessment should be reviewed by “New product approval Committee” when approving the new products.

d) If the compliance officer determines that the ML/TF risk is high, such products should not be launched.

e) If any ML risk is identified, strategies to mitigate such risks should be identified and documented by the CRO.

12. CLOSED –CIRCUIT TELEVISION (CCTV) OPERATIONS

Based on the Guidelines for Financial Institutions on CCTV operations for AML/CFT purposes, No. 2 of 2021 company need to have procedure to monitor CCTV operations.

12.1 The Requirements for CCTV Systems

As part of the constant commitment to enhance operational risk management and safeguard banking operations against risks of being abused for money laundering and financing of terrorism, every company is advised to have in place a robust CCTV system installed fully operational both within and outside of the premises. The business premises refer to the head office, branches, outlets and any other place or places where Customer Due Diligence (CDD) is conducted.

12.2 Placement of CCTV cameras

In order to enhance the effective usage of the CCTV system, company need to ensure that CCTV cameras are installed at appropriate locations, in a manner that the camera is able to clearly capture, monitor and record the relevant areas where business operations take place.

These locations are required to include the counters, customer interaction areas where CDD takes place, areas where safe deposit boxes are located, safe or vault and other cash handling areas, vehicle parking areas, the entrance and exit of the business premises, any other suitable areas, both inside and outside the building as detained by the company.

The CCTV surveillance systems must be aligned in a suitable manner and at an angle as to obtain a complete and unimpeded view of the area. Further, CCTVs need to be positioned in a manner where the capturing and processing inf01mation of the CCTV system is not interfered or impeded by internal or external lighting, glare, or any object.

12.3 Functions of CCTV system

- Company should ensure all images captured and recorded by the CCTV cameras are visible, recognizable and clear.
- The visual images or videos rendered through the CCTV cameras need to have the capability of identifying the features of the individuals, if any, that transact and should be clearly discernible from one image from another.
- In addition, adequate lighting must be maintained in order to capture clear CCTV footage.
- Quality digital equipment should be used in CCTV systems to capture a clear frontal images of individuals.
- The CCTV systems should pennit easy viewing, recording and retrieval of high-quality images (e.g., adequate number of pixels for improved zoom capabilities) of all information contained in CCTV system. Necessary technical specifications (e.g., resolution, frame rate) need to be maintained at a standard level to achieve an effective CCTV surveillance.
- The CCTV systems should remain operational throughout the 24-hours of a day - every day of the year, including during times when the FI is cJosed for business.
- CCFP should ensure real-time monitoring at the head office and/or branches or at a central monitoring unit, as far as practicable.

Company are advised to obtain assistance of its security services personnel or law enforcement agencies (LEAs) to mitigate immediate risks that may arise to the Fl's premises or to equipment, to its customers or to potential customers, or to any person at the vicinity of the CCTV camera, if such risk is detected based on CCTV footage obtained on real-time basis.

12.4 Maintenance of records

Company should maintain all infom1ation captured in the CCTV system for a minimum period of **90 days.**

CCFP, at their discretion, may retain the CCTV recordings relevant to observed suspicious. The FIU, LEAs or any other competent authority would, from time to time, instruct the company to retain the CCTV recordings relevant to a Suspicious Transactions Report furnished to FIU or any other

related CCTV footage of a possible offending until the relevant investigations are concluded by the LEAs or other relevant competent authorities.

In order to have an effective surveillance and monitoring of business operations, company should ensure that the CCTV system(s) deployed is/are properly maintained and operational, and remain under good working condition at all times. The CCTV system should be equipped with the relevant features and functions to enable to implement control measures that will prevent such system from being manipulated or misused by any unauthorized parties. Company should ensure activities relating to the maintenance and recalibration of the CCTV system including system upgrading and removal of records are clearly recorded in the system's maintenance log and reported to the senior management, as appropriate.

12.5 Authority to Access

- Branch Level - Branch Manager / Branch In charge and Operation Head
- Central Accesses - Access only to relevant Authorised personnel to ensure proper accountability for the assigned functions.

12.6 Auditing of the CCTV Operations

Procedures should be in place for periodical review and audit of the CCTV system(s) for number of existing cameras in the premises at branch level. Audits and reviews should ensure the adequacy of the number of cameras, functionality, accuracy, operability, record keeping and other salient requirements. A report of such review/ audit on the adequacy of CCTV coverage should be submitted to the Board of Directors (BOD) and to the senior management. The senior management and the BOD are advised to take appropriate steps to rectify such deficiency or increase the coverage as appropriate.

12.7 Money Value Transfer Services

MMBL Money Transfer operates through an expansive network of over 2000 payout locations, ensuring broad accessibility for consumers. These locations include banks, non-banking financial institutions, cooperative rural banks, corporate entities, pawning and money changers, agency post offices, and retail outlets, providing consumers with convenient, nearby locations for financial transactions.

MMBL Money Transfer, through its CCFP operation, holds a Western Union Sub-Representation Agreement that is subject to prior approval by the Central Bank of Sri Lanka (CBSL). The CCFP branch exclusively handles the processing of Western Union outward payments.

- **Transaction Process:**

1. Recipient Collection Process:

Recipients can collect transferred funds by presenting a valid identification document along with the Money Transfer Control Number (MTCN) provided by the sender.

2. Dual System Processing:

Each transaction must be processed in two systems:

Western Union System: The initial processing is conducted within the Western Union platform, accessed through a Virtual Private Network (VPN).

CCFP Core System: After the transaction is processed in the Western Union system, it is then processed in the CCFP Core System, allowing the disbursement of funds to the customer.

Identity Verification:

The identification of the recipient is conducted by CCFP officers at the branch when the customer comes to collect their funds. This in-person verification ensures the legitimacy of the transaction.

3. Customer Creation & Sanctions Screening

Customer profiles are created within the CCFP Core System. All customers undergo screening against the United Nations Security Council Resolution (UNSCR) sanctions list to ensure compliance with international regulations.

4. Customer Due Diligence (CDD)

- For cross-border wire transfers of rupees one hundred thousand or above or its equivalent in any foreign currency, a Company shall verify the identity of the beneficiary, and maintain the information in accordance with the CDD rule if the identity has not been previously verified.
- The CRO Should collect the Valid identity document as per the section 6.2.1 and Create the Customer in system and fill up the form given in **Annexure 7.**
- Company need to reject or suspend a wire transfer with insufficient beneficiary information and inform the Western Union Agent Immediately and Compliance team.
- Compliance Officer should decide to whether to raise an STR based on the circumstances.

5. Threshold Reporting:

Transactions exceeding Rs. 1 Million are subject to threshold reporting. Such transactions must be manually reported to the Financial Intelligence Unit (FIU) via the GoML system, ensuring compliance with regulatory requirements.

End of document