

ANTI-MONEY LAUNDERING AND COMBATING THE FINANCING OF
TERRORISM (AML / CFT)

COMPLIANCE DEPARTMENT
SWYCHR TECHNOLOGY USA LLC

Disclaimer:

Swychr Technology USA LLC, after referred to as SWYCHR compiles a booklet of Regulations from time to time for convenience of key stakeholders. The amendments are made in these regulations through issuance of Circulars/Circular letters to who may be concerned from time to time; therefore, this policy of Anti-Money Laundering/ Combating the Financing of Terrorism Regulations on a specific date may not reflect latest position.

PART – B REGULATIONS

REGULATION - 1

CUSTOMER DUE DILIGENCE (CDD)

When CDD measures are to be applied

1. Apply CDD measures;
 - (a) when establishing business relationship;
 - (b) while dealing with occasional customers;
 - (c) in other situations/ scenarios when there is suspicion of money laundering/ financing of terrorism, regardless of threshold; and
 - (d) when there are doubts about the veracity or adequacy of previously obtained customer identification data.

CDD Measures for Establishing Business Relationship
Identification of Customers

2. Every customer shall be identified for establishing business relationship. For this purpose, there is a range of documents which shall be obtained for different types of customers.
3. For identity and due diligence purposes, at the minimum following information shall also be obtained, verified and recorded on KYC/CDD form or account opening form and relevant Information Technology (IT) systems;
 - (a) Full name as per identity document;
 - (b) Identity document number or where the customer is not a natural person, the registration/ incorporation number or business registration number (as applicable);
 - (c) Existing residential address, registered or business address (as necessary), contact telephone number(s) and e-mail (as applicable);
 - (d) Date of birth, incorporation or registration (as applicable);
 - (e) Nationality or place of birth, incorporation or registration (as applicable);
 - (f) Nature of business, geographies involved and expected type of counter-parties (as applicable);
 - (g) Purpose of account;
 - (h) Type of account;
 - (i) Source of earnings;
 - (j) Expected monthly volume of business; and
 - (k) Normal or expected modes of transactions.

Verification of Identity

4. SWYCHR shall verify identities of the customers (natural persons) and in case of legal persons, identities of their natural persons from relevant authorities or where necessary using other reliable, independent sources and retain on record copies of all

reference documents used for identification and verification..

5. SWYCHR shall conduct biometric verification where practical for all customers, before establishing new relationships, except in cases of genuine reasons or technical issues as prescribed.

Identification and Verification of Natural Persons Acting on Behalf of Customer

6. In relation to Para 4 and 5 above, where one or more natural persons are acting on behalf of a customer/ occasional customer/ walk-in customer or where customer is legal person or legal arrangement, SWYCHR shall identify the natural persons who act on behalf of the customer, verify the identity of such persons and record the same in the relevant IT system. Moreover, SWYCHR shall seek information on powers (legal basis or authority) that regulate and bind the legal person or arrangement, as well as the names of the relevant persons having a senior management position in the legal person or arrangement.
7. Authority of such person to act on behalf of the customer shall be verified through documentary evidence including specimen signature of the persons so authorized.

Identification and Verification of Identity of Beneficial Owners

8. Reasonable measures shall be taken to obtain information to identify and verify the identities of the beneficial owner(s) in relation to a customer, using the relevant information or data obtained from a reliable source.
9. Where the customer is not a natural person, SWYCHR shall (i) take reasonable measures to understand the nature of the customer's business and its ownership and control structure for obtaining information required to determine the natural persons who ultimately own or control the customer.
10. In case there is doubt as to whether the persons with the controlling ownership interest is/are the beneficial owners or where no natural person exerts control through ownership interests, the identity of the natural persons (if any) exercising control of the legal person or arrangement should be identified and verified through other means. Where no natural person is identified, the identity of the relevant natural person who holds the position of senior managing official should be verified along with other due diligence measures.
11. For customers that are legal arrangements, SWYCHR is required to identify and take reasonable measures to verify the identity of beneficial owners through the following information:
 - (a) for trusts, the identity of the settlor, the trustee(s), the protector (if any), the beneficiaries or class of beneficiaries, and any other natural person exercising ultimate

effective control over the trust (including through a chain of control/ownership as ascertained during CDD/EDD);

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

12. SWYCHR shall obtain from legal entities, the ultimate beneficial ownership information i.e. natural persons or individuals who ultimately own or control the company, that are required to maintain such information.

Information on the Purpose and Intended Nature of Business Relations

13. SWYCHR shall obtain from customers, information as to the purpose and intended nature of business relations.

Timing of Verification

14. Verification of the identity of the customers and beneficial owners shall be completed before business relations are established.

15. SWYCHR may accept advance payment & wallet recharge at the time of submission of necessary documents by their prospective customers (individual natural persons only) subject to the following;

(a) Advance payment receipt will be issued with 'Disclaimer' that account shall be opened and conduct of business shall start after completing necessary due diligence including & verification through manual & technology assisted mechanism;

(b) The advance payment will be credited to customer's designated account only.

Where CDD Measures are Not Completed

16. In case TIK is not able to satisfactorily complete required CDD measures, business shall not be conducted with this customer.
17. If SWYCHR is unable to satisfactorily comply with CDD measures of an existing customer, the relationship shall be terminated and reporting of suspicious transaction be considered as per law. Further, SWYCHR shall serve a prior notice and record cogent reasons for terminating business relationships in their systems on a case to case basis.
18. In cases where SWYCHR form suspicion of money laundering, terrorist financing or other criminal activity, and they reasonably believe that performing the CDD process will tip-off the customer, they may not to pursue the CDD process, and instead alert the appropriate authority.

Ongoing Monitoring

19. All business relations with customers shall be monitored on an ongoing basis to ensure that the transactions are consistent with the SWYCHR knowledge of the customer, its business and risk profile and where appropriate, the sources of funds.
20. SWYCHR shall obtain information and examine, as far as possible the background and purpose of all complex, unusual large transactions, and all unusual patterns of transactions, which have no apparent economic or visible lawful purpose. The background and purpose of these transactions shall be inquired and findings shall be documented with a view to making this information available to the relevant competent authorities when required.
21. SWYCHR shall periodically review the adequacy of customer information obtained in respect of customers and beneficial owners and ensure that the information is kept up to date, particularly for higher risk categories of customers. The review period and procedures thereof should be decided on a case by case basis.

22. The customers' profiles should be revised keeping in view the spirit of KYC/CDD and basis of revision shall be documented and customers may be consulted, if necessary.

Anonymous or Fictitious Account

23. SWYCHR shall not conduct business with anonymous accounts or accounts in the name of fictitious persons or numbered accounts.
24. In case of an account/ relationship of an entity with abbreviated name or title, SWYCHR shall satisfy itself that the subject name/ title is in accordance with the constituent documents of the customer entity. Any account/ relationship shall not be allowed in abbreviated name in cases where entity has its complete name (non-abbreviated) in their constituent document.

Review of Products and Services including new Technologies

25. SWYCHR shall identify and assess the ML/TF/PF risks that may arise in relation to the development of new products, services and business practices including delivery mechanisms, and the use of new or developing technologies for both new and pre-existing products, especially those that may favor anonymity.
26. Furthermore, risk assessments shall be undertaken prior to the launch or use of such products, services and business practices and technologies. Appropriate measures should be taken to manage and mitigate the identified risks.

Government entities

27. SWYCHR shall not conduct business with personal names of the government official(s). Business with governments which is to be operated by an officer of the Federal/Provincial/Local Government in his/her official capacity, shall be conducted following a special resolution/authority from the concerned administrative department duly endorsed by the Ministry of Finance or Finance Department of the concerned Government.
28. However, in case of autonomous entities and Armed Forces including their allied offices, SWYCHR may conduct business with them on the basis of special resolution/authority from the concerned administrative department or highest executive committee/management committee of that entity duly endorsed by their respective unit of finance. SWYCHR shall also take into account any rules, regulations or procedures prescribed in the governing laws of such entities relating to conducting business of the specified nature.

Existing Customers

29. SWYCHR shall perform such CDD measures as may be appropriate to its existing customers having regard to its own assessment of materiality and risk but without compromise on identity and verification requirements.
30. SWYCHR is prohibited, on an ongoing basis, from conducting business with proscribed/ designated entities and persons or to those who are known for their association with such entities and persons, whether under the proscribed/ designated name or with a different name. SWYCHR should monitor their relationships on a continuous basis and ensure that no such relationship exists. If any such relationship is found, immediate action shall be taken as per law, including reporting to the appropriate authorities.
31. For existing customers who opened accounts with old NICs, SWYCHR shall ensure that attested copies of identity documents shall be filed. SWYCHR shall block accounts without identity document (after serving one month prior notice) irrespective of mode of payment, until the subject regulatory requirement is fulfilled. However, block from the accounts shall be removed upon submission of attested copy of identity document and verification of the same however appropriate.

Dormant accounts

32. For customers whose accounts are dormant or in-operative, SWYCHR will not allow transactions on this type of account until due verification and activation through the stipulated processes have been followed.

Prohibition of personal accounts for business purposes

33. SWYCHR shall not allow personal accounts to be used for business purposes except proprietorships, small businesses and professions where constituent documents are not available and SWYCHR & other relevant partners are satisfied with KYC profile of the account holder, purpose of relationship and expected turnover of the account keeping in view financial status & nature of business of that customer.

Politically Exposed Persons (PEPs)

34. In relation to PEPs and their close associates or family members, SWYCHR shall:
- (a) implement appropriate internal policies, procedures and controls to determine if a customer or beneficial owner is a PEP;

- (b) obtain approval from the senior management to establish or continue business relations where the customer or a beneficial owner is a PEP or subsequently becomes a PEP;
- (c) establish, by appropriate means, the sources of wealth or beneficial ownership of funds, as appropriate; including SWYCHR own assessment to this effect; and
- (d) conduct during the course of business relations, enhanced monitoring of business relations with the customer.

NGOs/NPOs/ Charities' accounts

35. SWYCHR should conduct enhanced due diligence (including obtaining senior management approval) while establishing relationship with Non-Governmental Organizations (NGOs)/Not-for-Profit Organizations (NPOs) and Charities to ensure that their transactions are for legitimate purposes and the transactions are commensurate with the stated objectives and purposes.
36. Business should be conducted in the name of relevant NGO/NPO as per title given in constituent documents of the entity. The individuals who are authorized to deal on behalf of the NGOs are all members of their governing body should also be subject to CDD separately. SWYCHR should ensure that these persons are not affiliated with any proscribed/ designated entity or person, whether under the same name or a different name.
37. Personal accounts shall not be allowed to be used for charity purposes/collection of donations.
38. All existing relationships of NGOs/NPOs/Charities should be reviewed and monitored to ensure that these organizations, their authorized signatories, members of their governing body and the beneficial owners are not linked with any proscribed/ designated entity or person, whether under the same name or a different name. In case of any positive match, SWYCHR should consider alerting the appropriate authorities.

Customers from High-Risk Jurisdictions

39. SWYCHR shall apply enhanced due diligence, proportionate to the risks, to business relationships and transactions with natural and legal persons (including financial institutions) from foreign jurisdictions.
40. SWYCHR shall apply countermeasures proportionate to the risks: (a) when called upon to do so by the appropriate authorities, or (b) independently of any call by the authorities to do so.

Prohibition on Reliance on Third Parties for CDD measures

41. SWYCHR shall not rely on third parties to perform any CDD measures as prescribed in these Regulations.

REGULATION - 3

WIRE TRANSFERS/ FUND TRANSFERS

1. The requirement under this Regulation shall apply to SWYCHR during the course of sending or receiving funds by wire transfer except transfer and settlement between branches of SWYCHR;

Responsibility of the Ordering Institution

2. SWYCHR as ordering institution (whether domestic or cross border wire transfer and regardless of threshold) shall;
 - (a) identify and verify the originator (if it has not already done under Regulation 1); and obtain details of beneficial owner(s) of funds; and
 - (b) record adequate details of the wire transfer so as to permit its reconstruction, including the date of the wire transfer, the type and amount of currency

involved, the value date, the purpose and details of the wire transfer beneficiary and the beneficiary institution, and relationship between originator and beneficiary, as applicable etc.

3. SWYCHR shall include the following information in the message or payment instruction which should accompany or remain with the wire transfer throughout the payment chain:
 - (a) the name of the originator;
 - (b) the originator's account number (or unique reference number which permits traceability of the transaction);
 - (c) the originator's address and CNIC/ passport number;
 - (d) the name of the beneficiary; and
 - (e) the beneficiary's address and CNIC/ passport number.
4. Where several individual cross-border wire transfers from a single originator are bundled in a batch file for transmission to beneficiaries, the batch file shall contain the required and accurate originator information (originator's account number or unique transaction reference number) and full beneficiary information that is fully traceable within the beneficiary country.

Responsibility of the Beneficiary Institution

5. Beneficiary institution shall verify the identity of the beneficiary, if the identity has not been previously verified, and record this information.
6. Beneficiary institution shall adopt risk-based internal policies, procedures and controls for identifying and handling in-coming wire transfers that are not accompanied by complete originator or beneficiary information. The incomplete originator or beneficiary information may be considered as a factor in assessing whether to execute or terminate the transaction, and in assessing whether the transaction is suspicious and merits reporting to the appropriate authorities.
7. SWYCHR shall remain cautious when entering into relationship or transactions with institutions which do not comply with the standard requirements set out for wire transfers by limiting or even terminating business relationship.

REGULATION - 4

REPORTING OF TRANSACTIONS

1. SWYCHR shall comply with the provisions of AML Act, rules and regulations issued there under for reporting suspicious transactions/currency transactions in the context of money laundering, financing of terrorism and financing of proliferation.
2. SWYCHR shall implement appropriate internal policies, procedures and controls for meeting their obligations under AML Act.
3. SWYCHR shall pay special attention to all complex, unusually large transactions, and all unusual patterns of transactions, which have no apparent economic or visible lawful purpose. The background and purpose of such transactions shall, as far as possible, be examined, the findings established in writing, and be available to assist the relevant authorities in inspection and investigation.
4. SWYCHR ensure to make use of technology and upgrade their systems and procedures in accordance with the changing profile of various risks. Accordingly, SWYCHR will implement automated Transaction Monitoring Systems (TMS) capable of producing meaningful alerts based on pre-defined parameters/thresholds and customer profile, for analysis and possible reporting of suspicious transactions. Further, SWYCHR shall establish criteria in their AML/CFT Policies and/or Procedures for management of such alerts.
5. The adequacy of staff posted for effective monitoring and reporting of suspicious transactions is a critical factor of Customer Due Diligence. SWYCHR shall place adequate number of analysts for monitoring and reporting purpose. Moreover, steps should be taken by SWYCHR to develop knowledge and skills of their staff and utilize technology solutions required for effective Targeted Financial Sanctions (TFS) monitoring and reporting of suspicious transactions.
6. The transactions, which are out of character or are inconsistent with the history, pattern, or normal operation of our business shall be viewed with suspicion, be properly investigated and referred to Compliance Officer for possible reporting to the appropriate authorities.
7. SWYCHR should note that, attempted transactions, should be reported regardless of the amount of the transactions; be reported for the transactions of significant amounts as per requirements of AML provisions in force.
8. The employees of the SWYCHR are strictly prohibited to disclose the fact to the customer or any other quarter that a suspicious transaction or related information is being or has been reported to any authority, except if required by law. This is made part of Code of Ethics to signed by employees and Directors of SWYCHR.

9. The reporting of suspicious transactions/currency transactions in the context of money laundering, financing of terrorism or financing of proliferation shall not be assigned to outsourced employees.

REGULATION - 5
RECORD KEEPING

1. SWYCHR shall maintain all necessary records on transactions, both domestic and international, including the results of any analysis undertaken (e.g. inquiries to establish the background and purpose of complex, unusual large transactions) for a minimum period of ten years from completion of the transaction.
2. The records shall be sufficient to permit reconstruction of individual transactions including the nature and date of the transaction, the type and amount of currency involved and the type and identifying number of any account involved in the transactions so as to provide, when necessary, evidence for prosecution of criminal activity. The transactions records may be maintained in paper or electronic form or on microfilm, provided it is admissible as evidence in a court of law.
3. The records of identification data obtained through CDD process like copies of identification documents, account opening forms, KYC forms, verification documents and other documents along with records of account files and business

correspondence, shall be maintained for a minimum period of ten years after the business relationship is ended. The identification records may be maintained in document as originals or copies.

4. SWYCHR shall, however, retain those records for longer period where transactions, customers or accounts involve litigation or it is required by court or other competent authority.
5. SWYCHR shall satisfy, on timely basis, any enquiry or order from the relevant competent authorities including law enforcement agencies or any other competent authority.

REGULATION - 6

INTERNAL CONTROLS, POLICIES, COMPLIANCE, AUDIT AND TRAINING

SWYCHR own AML/CFT policies, procedures & controls

1. SWYCHR shall formulate its own AML/CFT policy duly approved by their Board of Directors and cascade the same down the line to each and every business location and concerned employees for strict compliance. The detailed procedures and controls shall be developed by SWYCHR in the light of policy approved by the Board.
2. The policies, procedures and controls shall include, amongst other things, CDD measures, record retention, handling wire transfers, risk assessment procedures, the detection of unusual and/or suspicious transactions and the obligation to report suspicious transaction etc.
3. SWYCHR should update their internal risk assessment periodically or in case of any major event or in light of the National Risk Assessments (NRA) duly shared by other competent authorities issued from time to time.
4. In formulating policies, procedures and controls, SWYCHR shall take into consideration money laundering and financing of terrorism threats that may arise from the use of new or developing technologies, especially those having features of anonymity or inconsistency with the spirit of CDD measures.

Compliance

5. SWYCHR shall develop appropriate AML/ CFT compliance program, including at least, the appointment of a management level officer as the compliance officer in line with Regulation provided by appropriate authorities.
6. SWYCHR shall ensure that the compliance officer, as well as any other persons appointed to assist him, has timely access to all customer records and other relevant information which they may require to discharge their functions.
7. SWYCHR shall incorporate procedures to record and maintain data of potential customers whose business got rejected for compliance related issues.
8. SWYCHR shall:
 - (a) in addition to oversight and monitoring of ML/TF risks posed to the entity, the Board shall also be responsible for ensuring that entity has implemented effective AML/CFT controls (preventive measures) including Targeted Financial Sanctions (TFS) related. The board shall delegate oversight and monitoring function to any of the board sub-committees preferably Board Risk Management Committee (BRMC) or Board Audit Committee (BAC) and Compliance Risk Management Committee (CRMC) which has been constituted;
 - (b) include compliance and AML/ CFT related responsibilities in Key Performance Indicators (KPIs) of responsible staff down the line, in order to strengthen the compliance/ AML/CFT function. Moreover, ML/ TF risks should be included in KPIs of officer(s) responsible for Enterprise Risk Management and Operational Risk Management functions;
 - (c) not assign unrealistic business targets and conflicting roles to their employees. Appropriate strategies may be devised to ensure provision of safe and smooth banking services; and
 - (d) regularly assess working strength of the compliance function and all its sub-divisions and deficiency if any, observed should be addressed on priority basis.

Audit

9. SWYCHR shall maintain an independent audit function in line with Code of Corporate Governance that is adequately resourced and able to regularly assess the effectiveness of the bank's internal policies, procedures and controls, and its compliance with regulatory requirements.

Employee Due Diligence

10. SWYCHR shall develop and implement a comprehensive employee due diligence policy and procedure to be implemented/ carried out at the time of hiring all employees permanent, contractual, or through outsourcing to ensure high standards. This shall include but not limited to verification of antecedents and screening procedures to verify that person being inducted/ hired has a clean history.

Training

11. SWYCHR shall chalk out and implement suitable training program for relevant employees on annual basis, in order to effectively implement the regulatory requirements and SWYCHR own policies and procedures relating to AML/ CFT. The employees training shall enable them to understand new developments, money laundering and financing of terrorism techniques, methods and trends. The training should also include their responsibilities relating to AML and analysis of abnormal/out of pattern transactions and alerts generated thereof for possible reporting of suspicious transactions. SWYCHR shall also implement programs covering ML/TF risks and the AML obligations including the results of Risk Assessments conducted by any other Government Agencies. SWYCHR also share its own risk assessment results with its staffs which keep them more vigilant and alert when dealing with such customer, product, channel and geographies.
12. SWYCHR should note that the relevant AML/CFT training combined with optimum use of technology is becoming inevitable due to ever changing nature of methods and trends in illicit activities. It is also important to test the capability and knowledge of the relevant staff on periodic basis. The online trainings and AML/CFT Tests of varying nature are available in the market offering opportunity for companies like SWYCHR to equip their staff with relevant skills as per respective roles and responsibilities within the institution. As the periodic training of the front end staff is crucial, which is the first point of contact with customer; SWYCHR shall either purchase or internally develop comprehensive AML/CFT Computer- based/online Training Programs and Tests under a comprehensive plan with clear timelines for its implementation.

13. Independent testing

The testing of our AML program will be performed at least annually (on a calendar year basis) under the overall supervision of a competent officer with the required skill set, experience and independence to perform such an important task, personnel of our firm, none of whom are the AML Compliance Person nor do they perform the AML functions being tested nor do they report to any such persons. Their qualifications shall include a working knowledge of applicable

requirements under the BSA and its implementing regulations any other regulatory requirements by authorities of all unique regulatory jurisdictions where Swychr has operations at any point in time. To ensure that they remain independent, we will separate their functions from other AML activities. Independent testing will be performed more frequently if circumstances warrant the need for such frequent testing.

After completion of the independent testing, the officer in charge will report his/her team's findings to the audit committee made up mostly of independent non-executive directors and senior management (executive directors). We will promptly address each of the resulting recommendations and keep a record of how each noted deficiency was resolved

14. Adverse media screening

Swychr shall search for adverse media against every newly added account (user) at the time of account creation and then revisit the account based on a schedule guided by policy-designated risk criteria (i.e., account type, jurisdiction, expected activity, etc.).

Over and beyond the scheduled review based on the criteria set out above, Swychr shall also conduct event-triggered media reviews between the normal scheduled reviews as per policy. The activities that may warrant an 'unscheduled' investigation of news sources shall include but not limited to newly discovered account activity, law enforcement inquiries, or higher-risk counterparty relationships.

To ensure a more productive screening, Swychr shall look for digital solution that answers questions like, 'Who in the userbase has noteworthy news already compiled on them by a reputable data provider?' rather than, 'What information exists in the world that may be related to my customer?'. A possible service provider already identified for this are kyc2020.com and blockpass.

By automating the ongoing review of news media sources, we would be by so doing balance the obvious benefits of daily monitoring and surveillance while avoiding the pitfalls of overwhelming analysts with a sea of results containing very few actionable items—or worse, missing relevant actionable items.

Swychr shall develop models based on categories and severity of adverse media to both prioritize the reviews and more effectively understand the appropriate level of risk associated with a client as part of the general KYC profile.

Swychr shall determine the materiality of adverse media based on the age of information and other related factors as this could be effective in some instances. However, Swychr notes that there are certain types of severity related to adverse media that do not subside over time, such as negative news surrounding corruption or other serious financial crimes.

After determining when to search, what to search and how to evaluate results, Swychr would proceed to decide what to do with the information.

A one-and-done screening of any given user will at best identify risk related to historic activity. Whether findings are material or immaterial (i.e. not severe enough to align with a program's calculation of risk), Swychr would ensure to monitor initial findings for future updates.

With a separate, automated process to review updates and changes to known findings, our adverse

media screening policy approach allows for a more targeted use of resources. Otherwise, there is potential to lose sight of updates within the overall results of a volume-heavy adverse media screening system.

Annexure-I

Minimum Documents to be obtained from Various
Types of Customers under AML/CFT
Regulations

Sr	Type of Customers	Documents/papers to be obtained
1.	Individuals	<p>A photocopy of any one of the following valid identity documents;</p> <ul style="list-style-type: none"> (i) Computerized National Identity Card (ii) Passport; having valid visa on it or any other proof of legal stay along with passport (foreign national individuals only).
2.	Sole Proprietors	<ul style="list-style-type: none"> (i) Photocopy of identity document as per Sr. No. 1 above of the proprietor. (ii) Registration certificate for registered concerns. (iii) Sales tax (VAT) registration, wherever applicable. (iv) Certificate or proof of membership of trade bodies etc., wherever applicable. (v) Declaration of sole proprietorship on business letter head.
3.	Partnership	<ul style="list-style-type: none"> (i) Photocopies of identity documents as per Sr. No. 1 above of all the partners and authorized signatories. (ii) Attested copy of 'Partnership Deed' duly signed by all partners of the firm. (iii) Attested copy of Registration Certificate with Registrar of Firms. In case the partnership is unregistered, this fact shall be clearly mentioned. (iv) Authority letter from all partners, in original,
4.	Limited Companies / Corporations	<ul style="list-style-type: none"> (i) Certified copies of: <ul style="list-style-type: none"> (a) Resolution of Board of Directors for specifying the person(s) authorized to conduct business (not applicable for Single Member Company); (b) Memorandum of Association; (c) Articles of Association (wherever applicable);

		(ii) Photocopies of identity documents as per Sr. No. 1 above of all the directors and persons authorized to open and operate the account;
5.	Branch Office or Liaison Office of Foreign Companies	(i) A copy of permission letter from relevant authority i-e Board of Investment. (ii) Photocopies of valid passports of all the signatories of account. (iii) List of directors on company letter head or prescribed format under relevant laws/regulations. (iv) A Letter from Principal Office of the entity authorizing the person(s) to open and operate the account
6.	Trust, Clubs, Societies and Associations etc.	(i) Certified copies of: (a) Certificate of Registration/Instrument of Trust (b) By-laws/Rules & Regulations (ii) Resolution of the Governing Body/Board of Trustees/Executive Committee, if it is ultimate governing body, for opening of account authorizing the person(s) to operate the account. (iii) Photocopy of identity document as per Sr. No. 1 of the following: (a) authorized person(s) (b) members of Governing Body/Board of Trustees /Executive Committee, if it is ultimate governing body (c) settlor, the trustee(s), the protector (if any),
7.	NGOs/ NPOs/Charities	(i) Certified copies of (a) Registration documents/certificate (b) By-laws/Rules & Regulations (ii) Resolution of the Governing Body/ Board of Trustees/ Executive Committee, if it is ultimate governing body, for opening of account authorizing the person(s) to operate the account. (iii) Photocopy of identity document as per Sr. No. 1

		Body/ Board of Trustees/ Executive Committee, if it is ultimate governing body. (iv) Any other documents as deemed necessary including its annual accounts/ financial statements or disclosures in any form which may help to ascertain the detail of its activities, sources and usage of funds
--	--	---

Authorized by:

Name: AARON NKOMBOU MUNGA

Position: CHIEF EXECUTIVE OFFICER

Date: 12.12.2022.