Circular no.: MCX/INSP/710/2023 October 17, 2023

Master Circular on Know Your Client (KYC) norms for the securities market

---

SEBI has issued circular no. SEBI/HO/MIRSD/SECFATF/P/CIR/2023/169 dated October 12, 2023 regarding “Master Circular on Know Your Client (KYC) norms for the securities market”.

The aforesaid SEBI circular is enclosed herewith for ready reference.

Members are requested to take note of the above and comply with applicable regulatory requirements.

Vishal Patelia
Asst. Vice President
(Inspection & Audit)
Encl: SEBI circular no. SEBI/HO/MIRSD/SECFATF/P/CIR/2023/169 dated October 12, 2023.

Kindly contact Inspection & Audit Team on 022-66494150 or send an email at Inspection@mcxindia.com for further clarification.

---------- Corporate office ----------
Multi Commodity Exchange of India Limited
Exchange Square, CTS No. 255, Suren Road, Chakala, Andheri (East), Mumbai – 400 093
Tel.: 022 – 6649 4000 Fax: 022 – 6649 4151 CIN: L51909MH2002PLC135594
www.mcxindia.com email: customersupport@mcxindia.com

भारतीय प्रतिभूति और विनिमय बोर्ड
Securities and Exchange Board of India

MASTER CIRCULAR

SEBI/HO/MIRSD/SECFATF/P/CIR/2023/169 **October 12, 2023**

To,

1. **All Intermediaries registered with SEBI under Section 12 of the Securities and Exchange Board of India Act, 1992**
2. **Recognised Stock Exchanges**
3. **Association of Mutual Funds in India (AMFI)**
4. **Association of Portfolio Managers in India (APMI)**
5. **BSE Administration & Supervision Limited (BASL)**

Dear Sir / Madam,

Subject: Master Circular on Know Your Client (KYC) norms for the securities market

1. The Securities and Exchange Board of India (SEBI) has been issuing various circulars/directions from time to time on Know Your Client (KYC) norms to be followed by intermediaries in the securities market. In order to enable the users to have access to all the applicable circulars/directions at one place, this Master Circular on the captioned subject is being issued.
2. This Master Circular is a compilation of the circulars/directions issued by SEBI up to September 30, 2023 on the captioned subject and includes certain modifications to align such circulars/directions with the provisions of the Prevention of Money Laundering (Maintenance of Records) Rules, 2005[1] and the Securities and Exchange Board of India [KYC (Know Your Client) Registration Agency] Regulations, 2011[2]. The provisions of this Master Circular shall come into force from the date of its issue.
3. Any modifications/updation in existing KYC records, shall be effected in line with the provisions of this Circular by December 31, 2023.
4. On and from the date of issue of this Circular, all circulars for the purpose of KYC as listed in Appendix shall stand rescinded/modified as indicated therein.

[1] Prevention of Money Laundering (Maintenance of Records) Rules, 2005
[2] SEBI {KYC (Know Your Client) Registration Agency} Regulations, 2011

5. Notwithstanding such rescission,
    a) Anything done or any action taken or purported to have been done or taken under the rescinded circulars, prior to such rescission, shall be deemed to have been done or taken under the corresponding provisions of this Master Circular;
    b) Any application made to the Board under the rescinded circulars, prior to such rescission, and pending before it shall be deemed to have been made under the corresponding provisions of this Master Circular;
    c) The previous operation of the rescinded circulars or anything duly done or suffered thereunder, any right, privilege, obligation or liability acquired, accrued or incurred under the rescinded circulars, any penalty, incurred in respect of any violation committed against the rescinded circulars, or any investigation, legal proceeding or remedy in respect of any such right, privilege, obligation, liability, penalty as aforesaid, shall remain unaffected as if the rescinded circulars had never been rescinded.
6. This Master Circular is issued in exercise of powers conferred under Section 11 (1) of the Securities and Exchange Board of India Act, 1992, to protect the interest of investors in securities and to promote the development of, and to regulate, the securities market.
7. This Master Circular is issued with the approval of the Competent Authority.
8. This Master Circular is available at www.sebi.gov.in under the link Legal → Master Circulars.

Yours faithfully,

Sapna Sinha
Deputy General Manager
Email id: sapnas@sebi.gov.in

भारतीय प्रतिभूति और विनिमय बोर्ड
Securities and Exchange Board of India

TABLE OF CONTENTS

Section 1: Know Your Client (KYC) Requirements for the Securities Market 5

Definition 5

Background 7

Uniform KYC Format 7

Requirement of Permanent Account Number (PAN) 7

Exemptions/Clarifications to PAN requirements 8

List of documents admissible as Proof of Identity (PoI) 9

Proof of Address (PoA) 10

Acceptance of third party address as correspondence address 11

Identification of Beneficial Ownership 12

Requirement of additional documents for non-individuals (Legal Entities) 13

Requirement of Mobile Number and Email ID 14

Digital KYC 14

Features for online KYC App of the Intermediary 17

Requirement of In-Person Verification (IPV) 17

Adaptation of Aadhaar based e-KYC process and e-KYC Authentication facility for Resident Investors under section 11A of the Prevention of Money Laundering Act, 2002: KUA and Sub KUA mechanism 19

Entities permitted to undertake e-KYC Aadhaar Authentication service of UIDAI in Securities Market as sub-KUA 20

Onboarding process of Sub-KUA by UIDAI 20

KYC for SARAL Account Opening Form for resident individuals 23

Confidentiality of client information 24

Section 2: Know Your Client (KYC) Registration Agency 24

Guidelines for Intermediaries: 24

Guidelines for KRAs: 24

Rationalisation of Risk Management Framework at KRAs 25

Processing of Investor complaints against KRA {KYC (Know Your Client) Registration Agency} in SEBI Complaints Redress System (SCORES) 26

Cyber Security & Cyber Resilience framework for KYC Registration Agencies (KRAs) 27

Central KYC Records Registry (CKYCR) 27

Annexure A: Framework with regard to Cyber Security and Cyber Resilience for KRAs..... 29

Annexure B: Incident Reporting Form by KRA 38

Annexure C: Form for reporting Cyber attack/breach by KRA 38

Appendix: List of Circulars rescinded 41

Appendix: List of Circulars modified 43

Section 1: Know Your Client (KYC) Requirements for the Securities Market

Definition

1. In this Circular, unless the context otherwise requires, the terms used herein shall bear the meanings as assigned to them below:

a. "Aadhaar number" shall have the same meaning as assigned to it under sub-section (a) of section 2 of the Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016 and includes any alternative virtual identity generated under sub-section (4) of section 3 of that Act.

b. "Act", "Regulations", "Circulars" and "Guidelines" mean the Securities and Exchange Board of India Act, 1992 and the Regulations, Circulars and Guidelines made thereunder and amendments thereto.

c. "Authentication", in the context of Aadhaar authentication, shall have the same meaning as defined under sub-section (c) of section 2 of the Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016.

d. "Beneficial owner" shall have the same meaning as assigned to it under sub section 1 clause (fa) of section 2 of the Prevention of Money Laundering Act, 2002.

e. "Central KYC Records Registry" (CKYCR) shall have the same meaning as assigned to it under Rule 2 (1) (ac) of the Prevention of Money Laundering (Maintenance of Records) Rules, 2005.

f. "Client" shall have the same meaning as assigned to it under Section 2(ha) of the Prevention of Money Laundering Act, 2002.

g. "Client Due Diligence" shall have the same meaning as assigned to it under Rule 2 (1) (b) of the Prevention of Money Laundering (Maintenance of Records) Rules, 2005.

h. "Designated Director" shall have the same meaning as assigned to it under Rule 2 (1) (ba) of the Prevention of Money Laundering (Maintenance of Records) Rules, 2005.

i. “Digital KYC” shall have the same meaning as assigned to it under Rule 2 (1) (bba) of the Prevention of Money Laundering (Maintenance of Records) Rules, 2005.

j. “Digital Signature” shall have the same meaning as assigned to it under clause (p) of subsection (1) of section (2) of the Information Technology Act, 2000 (21 of 2000).

k. "e-KYC authentication facility" shall have the same meaning as assigned to it under clause (j) of sub section (1) of section (2) of Aadhaar (Authentication and Offline Verification) Regulations, 2021.

l. "Electronic Signature" shall have the same meaning assigned to it under clause (ta) of subsection (1) of section (2) of the Information Technology Act, 2000 (21 of 2000).

m. “Equivalent e-document” shall have the same meaning as assigned to it under Rule 2 (1) (cb) of Prevention of Money Laundering (Maintenance of Records) Rules, 2005.

n. “e-Sign” is an online electronic signature service which can be integrated with service delivery applications via an API to facilitate an e-Sign user to digitally sign a document.

o. “Intermediary” shall have the same meaning as assigned to it under sub section 1 clause (g) of section (2) of the Securities and Exchange Board of India (Intermediaries) Regulations, 2008.

p. "Know Your Client (KYC)" means the procedure specified by the Board for identifying and verifying the Proof of Address, Proof of Identity and compliance with rules, regulations, guidelines and circulars issued by the Board or any other authority for Prevention of Money Laundering from time to time.

q. “Person” shall have the same meaning as assigned to it under sub section 1 clause (s) of section 2 of the Prevention of Money laundering Act, 2002.

r. “PMLA” means The Prevention of Money Laundering Act, 2002 (Act No. 15 of 2003) and includes the amendments thereto.

s. “PML Rules” means The Prevention of Money Laundering (Maintenance of Records) Rules, 2005 and includes the amendments thereto.

Background

2. KYC and Client Due Diligence (CDD) policies as part of KYC are the foundation of an effective Anti-Money Laundering process. The KYC process requires every SEBI registered intermediary to obtain and verify the Proof of Identity (PoI) and Proof of Address (PoA) from the client at the time of commencement of an account-based relationship.

3. The registered intermediaries shall not open or keep any anonymous account or account in fictitious names or account on behalf of other persons whose identity has not been disclosed or cannot be verified. The intermediaries shall also continue to abide by circulars issued by SEBI from time to time for prevention of money laundering.

Uniform KYC Format[3]

4. SEBI registered intermediaries shall perform KYC in securities market through physical mode/ digital (online or app based) mode. To bring about uniformity in securities market, all SEBI registered intermediaries shall use the same KYC form and supporting documents. Foreign Portfolio Investors and Eligible Foreign Investors shall be guided as per provisions of SEBI Circular SEBI/HO/AFD-2/CIR/P/2022/175 December 19, 2022 and amendments thereto.

5. The account opening form (AOF) for client shall be divided into two parts. Part I of the AOF shall be the KYC form which shall capture the basic details about the client. For this purpose, all registered intermediaries shall use the KYC templates provided by Central Registry of Securitisation Asset Reconstruction and Security Interest of India (CERSAI) for individuals and for legal entities for capturing the KYC information. The CKYCR templates - Individual and Legal Entity provided by CERSAI is available at https://www.ckycindia.in/ckyc/?r=download.

6. Part II of the form shall obtain the additional information specific to the area of activity of the intermediary, as considered appropriate by them. The instant Master Circular deals with the provisions of Part I -KYC form.

Requirement of Permanent Account Number (PAN)

7. In order to strengthen the KYC norms and identify every participant in the securities market with their respective PAN thereby ensuring sound audit trail of all the transactions, PAN shall be the unique identification number

[3] SEBI Circular No.CIR/MIRSD/16/2011 dated August 22, 2011 and No.MIRSD/SE/Cir-21/2011 dated October 05, 2011

for all participants transacting in the securities market, irrespective of the amount of transaction.

8. The registered intermediaries shall verify the PAN of their clients online at the Income Tax website without insisting on the original or copy of PAN card.

9. As per the provisions of Income-tax Act, 1961 (Income Tax Act), the PAN allotted to a person shall become inoperative if it is not linked with Aadhaar. Since PAN is the key identification number and part of KYC requirements for all transactions in the securities market, all registered intermediaries shall ensure valid PAN in the KYC documentation for all clients.

10. Status of Aadhaar and PAN linkage shall be flagged at the system of KRA.

Exemptions/Clarifications to PAN requirements[4]

11. The following are exempted from the mandatory requirement of PAN:

i. Transactions undertaken on behalf of Central Government and/or State Government and by officials appointed by Courts e.g. Official liquidator, Court receiver etc. (under the category of Government) for transacting in the securities market.

ii. Investors residing in the state of Sikkim.

iii. UN entities/multilateral agencies exempt from paying taxes/filing tax returns in India.

iv. SIP of Mutual Funds upto ₹50,000/- per year.

In case there is change in the name subsequent to issuance of PAN of the client, registered intermediaries can collect the PAN card proof as submitted by the client provided it is supported by a marriage certificate issued by the State Government or gazette notification, indicating such a change of name.

The e-PAN issued by Central Board of Direct Taxes (CBDT) can also be produced by client for KYC compliance. e-PAN is a digitally signed PAN card issued in electronic format by the Income-tax department.

[4] SEBI Circular No.CIR/MIRSD/16/2011 dated August 22, 2011 and No.MIRSD/SE/Cir-21/2011 dated October 05, 2011

List of documents admissible as Proof of Identity (PoI)[5]

12. Registered intermediaries at the time of commencement of an account-based relationship shall identify their clients, verify their identity and obtain information on the purpose and intended nature of the business relationship.

13. The name as mentioned in the KYC form shall match the name as mentioned in the Proof of Identity (PoI) submitted.

14. The following documents shall be accepted as PoI:

    a. Officially valid document (OVD) defined as per Rule 2 (d) of Prevention of Money-Laundering (Maintenance of Records) Rules, 2005 (PML Rules):
        i. the passport;
        ii. the driving licence;
        iii. proof of possession of Aadhaar number;
        iv. the Voter's Identity Card issued by Election Commission of India;
        v. job card issued by NREGA duly signed by an officer of the State Government;
        vi. the letter issued by the National Population Register containing details of name address; or
        vii. any other document as notified by the Central Government in consultation with the Regulator.

    b. Further, in terms of proviso to the above Rule, where simplified measures are applied for verifying the identity of the clients, the following documents shall also be deemed to be officially valid document:

        i. Identity card/ document with applicant's photo, issued by the Central/State Government Departments, Statutory/Regulatory Authorities, Public Sector Undertakings, Scheduled Commercial Banks and Public Financial Institutions;
        ii. Letter issued by a gazetted officer, with a duly attested photograph of the person.

[5] SEBI Circular No.CIR/MIRSD/16/2011 dated August 22, 2011 and No.MIRSD/SE/Cir-21/2011 dated October 05, 2011

15. The registered intermediaries shall not store/ save the Aadhaar number of client in their system. Further, in terms of PML Rule 9(16), every registered intermediary shall, where the client submits his Aadhaar number, ensure that such client redacts or blacks out his Aadhaar number by appropriate means where the authentication of Aadhaar number is not required under sub rule (15) of PML Rule 9.

Proof of Address (PoA)[6]

16. At the time of commencement of an account-based relationship, the registered intermediaries shall along with the PoI, obtain documents as proof of address.

17. The following documents shall be accepted as PoA:

    a. "officially valid document" defined as per Rule 2 (d) of Prevention of Money-Laundering (Maintenance of Records) Rules, 2005 (PML Rules):
        i. the passport;
        ii. the driving licence;
        iii. proof of possession of Aadhaar number;
        iv. the Voter's Identity Card issued by Election Commission of India;
        v. job card issued by NREGA duly signed by an officer of the State Government;
        vi. the letter issued by the National Population Register containing details of name, address; or
        vii. any other document as notified by the Central Government in consultation with the Regulator.

    b. Further, in terms of Rule 9(18) of PML rules, 2005, in case the officially valid document furnished by the client does not contain updated address, the following documents (or their equivalent e-documents thereof) shall be as deemed to be officially valid document for the limited purpose of proof of address, provided that the client shall submit updated officially valid document (or their equivalent e-documents thereof) with current address within a period of three months of submitting the following documents:

    i. utility bill which is not more than two months old of any service provider (electricity, telephone, post-paid mobile phone, piped gas, water bill);

[6] SEBI Circular No.CIR/MIRSD/16/2011 dated August 22, 2011 and No.MIRSD/SE/Cir-21/2011 dated October 05, 2011

ii. property or municipal tax receipt;

iii. pension or family pension payment orders (PPOs) issued to retired employees by Government Departments or Public Sector Undertakings, if they contain the address;

iv. letter of allotment of accommodation from employer issued by state or central government departments, statutory or regulatory bodies, public sector undertakings, scheduled commercial banks, financial institutions and listed companies and leave and licence agreements with such employers allotting official accommodation.

18. In terms of the PML Rules, cases where the client submits his proof of possession of Aadhaar number as an officially valid document, he may submit it in such form as is issued by the UIDAI.

19. A document shall be deemed to an officially valid document even if there is a change in the name subsequent to its issuance provided it is supported by a Marriage Certificate issued by the State Government or a gazette notification, indicating such change of name.

20. For non-residents and foreign nationals, (allowed to trade subject to RBI and FEMA guidelines), copy of passport/Persons of Indian Origin (PIO) Card/Overseas Citizenship of India (OCI) Card and overseas address proof is mandatory.

21. In case the officially valid document presented by a foreign national does not contain the details of address, the documents issued by the Government departments of foreign jurisdictions and letter issued by the Foreign Embassy or Mission in India shall be accepted as proof of address.

22. If any proof of address is in a foreign language, then translation into English shall be required.

23. If correspondence and permanent address is different, then proof for both shall be submitted.

Acceptance of third party address as correspondence address

24. A client can authorize to capture address of a third party as a correspondence address, provided that all prescribed ‘Know Your Client’ norms are also fulfilled for the third party. The intermediary shall obtain proof of identity and proof of address for the third party. The intermediary shall

also ensure that client due diligence norms as specified in Rule 9 of PML Rules are complied with in respect of the third party.

25. Registered intermediaries at the time of commencement of an account-based relationship shall determine whether the client purports to act on behalf of juridical person or individual or trust and the registered intermediary shall verify that any person purporting to act on behalf of such client is so authorized and verify the identity of that person.

Identification of Beneficial Ownership

26. SEBI Master Circular SEBI/HO/MIRSD/MIRSD-SEC-5/P/CIR/2023/022 dated February 03, 2023 on Guidelines on Anti-Money Laundering (AML) Standards and Combating the Financing of Terrorism (CFT) /Obligations of Securities Market Intermediaries under the Prevention of Money Laundering Act, 2002 and Rules framed there under has prescribed the approach to be followed towards identification of beneficial ownership at Para 11 (iii) therein. Accordingly, the registered intermediaries may be guided by the provisions of the said Master Circular and amendments thereto for the purpose of identification of beneficial ownership of the client.

27. Whenever it is apparent that the securities acquired or maintained through an account are beneficially owned by a party other than the client, that party shall be identified using client identification and verification procedures.

28. The registered intermediaries shall conduct ongoing CDD where inconsistencies are noticed in the information provided. The underlying objective shall be to follow the requirements enshrined in the PMLA, PML Rules, SEBI Act and Regulations, directives and circulars issued thereunder so that the intermediary is aware of the clients on whose behalf it is dealing.

29. The registered intermediaries shall periodically update all documents, data or information of all clients and beneficial owners collected under the CDD process.

30. The stock exchanges and depositories shall monitor the compliance of the aforementioned provision on identification of beneficial ownership through half yearly internal audits. In case of mutual funds, compliance of the same shall be monitored by the Boards of the Asset Management Companies and the Trustees and in case of other registered intermediaries, by their Board of Directors.

Requirement of additional documents for non-individuals (Legal Entities)[7]

31. In case of non-individuals, additional documents (certified copies of equivalent e-documents) to be obtained are mentioned below:

i. Corporate body:

a. Certificate of incorporation.
b. Memorandum and Articles of Association.
c. Board Resolution for investment in securities market.
d. Power of Attorney granted to its managers, officers or employees, as the case may be, to transact on its behalf.
e. Authorised signatories list with specimen signatures.
f. Copy of the balance sheet for the last financial year (initially for the last two financial years and subsequently for every last financial year).
g. Latest share holding pattern including list of all those holding control, either directly or indirectly, in the company in terms of SEBI takeover Regulations, duly certified by the company secretary/whole time director/ MD (to be submitted every year).
h. Photograph, POI, POA, PAN and DIN numbers of whole time directors/two directors in charge of day to day operations.
i. Photograph, POI, POA, PAN of individual promoters holding control - either directly or indirectly.

ii. Partnership firm:

a. Certificate of registration (for registered partnership firms only).
b. Copy of partnership deed.
c. Copy of the balance sheet for the last financial year (initially for the last two financial years and subsequently for every last financial year).
d. Authorised signatories list with specimen signatures.
e. Photograph, POI, POA, PAN of Partners.

iii. Trust:

a. Certificate of registration (for registered trust only).
b. Copy of Trust deed.
c. Copy of the balance sheet for the last financial year (initially for the last two financial years and subsequently for every last financial year).
d. List of trustees certified by managing trustees/CA.
e. Photograph, POI, POA, PAN of Trustees.

[7] SEBI Circular No.CIR/MIRSD/16/2011 dated August 22, 2011 and No.MIRSD/SE/Cir-21/2011 dated October 05, 2011

iv. HUF:
   a. Deed of declaration of HUF/ List of coparceners.
   b. Bank pass-book/bank statement in the name of HUF.
   c. Photograph, POI, POA, PAN of Karta.

v. Unincorporated association or a body of individuals:
   a. Proof of Existence/Constitution document.
   b. Resolution of the managing body & Power of Attorney granted to transact business on its behalf.
   c. Authorized signatories list with specimen signatures.

vi. Banks/Institutional Investors:
   a. Copy of the constitution/registration or annual report/balance sheet for last financial year (initially for the last two financial years and subsequently for every last financial year).
   b. Authorized signatories list with specimen signatures.

vii. Army/ Government Bodies:
   a. Self-certification on letterhead.
   b. Authorized signatories list with specimen signatures.

viii. Registered Society:
   a. Copy of Registration Certificate under Societies Registration Act.
   b. List of Managing Committee members.
   c. Committee resolution for persons authorised to act as authorised signatories with specimen signatures.
   d. True copy of Society Rules and Bye Laws certified by the Chairman/Secretary.

Requirement of Mobile Number and Email ID

32. The registered intermediaries shall upload the details of mobile number and email address on the KRA system. It shall be ensured that the mobile number/email addresses of their employees/authorized persons, distributors etc. are not uploaded on behalf of clients.

Digital KYC

33. In order to enable the online KYC process for establishing account based relationship with the registered intermediary, client's KYC shall be completed through digital (online / Application (App) based) KYC, in-person verification through video, online submission of officially valid document / other documents, using electronic/digital signature, including Aadhaar e-Sign.

34. The client shall visit the website/App/digital platform of the registered intermediary and fill up the online KYC form and submit requisite documents.

35. SEBI registered intermediaries shall obtain the express consent of the client before undertaking online KYC.

36. The PAN, name, photograph, address, mobile number and email ID of the client shall be captured digitally and officially valid document shall be provided as a photo / scan of the original under electronic/digital signature, including Aadhaar e-Sign and the same shall be verified.

37. Any officially valid document other than Aadhaar shall be submitted through Digiocker / using electronic/digital signature, including Aadhaar e-Sign.

38. The mobile number of client accepted as part of KYC should preferably be the one seeded with Aadhaar.

39. Mobile and email shall be verified through One Time Password (OTP) or other verifiable mechanism.

40. Aadhaar shall be verified through UIDAI's authentication/ verification mechanism. Further, in terms of PML Rule 9(16), every intermediary shall, where the client submits his Aadhaar number, ensure that such client redacts or blacksout his Aadhaar number through appropriate means where the authentication of Aadhaar number is not required under sub-rule (15) under PML Rule.

41. e-KYC through Aadhaar Authentication service of UIDAI (e-KYC) or offline verification through Aadhaar QR Code/ XML file can be undertaken, provided the XML file or Aadhaar Secure QR Code generation date is not older than 3 days from the date of carrying out KYC.

42. The usage of Aadhaar shall be optional and purely on a voluntary basis by the client.

43. Any document, except for the documents mentioned in the First Schedule of the Information Technology Act, 2000, shall be authenticated by a client by way of electronic/digital signature including Aadhaar e-Sign. Accordingly, the process of performing KYC shall be completed by using electronic/digital signature including Aadhaar e-Sign.

44. A client can use the electronic/digital signature, including Aadhaar e-Sign service to submit the document to the registered intermediary.

45. In case of non-individual clients, intermediaries shall exercise caution and satisfy themselves regarding the genuineness of the authorization and identity of the authorized signatories.

46. The electronic/digital signature, including Aadhaar e-Sign shall be accepted in lieu of wet signature on the documents provided by the client. The cropped signature affixed on the online KYC form under electronic/digital signature, including Aadhaar e-Sign shall also be accepted as valid signature.

47. Bank details of the client shall be captured online and signed cancelled cheque shall be provided as a photo / scan of the original under electronic/digital signature including Aadhaar e-Sign. Bank account details shall be verified by Penny Drop mechanism or any other mechanism using API of the Bank. The name and bank details as obtained shall be verified with the information provided by client.

48. Once all the required information as per the online KYC form is filled up by the investor, KYC process shall be completed as under:

    a. The client shall take a print out of the completed KYC form and after affixing their wet signature, send the scanned copy / photograph of the same to the registered intermediary under electronic/digital signature including Aadhaar e-Sign or
    b. Affix online the cropped signature on the filled KYC form and submit the same to the registered intermediary under electronic/digital signature including Aadhaar e-Sign.
    c. The “original seen and verified” requirement for officially valid document would be met where the investor provides the officially valid document in the following manner:
        i. As a clear photograph or scanned copy of the original officially valid document, through the electronic/digital signature including Aadhaar e-Sign, or;
        ii. As digitally signed document of the officially valid document, issued through the DigiLocker by the issuing authority.

Features for online KYC App of the Intermediary

49. SEBI registered intermediary can implement its own App for undertaking online KYC of clients.

50. The App shall facilitate taking photograph, scanning, acceptance of officially valid document through Digilocker, video capturing in live environment and usage of the App only by authorized person of the intermediary.

51. The App shall also have features of random action initiation for client response to establish that the interactions are not pre-recorded along with time stamping and geo-location tagging to ensure the requirement like physical location being in India etc are also implemented.

52. Registered intermediaries shall ensure that the process is a seamless, real-time, secured, end-to-end encrypted audio-visual interaction with the client and the quality of the communication is adequate to allow identification of the client beyond doubt. Registered intermediaries shall carry out the liveliness check in order to guard against spoofing and such other fraudulent manipulations.

53. The intermediaries shall, before rolling out and periodically, carry out software and security audit and validation of their App. The intermediaries can have additional safety and security features other than as prescribed above.

Requirement of In-Person Verification (IPV)

54. It shall be mandatory for all the registered intermediaries to carry out IPV of their clients.

55. The intermediaries shall ensure that the details like name of the person doing IPV, his designation, organization with his signatures and date are recorded on the KYC form at the time of IPV.

56. The IPV carried out by one SEBI registered intermediary can be relied upon by another intermediary.

57. In case of Stock brokers, their Authorised Persons (appointed by the stock brokers after getting approval from the concerned Stock Exchanges) can perform the IPV.

58. In case of Mutual Funds, their Asset Management Companies (AMCs) and the distributors who comply with the certification process of National Institute of Securities Market (NISM) or Association of Mutual Funds (AMFI) and have undergone the process of 'Know Your Distributor (KYD)', can perform the IPV. Additionally, entities registered as Category 1 Execution Only Platform (EOP) can perform the IPV.

59. In case of applications received by the mutual funds directly from the clients (i.e. not through any distributor), they may also rely upon the IPV performed by the scheduled commercial banks.

60. To enable ease of completing IPV of an investor, intermediary may undertake the Video in Person Verification (VIPV) of an individual investor through their App. The following process shall be adopted in this regard:

    a) Intermediary through their authorised official, specifically trained for this purpose, may undertake live VIPV of an individual client, after obtaining his/her informed consent. The activity log along with the credentials of the person performing the VIPV shall be stored for easy retrieval.
    b) The VIPV shall be in a live environment.
    c) The VIPV shall be clear and still, the client in the video shall be easily recognisable and shall not be covering their face in any manner.
    d) The VIPV process shall include random question and response from the investor including displaying the officially valid document, KYC form and signature or could also be confirmed by an OTP.
    e) The intermediary shall ensure that photograph of the client downloaded through the Aadhaar authentication / verification process matches with the investor in the VIPV.
    f) The VIPV shall be digitally saved in a safe, secure and tamper-proof, easily retrievable manner and shall bear date and time stamping.
    g) The intermediary may have additional safety and security features other than as prescribed above.

61. IPV shall not be required in the cases where:

    a) the KYC of the client has been completed using the Aadhaar authentication/ verification of UIDAI.
    b) the KYC form has been submitted online, documents have been provided through Digilocker or any other source which could be verified online.

Adaptation of Aadhaar based e-KYC process and e-KYC Authentication facility for Resident Investors under section 11A of the Prevention of Money Laundering Act, 2002: KUA and Sub KUA mechanism

62. Registered intermediaries for reasons such as online on-boarding of clients, client convenience, increased efficiency and reduced time for client onboarding would prefer to use Aadhaar based e-KYC facility to complete KYC of the client.

63. The e-KYC service launched by UIDAI shall be accepted as a valid process for KYC verification.

64. As per the process outlined by Department of Revenue (DoR), Ministry of Finance (MoF) vide circular dated May 09, 2019 for use of Aadhaar authentication services by entities other than the banking companies, entities in the securities market as may be notified by the Central Government shall be allowed to undertake Aadhaar Authentication under section 11A of the PMLA .

65. These entities would be registered with UIDAI as KYC user agency (KUA)/sub KYC user Agency (sub-KUA).The KUAs shall allow the SEBI registered intermediaries as sub-KUA to undertake Aadhaar Authentication of their clients for the purpose of KYC.

66. The following entities shall get registered with UIDAI as KYC user agency ("KUA") and shall allow SEBI registered intermediaries to undertake Aadhaar Authentication in respect of their clients for the purpose of KYC.

    (i) Bombay Stock Exchange Limited
    (ii) National Securities Depository Limited
    (iii) Central Depository Services (India) Limited
    (iv) CDSL Ventures Limited
    (v) NSDL Database Management Limited
    (vi) NSE Data and Analytics Limited
    (vii) CAMS Investor Services Private Limited
    (viii) Computer Age Management Services Private Limited
    (ix) National Stock Exchange of India Limited (NSE).

67. SEBI registered intermediaries who want to undertake Aadhaar authentication services through KUAs, shall enter into an agreement with any one KUA and get themselves registered with UIDAI as Sub-KUAs. The agreement in this regard shall be as prescribed by UIDAI.

Entities permitted to undertake e-KYC Aadhaar Authentication service of UIDAI in Securities Market as sub-KUA

68. Department of Revenue (DoR), Ministry of Finance (MoF), Government of India, vide Gazette Notification Nos. S.O. 3187(E) dated July 13, 2022 and S.O. 446 (E) dated January 30, 2023 has notified reporting entities to use Aadhaar authentication services of UIDAI under section 11A of the Prevention of Money-laundering Act, 2002. The notifications can be accessed at the links (Govt. Notification dated July 13, 2022 and Govt Notification dated Jan 30, 2023.pdf). These entities shall act as Sub-KUA.

69. The KUAs shall facilitate the onboarding of these entities as Sub-KUAs to provide the services of Aadhaar authentication with respect to KYC.

Onboarding process of Sub-KUA by UIDAI

70. As provided in the DoR circular dated May 09, 2019, SEBI after scrutiny of the application forms of KUAs shall forward the applications along with its recommendation to UIDAI.

71. For appointment of SEBI registered intermediary as Sub-KUAs, KUA shall send list of proposed Sub-KUAs to SEBI and SEBI would forward the list of recommended Sub-KUAs to UIDAI for onboarding.

72. An agreement shall be signed between KUA and Sub-KUA, as prescribed by UIDAI. Sub-KUA shall also comply with the Aadhaar Act, 2016, regulations, circulars, guidelines etc. issued by UIDAI from time to time.

73. Each sub-KUA shall be assigned a separate Sub-KUA code by UIDAI.

74. The KUA/sub-KUA shall be guided by the above for use of Aadhaar authentication services of UIDAI for e-KYC.

75. The KUAs and sub KUAs shall adopt the following process for Aadhaar e-KYC of investors (resident) in the securities market:

A. Online Portal based Investor (Resident) e-KYC Process (Aadhaar as an officially valid document)

i. Client visits portal of KUA or the SEBI registered intermediary which is also a Sub-KUA to open account/invest through intermediary.

ii. For Aadhaar e-KYC, client is redirected to KUA portal. Client enters the Aadhaar Number or Virtual Id and provides consent on KUA

portal. Adequate controls shall be in place to ensure that Aadhaar Number is not stored anywhere by the Sub-KUA or KUA.

iii. Client shall receive OTP in mobile number registered with Aadhaar. Client enters the OTP sent by UIDAI on KUA portal for Aadhaar e-KYC.

iv. KUA shall receive the e-KYC details from UIDAI upon successful Aadhaar authentication which shall be further forwarded to Sub-KUA in encrypted format (using KUAs own encryption key) and shall be displayed to the client on portal.

v. Sharing of e-KYC data by the KUA with Sub-KUA shall be allowed under Regulation 16(2) of Aadhaar (Authentication) Regulations, 2016. Sub-KUA shall clearly specify the name of the KUA and Sub-KUA, and details of sharing of data among KUA and Sub-KUA while capturing client consent.

vi. Client shall fill the additional detail as required under KYC format.

B. Assisted Investor (Resident) e-KYC process (Aadhaar as an officially valid document):

i. Client approaches any of the SEBI Registered Entity/ Sub-KUAs for e-KYC through Aadhaar.

ii. SEBI registered entities (Sub-KUAs) shall perform e-KYC using registered / whitelisted devices with KUAs.

iii. KUA shall ensure that all devices and device operators of Sub-KUA are registered / whitelisted devices with KUA.

iv. Client shall enter Aadhaar No. or Virtual Id and provide consent on the registered device.

v. Client provides biometric on the registered device.

vi. SEBI registered intermediary (Sub-KUA) fetches the e-KYC details through the KUA from UIDAI which shall be displayed to the client on the registered device.

vii. Client shall also provide the additional detail as required.

76. The KUA/ sub-KUA while performing the Aadhaar authentication shall comply with the following:

i. For sharing of e-KYC data with Sub-KUA under Regulation 16(2) of Aadhaar (Authentication) Regulations, 2016, KUA shall obtain special permission from UIDAI by submitting an application in this regard. Such permissible sharing of e-KYC details by KUA can be allowed with their associated Sub-KUAs only.

ii. KUA shall not share UIDAI digitally signed e-KYC data with other KUAs. However, KUAs may share data after digitally signing it using their own signature for internal working of the system.

iii. e-KYC data received as response upon successful Aadhaar authentication from UIDAI shall be stored by KUA and Sub-KUA in the manner prescribed by Aadhaar Act/Regulations and circulars issued by UIDAI time to time.

iv. KUA/Sub-KUA shall not store Aadhaar number in their database under any circumstances. It shall be ensured that Aadhaar number is captured only using UIDAI's Aadhaar Number Capture Services (ANCS).

v. The KUA shall maintain auditable logs of all such transactions where e-KYC data has been shared with sub-KUA, for a period specified by the Authority.

vi. It shall be ensured that full Aadhaar number is not stored and displayed anywhere in the system and wherever required only last 4 digits of Aadhaar number may be displayed.

vii. As per Regulation 14(i) of the Aadhaar (Authentication) Regulation, 2016, requesting entity shall implement exception-handling mechanisms and backup identity authentication mechanism to ensure seamless provision of authentication services to Aadhaar number holders.

viii. UIDAI may conduct audit of all KUAs and Sub KUAs as per the Aadhaar Act, Aadhaar Regulations, AUA/KUA Agreement, Guidelines, circulars etc. issued by UIDAI from time to time.

ix. Monitoring of irregular transactions - KUAs shall develop appropriate monitoring mechanism to record irregular transactions and their reporting to UIDAI.

x. Investor Grievance Handling Mechanism - Investor may approach KUA for their grievance redressal. KUA shall ensure that the grievance is redressed within the timeframe as prescribed by UIDAI. KUA shall also submit report on grievance redressal to UIDAI as per timelines prescribed by UIDAI.

77. For non-compliances if any observed on the part of the reporting entities (KUAs/ Sub KUAs), SEBI shall take necessary action under the applicable laws and also bring the same to the notice of DoR / FIU/UIDAI for further necessary action, if any.

78. The registered intermediary (KUAs/Sub-KUAs) shall also adhere to the continuing compliances and standards of privacy and security prescribed by UIDAI to carry out Aadhaar Authentication Services under section 11A of PMLA.

79. Based on a report from SEBI / UIDAI or otherwise, if it is found that the reporting entity no longer fulfils the requirements for performing authentication under clause (a) of section 11A(1) of PMLA, the Central Government may withdraw the notification after giving an opportunity to the reporting entity.

KYC for SARAL Account Opening Form for resident individuals

80. For individual clients participating in the cash segment without obtaining various other facilities such as internet trading, margin trading, derivative trading and use of power of attorney, the requirement of submission of 'proof of address' shall be as follows:

    a. Individual client may submit only one documentary proof of address (either residence/correspondence or permanent) while opening a trading account and / or demat account or while undergoing updation.

    b. In case the proof of address furnished by the said client is not the address where the client is currently residing, the intermediary may take a declaration of the residence/correspondence address on which all correspondence shall be made by the intermediary with the client. No proof is required to be submitted for such correspondence/residence address. In the event of change in this address due to relocation or any other reason, client may intimate the new address for correspondence to the intermediary within two weeks of such a change. The residence/ correspondence address and any such change thereof may be verified by the intermediary through 'positive confirmation' such as (i) acknowledgment of receipt Welcome Kit/ dispatch of contract notes / any periodical statement, etc. (ii) telephonic conversation; (iii) visits, etc.

    c. The registered intermediaries shall forward the KYC completion intimation letter through registered post/ speed post or courier, to the address of the client in cases where the client has given address other than as given in the officially valid document. In such cases of return of the intimation letter for wrong / incorrect address, addressee not available etc, no transactions shall be allowed in such account and intimation shall also sent to the Stock Exchange and Depository.

    d. The registered intermediaries and KRAs shall flag such accounts in their records/systems.

Confidentiality of client information

81. Registered intermediaries shall keep confidential every information maintained, furnished or verified, save as otherwise provided under any law for the time being in force.

Section 2: Know Your Client (KYC) Registration Agency

82. A mechanism of Know Your Client Registration Agency (KRAs) in the securities market has been developed for centralization of the KYC records. The KRAs shall be administered under SEBI KYC Registration Agency (KRA) Regulations, 2011.

Guidelines for Intermediaries:

83. The client shall be allowed to open an account with intermediaries and transact in securities market as soon as the KYC process is completed.

84. After doing the initial KYC of the new clients, the intermediary shall forthwith upload the KYC information on the system of the KRA within 3 working days from the date of completion of KYC process.

85. In case a client's KYC documents sent by the intermediary to KRA are not complete, the KRA shall inform the same to the intermediary who shall forward the required information / documents promptly to KRA.

86. For existing clients, the KYC data shall be uploaded by the intermediary provided they are in conformity with details sought in the uniform KYC format. While uploading these clients' data the intermediary shall ensure that there is no duplication of data in the KRA system.

87. The intermediaries shall maintain electronic records of KYCs of clients and keeping physical records would not be necessary.

88. The intermediary shall promptly provide KYC related information to KRA, as and when required.

89. The intermediary shall have adequate internal controls to ensure the security / authenticity of data uploaded by it.

Guidelines for KRAs:

90. KRA system shall provide KYC information in data and image form to the intermediary.

91. KRA shall send a letter to the client within 2 working days of the receipt of the initial/updated KYC documents from intermediary, confirming the details thereof and maintain the proof of dispatch.

92. KRA(s) shall develop systems, in co-ordination with each other, to prevent duplication of entry of KYC details of a client and to ensure uniformity in formats of uploading / modification / downloading of KYC data by the intermediary.

93. KRA shall maintain an audit trail of the upload / modifications / downloads made in the KYC data, by the intermediary in its system.

94. KRA shall ensure that a comprehensive audit of its systems, controls, procedures, safeguards and security of information and documents is carried out annually by an independent auditor. The Audit Report along with the steps taken to rectify the deficiencies, if any, shall be placed before its Board of Directors. Thereafter, the KRA shall send the Action Taken Report to SEBI within 3 months.

95. KRA systems shall clearly indicate the status of clients falling under PAN exempt categories viz. investors residing in the state of Sikkim, UN entities / multilateral agencies exempt from paying taxes / filing tax returns in India, etc.

Rationalisation of Risk Management Framework at KRAs

96. As a part of risk management framework, the KRAs shall verify the following attributes of records of all clients within 2 days of receipt of KYC records:

    a. PAN (including PAN Aadhaar linkage, as referred to in rule 114 AAA of the Income-tax Rules, 1962)
    b. Name
    c. Address

97. Additionally, the KRAs shall verify the client's mobile number and email id.

98. In case of PAN exempt records, the other attributes i.e. name, address, mobile number and email id shall be verified by the KRAs.

99. Clients in whose case, attributes of records as mentioned in para 96/97 above cannot be verified, shall not be allowed to transact further in securities market until the attributes are verified.

100. The records of those clients in respect of which all attributes mentioned in para 96/97 above are verified by KRAs with official databases (such as Income Tax Department database on PAN, Aadhaar XML/Digilocker/ M-Aadhaar) shall be considered as Validated Records.

101. The validated records shall be allowed portability i.e. the client need not undergo the KYC process again when the client approaches different intermediary in securities market and the intermediary shall fetch the validated records from the KRA database.

102. The KRAs shall follow uniform internal guidelines/standards detailing aspects of identification of attributes and procedures for verification/ validation, in consultation with SEBI.

103. The systems of intermediaries and the KRAs shall be integrated to facilitate seamless movement of documents/information to and from the intermediary to the KRAs for verification/validation of attributes under risk management framework.

104. The records of all existing clients whose KYC has been completed based on OVDs other than Aadhaar, shall be verified by December 31, 2023.

Processing of Investor complaints against KRA {KYC (Know Your Client) Registration Agency} in SEBI Complaints Redress System (SCORES)

105. All complaints pertaining to KRAs will be electronically sent through SCORES at http://scores.gov.in/Admin. KRAs are directed to view the pending complaints and submit the ATR along with supporting documents electronically in SCORES. Updation of action taken would not be possible with physical ATRs. Hence, submission of physical ATR will not be accepted for complaints lodged in SCORES.

106. KRAs shall take adequate steps for redressal of grievances within one month from the date of receipt of the complaint and keep the investor and SEBI duly informed on the action taken thereon. Failure to comply with the said requirement will render the KRA liable for penal action.

107. KRAs are advised to:
    a. develop the monitoring mechanism through internal audit and inspections.
    b. encourage investor to use SCORES for lodging their grievances.

Cyber Security & Cyber Resilience framework for KYC Registration Agencies (KRAs)

108. Rapid technological developments in securities market have highlighted the need for maintaining robust Cyber Security and Cyber Resilience framework to protect the integrity of data and guard against breaches of privacy.

109. A robust Cyber Security and Cyber Resilience framework should identify the plausible sources of operational risk, both internal and external, and mitigate the impact through the use of appropriate systems, policies, procedures, and controls. Systems should be designed to ensure a high degree of security and operational reliability and should have adequate, scalable capacity. Business continuity management should aim for timely recovery of operations and fulfilment of its obligation in the event of cyber-attack.

110. Since KRAs perform important function of maintaining KYC records of the clients in the securities market, the KRAs shall have robust Cyber Security and Cyber Resilience framework in order to provide essential facilities and perform systemically critical functions relating to securities market.

111. The framework placed at **Annexure A** shall be complied by the KRAs with regard to Cyber Security and Cyber Resilience.

112. The KRAs shall conduct comprehensive cyber audit at least twice in a financial year. All KRAs shall submit a declaration from the MD/ CEO certifying compliance by the KRAs with all SEBI Circulars and advisories related to Cyber security from time to time, along with the cyber audit report

Central KYC Records Registry (CKYCR)

113. Government of India has authorized the Central Registry of Securitization Asset Reconstruction and Security interest of India (CERSAI), set up under sub-section (1) of Section 20 of Securitization and Reconstruction of Financial Assets and Enforcement of Security Interest Act, 2002, to act as, and to perform the functions of, the Central KYC Records Registry under the PML Rules, 2005, including receiving, storing, safeguarding and retrieving the KYC records in digital form of a “client”, as defined in clause (ha) sub-section (1) of Section 2 of the PMLA, 2002.

114. As required under the PML Rules, registered intermediaries shall capture the KYC information for sharing with the Central KYC Records Registry in the manner mentioned in the PML Rules, as per the KYC template finalised by CERSAI.

115. Registered intermediaries shall within ten days after the commencement of an account-based relationship with a client, file the electronic copy of the client's KYC records with the CKYCR.

116. Registered intermediaries shall ensure that all existing KYC records of legal entities and of individual clients are uploaded on to CKYCR when the updated information is obtained/received from the client.

117. The Central KYC Records Registry User Manual for uploading KYC records on CKYCR finalised by CERSAI is available at https://www.ckycindia.in/ckyc/assets/doc/User_Manual_1.12.1.pdf.

118. Registered intermediaries shall ensure compliance with requirements contained in the PML Rules in this regard.

119. For addressing any difficulty in uploading KYC records to CKYCR, CERSAI has operationalised a help desk. Contact details of the CKYCR Helpdesk: Phone: 022-61102592 /022 50623300 Email: helpdesk@ckycindia.in

Annexure A: Framework with regard to Cyber Security and Cyber Resilience for KRAs

1. Cyber-attacks and threats attempt to compromise the confidentiality, integrity and availability (CIA) of the computer systems, networks and databases (Confidentiality refers to limiting access of systems and information to authorized users, Integrity is the assurance that the information is reliable and accurate, and Availability refers to guarantee of reliable access to the systems and information by authorized users).Cyber security framework includes measures, tools and processes that are intended to prevent cyber-attacks and improve cyber resilience. Cyber Resilience is an organisation's ability to prepare and respond to a cyber-attack and to continue operation during, and recover from, a cyber-attack.

Governance

2. As part of the operational risk management framework to manage risk to systems, networks and databases from cyber-attacks and threats, KRAs shall formulate a comprehensive Cyber Security and Cyber Resilience policy document encompassing the framework mentioned hereunder. The policy document shall be approved by the Board of KRAs, and in case of deviations from the suggested framework, reasons for such deviations shall also be provided in the policy document. The policy document shall be reviewed by the Board of KRAs at least annually with the view to strengthen and improve its Cyber Security and Cyber Resilience framework.

3. The Cyber Security and Cyber Resilience policy shall include the following process to identify, assess, and manage cyber security risk associated with processes, information, networks and systems

    3.1. 'Identify' critical IT assets and risks associated with such assets,
    3.2. 'Protect' assets by deploying suitable controls, tools and measures,
    3.3. 'Detect' incidents, anomalies and attacks through appropriate monitoring tools/processes,
    3.4. 'Respond' by taking immediate steps after identification of the incident, anomaly or attack,
    3.5. 'Recover' from incident through incident management, disaster recovery and business continuity framework.

4. The Cyber security policy shall encompass the principles prescribed by National Critical Information Infrastructure Protection Centre (NCIIPC) of National Technical Research Organisation (NTRO), Government of India, in the report titled 'Guidelines for Protection of National Critical Information Infrastructure' and subsequent revisions, if any, from time to time.

5. KRAs shall also incorporate best practices from standards such as ISO 27001, ISO 27002, COBIT 5, etc., or their subsequent revisions, if any, from time to time.

6. KRAs shall designate a senior official as Chief Information Security Officer (CISO) whose function would be to assess, identify and reduce cyber security risks, respond to incidents, establish appropriate standards and controls, and direct the establishment and implementation of processes and procedures as per the cyber security and resilience policy approved by the Board of the KRAs.

7. The Board of the KRAs shall constitute a Technology Committee comprising experts proficient in technology. This Technology Committee shall on a quarterly basis review the implementation of the Cyber Security and Cyber Resilience policy approved by their Board, and such review shall include review of their current IT and Cyber Security and Cyber Resilience capabilities, set goals for a target level of cyber resilience, and establish a plan to improve and strengthen Cyber Security and Cyber Resilience. The review shall be placed before the Board of the KRAs for appropriate action.

8. KRAs shall establish a reporting procedure to facilitate communication of unusual activities and events to CISO or to the senior management in a timely manner.

9. The aforementioned committee and the senior management of the KRAs, including the CISO, shall periodically review instances of cyber attacks, if any, domestically and globally, and take steps to strengthen Cyber Security and Cyber Resilience framework.

10. KRAs shall define responsibilities of its employees, outsourced staff, and employees of vendors, members or participants and other entities, who may have access or use KRA's systems / networks, towards ensuring the goal of cyber security.

Identification

11. KRAs shall identify and classify critical assets based on their sensitivity and criticality for business operations, services and data management. The critical assets shall include business critical systems, internet facing applications /systems, systems that contain sensitive data, sensitive personal data, sensitive financial data, Personally Identifiable Information (PII) data, etc. All the ancillary systems used for accessing/communicating with critical systems either for operations or maintenance shall also be classified

as critical system. The Board of the KRAs shall approve the list of critical systems.

To this end, KRAs shall maintain up-to-date inventory of its hardware and systems, software and information assets (internal and external), details of its network resources, connections to its network and data flows.

12. KRAs shall accordingly identify cyber risks (threats and vulnerabilities) that it may face, along with the likelihood of such threats and impact on the business and thereby, deploy controls commensurate to the criticality.

13. KRAs shall also encourage its third-party providers, if any, to have similar standards of Information Security.

Protection

Access Controls

14. No person by virtue of rank or position shall have any intrinsic right to access confidential data, applications, system resources or facilities.

15. Any access to KRA's systems, applications, networks, databases, etc., shall be for a defined purpose and for a defined period. KRAs shall grant access to IT systems, applications, databases and networks on a need-to-use basis and based on the principle of least privilege. Such access shall be for the period when the access is required and shall be authorized using strong authentication mechanisms.

16. KRAs shall implement strong password controls for users' access to systems, applications, networks and databases. Password controls shall include a change of password upon first log-on, minimum password length and history, password complexity as well as maximum validity period. The user credential data shall be stored using strong and latest hashing algorithms.

17. KRAs shall ensure that records of user access are uniquely identified and logged for audit and review purposes. Such logs shall be maintained and stored in encrypted form for a time period not less than two (2) years.

18. KRAs shall deploy additional controls and security measures to supervise staff with elevated system access entitlements (such as admin or privileged users). Such controls and measures shall inter-alia include restricting the number of privileged users, periodic review of privileged users' activities, disallow privileged users from accessing systems logs in which their activities are being captured, strong controls over remote access by privileged users, etc.

19. Account access lock policies after failure attempts shall be implemented for all accounts.

20. Employees and outsourced staff such as employees of vendors or service providers, who may be given authorised access to the KRA's critical systems, networks and other computer resources, shall be subject to stringent supervision, monitoring and access restrictions.

21. Two-factor authentication at log-in shall be implemented for all users that connect using online/internet facility.

22. KRAs shall formulate an Internet access policy to monitor and regulate the use of internet and internet based services such as social media sites, cloud-based internet storage sites, etc.

23. Proper 'end of life' mechanism shall be adopted to deactivate access privileges of users who are leaving the organization or whose access privileges have been withdrawn.

Physical security

24. Physical access to the critical systems shall be restricted to minimum. Physical access of outsourced staff/visitors shall be properly supervised by ensuring at the minimum that outsourced staff/visitors are accompanied at all times by authorised employees.

25. Physical access to the critical systems shall be revoked immediately if the same is no longer required.

26. KRAs shall ensure that the perimeter of the critical equipment room are physically secured and monitored by employing physical, human and procedural controls such as the use of security guards, CCTVs, card access systems, mantraps, bollards, etc. where appropriate.

Network Security Management

27. KRAs shall establish baseline standards to facilitate consistent application of security configurations to operating systems, databases, network devices and enterprise mobile devices within the IT environment. The KRAs shall conduct regular enforcement checks to ensure that the baseline standards are applied uniformly.

28. KRAs shall install network security devices, such as firewalls as well as intrusion detection and prevention systems, to protect their IT infrastructure from security exposures originating from internal and external sources.

29. Anti-virus software shall be installed on servers and other computer systems. Updation of anti-virus definition files and automatic anti-virus scanning shall be done on a regular basis.

Security of Data

30. Data-in-motion and Data-at-rest shall be in encrypted form by using strong encryption methods such as Advanced Encryption Standard (AES), RSA, SHA-2, etc.

31. KRAs shall implement measures to prevent unauthorised access or copying or transmission of data / information held in contractual or fiduciary capacity. It shall be ensured that confidentiality of information is not compromised during the process of exchanging and transferring information with external parties.

32. The information security policy shall also cover use of devices such as mobile phone, faxes, photocopiers, scanners, etc. that can be used for capturing and transmission of data.

33. KRAs shall allow only authorized data storage devices through appropriate validation processes.

Hardening of Hardware and Software

34. Only a hardened and vetted hardware / software shall be deployed by the KRAs. During the hardening process, KRAs shall inter-alia ensure that default passwords are replaced with strong passwords and all unnecessary services are removed or disabled in equipment / software.

35. All open ports which are not in use or can potentially be used for exploitation of data shall be blocked. Other open ports shall be monitored and appropriate measures shall be taken to secure the ports.

Application Security and Testing

36. KRAs shall ensure that regression testing is undertaken before new or modified system is implemented. The scope of tests shall cover business logic, security controls and system performance under various stress-load scenarios and recovery conditions.

Patch Management

37. KRAs shall establish and ensure that the patch management procedures include the identification, categorisation and prioritisation of security patches. An implementation timeframe for each category of security patches shall be established to implement security patches in a timely manner.

38. KRAs shall perform rigorous testing of security patches before deployment into the production environment so as to ensure that the application of patches do not impact other systems.

Disposal of systems and storage devices

39. KRAs shall frame suitable policy for disposals of the storage media and systems. The data / information on such devices and systems shall be removed by using methods viz. wiping / cleaning / overwrite, degauss and physical destruction, as applicable.

Vulnerability Assessment and Penetration Testing (VAPT)

40. KRAs shall carry out periodic vulnerability assessment and penetration tests(VAPT) which inter-alia include critical assets and infrastructure components like Servers, Networking systems, Security devices, load balancers, other IT systems pertaining to the activities done as KRAs etc., in order to detect security vulnerabilities in the IT environment and in-depth evaluation of the security posture of the system through simulations of actual attacks on its systems and networks.

    KRAs shall conduct VAPT at least once in a financial year. However, for the KRAs, whose systems have been identified as “protected system” by NCIIPC under the Information Technology (IT) Act, 2000, VAPT shall be conducted at least twice in a financial year. Further, all KRAs are required to engage only CERT-In empanelled organizations for conducting VAPT. The final report on said VAPT shall be submitted to SEBI after approval from Technology Committee of respective KRAs, within one month of completion of VAPT activity.

41. Any gaps/vulnerabilities detected shall be remedied on immediate basis and compliance of closure of findings identified during VAPT shall be submitted to SEBI within 3 months post the submission of final VAPT report.

42. In addition, KRAs shall perform vulnerability scanning and conduct penetration testing prior to the commissioning of a new system which is a critical system or part of an existing critical system.

Monitoring and Detection

43. KRAs shall establish appropriate security monitoring systems and processes to facilitate continuous monitoring of security events and timely detection of unauthorised or malicious activities, unauthorised changes, unauthorised access and unauthorized copying or transmission of data / information held in contractual or fiduciary capacity, by internal and external parties. The security logs of systems, applications and network devices shall also be monitored for anomalies.

44. Further, to ensure high resilience, high availability and timely detection of attacks on systems and networks, KRAs shall implement suitable mechanism to monitor capacity utilization of its critical systems and networks.

45. Suitable alerts shall be generated in the event of detection of unauthorized or abnormal system activities, transmission errors or unusual online transactions.

Response and Recovery

46. Alerts generated from monitoring and detection systems shall be suitably investigated, including impact and forensic analysis of such alerts, in order to determine activities that are to be performed to prevent expansion of such incident of cyber attack or breach, mitigate its effect and eradicate the incident.

47. The response and recovery plan of the KRAs shall aim at timely restoration of systems affected by incidents of cyber attacks or breaches. KRAs shall have the same Recovery Time Objective (RTO) and Recovery Point Objective (RPO) as specified by SEBI for Market Infrastructure Institutions vide SEBI circular CIR/MRD/DMS/17/20 dated June 22, 2012 as amended from time to time.

48. The response plan shall define responsibilities and actions to be performed by its employees and support / outsourced staff in the event of cyber attacks or breach of cyber security mechanism.

49. Any incident of loss or destruction of data or systems shall be thoroughly analysed and lessons learned from such incidents shall be incorporated to strengthen the security mechanism and improve recovery planning and processes.

50. KRAs shall also conduct suitable periodic drills to test the adequacy and effectiveness of response and recovery plan.

Sharing of information

51. All Cyber-attacks, threats, cyber-incidents and breaches experienced by KRAs shall be reported to SEBI within 6 hours of noticing / detecting such incidents or being brought to notice about such incidents.

    The incident shall also be reported to Indian Computer Emergency Response team (CERT-In) in accordance with the guidelines / directions issued by CERT-In from time to time. Additionally, the KRAs, whose systems have been identified as "Protected system" by National Critical Information Infrastructure Protection Centre (NCIIPC) shall also report the incident to NCIIPC.

    The quarterly reports containing information on cyber-attacks, threats, cyber-incidents and breaches experienced by KRAs and measures taken to mitigate vulnerabilities, threats and attacks including information on bugs/ vulnerabilities/threats that may be useful for other KRAs shall be submitted to SEBI within 15 days from the quarter ended June, September, December and March of every year. The above information shall be shared through the dedicated e-mail id: kra@sebi.gov.in. The format for submitting the quarterly reports is attached as Annexure C.

52. Such details as are felt useful for sharing with other KRAs in masked and anonymous manner shall be shared using mechanism to be specified by SEBI from time to time.

Training

53. KRAs shall conduct periodic training programs to enhance awareness level among the employees and outsourced staff, vendors, etc. on IT / Cyber security policy and standards. Special focus shall be given to build awareness levels and skills of staff from non-technical disciplines.

54. The training program shall be reviewed and updated to ensure that the contents of the program remain current and relevant.

Periodic Audit

55. KRAs shall arrange to have its systems audited on an annual basis by an CERT-IN empanelled auditor, an independent DISA (ICAI) Qualification, CISA (Certified Information System Auditor) from ISACA, CISM (Certified Information Securities Manager) from ISACA, CISSP (Certified Information

Systems Security Professional) from International Information Systems Security Certification Consortium (commonly known as (ISC)2), to check compliance with the above areas and shall submit the report to SEBI along with the comments of the Board of KRAs within three months of the end of the financial year.

56. Further, the KRAs shall conduct comprehensive cyber audit at least twice a financial year. All KRAs shall submit a declaration from the MD/ CEO certifying compliance by the KRAs with all SEBI Circulars and advisories related to Cyber security from time to time, along with the cyber audit report.

57. KRAs shall take necessary steps to put in place systems for implementation of this framework.

भारतीय प्रतिभूति और विनिमय बोर्ड
Securities and Exchange Board of India

Annexure B: Incident Reporting Form by KRA

Incident Reporting Form		
1. Letter / Report Subject -		
Name of the intermediary - SEBI Registration no. - Type of intermediary -		
2. Reporting Periodicity Year-		
☐ Quarter 1 (Apr-Jun) ☐ Quarter 2 (Jul-Sep)	☐ Quarter 3 (Oct-Dec) ☐ Quarter 4 (Jan-Mar)	
3. Designated Officer (Reporting Officer details) -		
Name:	Organization:	Title:
Phone / Fax No:	Mobile:	Email:
Address:		
Cyber-attack / breach observed in Quarter: (If yes, please fill **Annexure C**) (If no, please submit the NIL report)		
Date & Time	Brief information on the Cyber-attack / breached observed	

Annexure C: Form for reporting Cyber attack/breach by KRA	
1. Physical location of affected computer / network and name of ISP -	
2. Date and time incident occurred -	
Date:	Time:

3. Information of affected system -

IP Address:	Computer / Host Name:	Operating System (incl. Ver. / release No.):	Last Patched/ Updated:	Hardware Vendor/ Model:

4. Type of incident -

☐ Phishing ☐ Network scanning /Probing Break-in/Root Compromise ☐ Virus/Malicious Code ☐ Website Defacement ☐ System Misuse	☐ Spam ☐ Bot/Botnet ☐ Email Spoofing ☐ Denial of Service(DoS) ☐ Distributed Denial of Service(DDoS) ☐ User Account Compromise	☐ Website Intrusion ☐ Social Engineering ☐ Technical Vulnerability ☐ IP Spoofing ☐ Ransomware ☐ Other_____

5. Description of incident -

6. Unusual behaviour/symptoms (Tick the symptoms) -

☐ System crashes ☐ New user accounts/ Accounting discrepancies ☐ Failed or successful social engineering attempts ☐ Unexplained, poor system performance ☐ Unaccounted for changes in the DNS tables, router rules, or firewall rules ☐ Unexplained elevation or use of privileges Operation of a program or sniffer device to capture network traffic; ☐ An indicated last time of usage of a user account that does not correspond to the actual last time of usage for that user ☐ A system alarm or similar indication from an intrusion detection tool ☐ Altered home pages, which are usually the intentional target for visibility, or other	☐ Anomalies ☐ Suspicious probes ☐ Suspicious browsing New files ☐ Changes in file lengths or dates ☐ Attempts to write to system ☐ Data modification or deletion ☐ Denial of service ☐ Door knob rattling ☐ Unusual time of usage ☐ Unusual usage patterns ☐ Unusual log file entries ☐ Presence of new setuid or setgid files Changes in system directories and files ☐ Presence of cracking utilities

pages on the Web server	☐ Activity during non-working hours or holidays ☐ Other (Please specify)

7. Details of unusual behaviour/symptoms -

8. Has this problem been experienced earlier? If yes, details -

9. Agencies notified -

Law Enforcement	Private Agency	Affected Product Vendor	Other _____

10. IP Address of apparent or suspected source -

Source IP address:	Other information available:

11. How many host(s) are affected -

1 to 10	10 to 100	More than 100

12. Details of actions taken for mitigation and any preventive measure applied -

Appendix: List of Circulars rescinded

Sr. No.	Circular No. and date	Subject
1.	SEBI/MIRSD/Cir.No.02/2010 dated 18-Jan-10	Mandatory Requirement of "In-Person" Verification of clients
2.	CIR/MIRSD/22/2011 dated 25-Oct-11	In-person verification (IPV) of clients by subsidiaries of Stock Exchanges, acting as Stock Brokers
3.	MIRSD/Cir-23/2011 dated 02-Dec-11	The Securities And Exchange Board of India (KYC Registration Agency) Regulations, 2011
4.	MIRSD/Cir-26/2011 Dated 23-Dec-11	Guidelines In Pursuance of The SEBI KYC Registration Agency (KRA) Regulations, 2011 And For In-Person Verification (IPV)
5.	MIRSD/CIR-5/2012 dated 13-Apr-12	Uploading of The Existing Clients' KYC Details In The KYC Registration Agency (KRA) System by The Intermediaries
6.	CIR/MIRSD/09/2012 dated 13-Aug-12	Aadhaar Letter As Proof of Address For Know Your Client (KYC) Norms
7.	CIR/MIRSD/12/2012 dated 21-Sep-12	Processing of investor complaints against KRA {KYC (Know Your Client) Registration Agency} in SEBI Complaints Redress System (SCORES)
8.	CIR/MIRSD/01/2013 dated 04-Jan-13	Rationalisation Process For Obtaining PAN by Investors
9.	CIR/MIRSD/2/2013 dated 24-Jan-13	Guidelines On Identification of Beneficial Ownership
10.	CIR/MIRSD/ 4 /2013 dated 28-Mar-13	Amendment to SEBI {(Know Your Client) Registration Agency} Regulations, 2011 and relevant circulars
11.	CIR/MIRSD/09/2013 dated 08-Oct-13	For Know Your Client Requirements
12.	CIR/MIRSD/13/2013 dated 26-Dec-13	For Know Your Client Requirements
13.	CIR/MIRSD/1/2015 dated 04-Mar-15	Saral Account Opening Form For Resident Individuals
14.	CIR/MIRSD/29/2016 dated 22-Jan-16	Know Your Client Requirements - Clarification On Voluntary Adaptation of Aadhaar Based E-KYC Process

15.	CIR/MIRSD/66/2016 dated 21-Jul-16	Operationalisation of Central KYC Records Registry (CKYCR)
16.	CIR/MIRSD/120/2016 dated 10-Nov-16	Uploading of The Existing Clients' KYC Details With Central KYC Records Registry (CKYCR) System by The Registered Intermediaries
17.	SEBI/HO/MIRSD/DOP/CIR/P/2019/111 dated 15-Oct-19	Cyber Security &Cyber Resilience framework for KYC Registration Agencies
18.	SEBI/HO/MIRSD/DOP/CIR/P/2019/123 dated 05-Nov-19	E-KYC Authentication Facility Under Section 11A of The Prevention of Money Laundering Act, 2002 by Entities In The Securities Market For Residents Investor
19.	SEBI/HO/MIRSD/DOP/CIR/P/2020/73 dated 24-Apr-20	Clarification On Know Your Client (KYC) Process And Use of Technology For KYC
20.	SEBI/HO/MIRSD/DOP/CIR/P/2020/80 dated 12-May-20	Entities Permitted To Undertake E-KYC Aadhaar Authentication Service of UIDAI In Securities Market
21.	SEBI/HO/MIRSD/DOP/CIR/P/2020/167 dated 08-Sep-20	Entities Permitted To Undertake E-KYC Aadhaar Authentication Service of UIDAI In Securities Market – Addition of NSE To The List
22.	SEBI/HO/MIRSD/DOP/CIR/P/2021/31 dated 10-Mar-21	Rollout of Legal Entity Template
23.	SEBI/HO/MIRSD/DoP/P/CIR/2022/74 dated 30-May-22	Modification in Cyber Security and Cyber resilience framework of KYC Registration Agencies (KRAs)
24.	SEBI/HO/MIRSD/DoP/P/Cir/2022/89 dated 24-Jun-22	Implementation of Circular on 'Guidelines in pursuance of amendment to SEBI KYC (Know Your Client) Registration Agency (KRA) Regulations 2011
25.	SEBI/HO/MIRSD/TPD/P/CIR/2022/95 dated 05-Jul-2022	Modification in Cyber Security and Cyber resilience framework of KYC Registration Agencies (KRAs)
26.	SEBI/HO/MIRSD/DoP/P/Cir/2022/89 dated 20-Jul-22	Entities allowed to use e-KYC Aadhaar Authentication Services of UIDAI in Securities Market as Sub KUA
27.	SEBI/HO/MIRSD/SEC-5/0/CIR/2022/100 dated 27-Jul-22	Implementation of Circular on 'Guidelines in pursuance of amendment to SEBI KYC (Know Your Client) Registration Agency (KRA) Regulations 2011'
28.	SEBI/HO/MIRSD/SEC-5/P/CIR/2023/0026 dated 08-Feb-2023	Entities allowed to use e-KYC Aadhaar Authentication Services of UIDAI in Securities Market as Sub KUA

29.	SEBI/HO/MIRSD/FATF/P/CIR/2023/0144 dated 11-Aug-2023	Simplification of KYC process and rationalisation of Risk Management Framework at KYC (Know Your Client) Registration Agencies (KRAs)

Appendix: List of Circulars modified

Sr. No.	Circular No. and date	Subject
1.	CIR/MIRSD/16/2011 dated 22-Aug-2011	Simplification and Rationalization of Trading Account Opening Process.
2.	MIRSD/SE/CIR-21/2011 dated 05-Oct-11	Uniform Know Your Client (KYC) Requirements For The Securities Markets